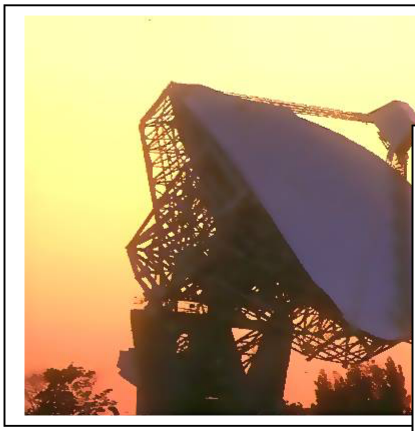
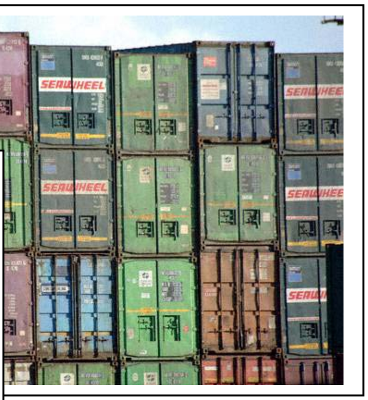
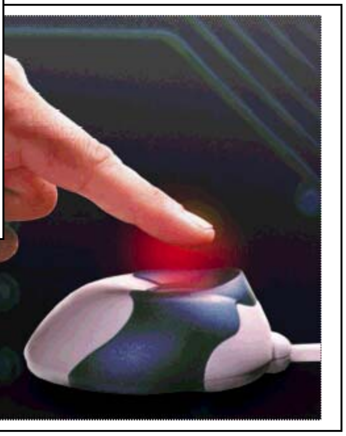
Homeland Security and the Trucking Industry







Final Report

Prepared by:
Max Donath
University of Minnesota

Dan Murray
Jeff Short
American Transportation Research Institute

Prepared for:
International Truck & Engine Corporation

Published by:
Intelligent Transportation Systems Institute
Center for Transportation Studies, University of Minnesota
In conjunction with
American Transportation Research Institute

CTS 05-08

Technical Report Documentation Page

1. Report No.
CTS 05-08

2.

3. Recipients Accession No.

4. Title and Subtitle
Homeland Security and the Trucking Industry

5. Report Date
July, 2005

6.

7. Author(s)
Max Donath, University of Minnesota, Dan Murray and Jeff Short, American Transportation Research Institute

8. Performing Organization Report No.

9. Performing Organization Name and Address

Dept of Mechanical Engineering
and the Intelligent Transportation
Systems Institute,
University of Minnesota
111 Church St. SE
Minneapolis, MN 55455

American Transportation Research
Institute
2200 Mill Road
Alexandria, VA 22314

10. Project/Task/Work Unit No.

11. Contract (C) or Grant (G) No.
U of MN Cufs # 1743-530-6637

12. Sponsoring Organization Name and Address
International Truck and Engine Corporation
2911 Meyer Road,
Ft. Wayne, IN 46803

13. Type of Report and Period Covered

14. Sponsoring Agency Code

15. Supplementary Notes
http://www.cts.umn.edu/pdf/CTS-05-08.pdf

16. Abstract (Limit: 200 words)

The University of Minnesota's Intelligent Transportation Systems (ITS) Institute was contracted by International Truck to undertake an analysis of commercial vehicle operations (CVO) and to determine how new technologies and post-9/11 security programs and policies may impact the operational environment of the trucking industry.

The University of Minnesota and the American Transportation Research Institute, the research arm of the trucking industry, conducted a series of interviews, literature scans and analyses on security programs, industry trends and technology systems.

The following report attempts to document existing and developing trends in CVO economics and technology investment with an emphasis on onboard systems, and their inter-relationships with security preparedness and issues and implications associated with homeland security imperatives. An in-depth review of smart card applications, biometric verification systems and cargo management devices are included.

17. Document Analysis/Descriptors

Commercial Vehicle Operations
Technology
Security
Smart Card
Biometric Verification
Cargo Management

18.Availability Statement
No restrictions. Document available from: National Technical Information Services, Springfield, Virginia 22161

19. Security Class (this report)	20. Security Class (this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	103	

Homeland Security and the Trucking Industry

Final Report

Prepared by:
Max Donath
University of Minnesota

Dan Murray
Jeff Short
American Transportation Research Institute

Prepared for:
International Truck & Engine Corporation

July 2005

Intelligent Transportation Systems Institute
Center for Transportation Studies
University of Minnesota
In conjunction with
American Transportation Research Institute

CTS 05-08

ACKNOWLEDGEMENTS

We would like to thank Saflink Corporation for their assistance in documenting security technologies.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

EXECUTIVE SUMMARY

Since 1904, the year that the trucking industry was first formalized, commercial vehicles have played a vital role in almost every segment of our country's growth. Far from glamorous, the truck has hauled nearly every conceivable commodity in peacetime and in wartime, from coast-to-coast and every location in between. In fact, 72 percent of communities in the United States are now served exclusively by truck. The trucking industry's ability to respond rapidly to changes in economic supply and demand has made it the largest single freight mode in the world in terms of both tonnage moved and freight revenue.

However, this growth and dynamism is not without consequences. The modern, post-deregulation trucking industry suffers from severe competition, low operating margins, critical driver shortages and a growing gap in size, sophistication and resources between small and large carriers. Furthermore, the criticality and complexity of the trucking industry may ostensibly increase its security vulnerabilities and threats.

Historical references to security in the trucking industry have almost always related to some variation of crime, cargo theft, trucking safety or personal protection for drivers. Prior to September 11, 2001, trucks were not a typical target – or conduit – for terrorism. Throughout the world, there are probably fewer than a dozen documented cases of Class 8-sized trucks being used in terrorist attacks. Here in the U.S. there have only been one or two isolated cases where large trucks were used as weapons, and in those instances it was not part of an organized campaign but rather a disturbed individual. Other "trucking-oriented terrorism" examples such as the Oklahoma City bombing also fail to meet many typical post-9/11 terrorism standards since it utilized a smaller straight truck and was organized by several disgruntled U.S. citizens.

Nevertheless, it is well accepted that the trucking industry possesses some important attributes associated with terrorism, including access, sizeable volumes, adequate kinetic energy and an open operational environment. For these reasons, there has been considerable attention paid to the trucking industry by politicians, law enforcement personnel and national security analysts.

The first part of this report documents and describes numerous non-security realities that are manifest in the industry. These include economic and operational realities; personnel issues; technology applications and uses; and the regulatory and political environment in which motor carriers operate. In each case, the authors have attempted to explain the (sometimes subtle) security implications associated with what appear to be disparate topics and issues.

Furthermore, as an industry that is extremely sensitive to the consequences that might arise from a truck-based attack, and cognizant of their responsibilities, motor carriers have worked with security stakeholders to research, analyze, develop and sometimes invest in a host of programs, strategies, and technologies that directly or indirectly address security concerns. In some cases, these trucking industry security partnerships are still attempting to define the problems, threats and vulnerabilities. Until appropriate risk assessments are performed, solutions cannot be applied, which raises concerns that certain vulnerabilities may remain unresolved and the window of opportunity for attack remains wide open. Unfortunately, it is nearly impossible to identify and institute valid solutions without comprehensive risk and threat assessments.

In this regard, this report attempts to identify, amalgamate and analyze numerous security initiatives, technologies and policies that either exist in the industry, or are being considered for implementation. In an effort to manage the scope of the topic, the authors have over-simplified the industry into three primary components:

- Cargo;
- Assets/Conveyance/Facilities; and
- Personnel.

The report has placed considerable attention on the role and impact of technologies in the trucking industry. New and emerging security technologies have been identified and/or reviewed for industry applications; these include electronic seals (cargo management), biometric identification systems (personnel management) and tracking systems (asset management). However, since the post-9/11 trucking industry security technology field is less than four years old, the authors have taken the liberty of analyzing and proposing existing motor carrier technologies for security purposes. One of the more common technology errors is extrapolating and inferring security benefits from one industry sector or application to another. For example: at least one federally sponsored research initiative discussed herein reviewed trucking industry security technologies in different operating scenarios and documented dramatically different returns on investment (ROI) for nearly identical systems. In total, the authors have attempted to go beyond system descriptions to include technology opportunities and limitations. Much of this is based on related secondary research that has tested or considered the efficacy of the devices and systems. Whenever possible, cost-benefit and/or ROI findings are included to provide both industry and government readers with additional empirical data.

There are myriad agencies and programs that have direct or indirect oversight of the trucking industry. For example, one analysis concluded that there are more than 25 different jurisdictions charged with managing U.S.-Canadian cross-border freight movements. While the security interest of these jurisdictions is smaller and presupposes a smaller number of stakeholders, the security management environment is large and complex. There are new congressionally mandated agencies and programs with a focus on motor carrier security. There are also new programs – both voluntary and mandatory – that have been created by pre-9/11 jurisdictions, and there are new entities still being considered. This report attempts to document and organize (generally by jurisdiction) the various programs and agencies that have a nexus to trucking industry security. It is certainly not an exhaustive list.

It is well recognized that many security technologies and programs are relatively untested in the real-world trucking environment. This may be the single biggest concern for both industry practitioners and those specifically tasked with safeguarding the country. As appropriate, the authors have attempted to document where and when additional research is needed on a particular topic or technology. These assertions are based on a knowledge of the trucking industry, a general understanding of technologies, programs and policies that have been field-tested, and consideration of the objectivity of the test environment.

Lastly, in an effort to simply the complex world of technology, security and the trucking industry, this report provides various resources and references for understanding trucking security-related acronyms, programs and industry concepts.

CHAPTER 1. BACKGROUND

1.1 A Primer on the Trucking Industry

The economic health of the U.S. trucking industry and our nation's security are intertwined in a complex relationship which requires a concurrent effort to identify and reduce security vulnerabilities while enhancing freight-generating economic growth. At the most extreme level, freight-related security issues can be resolved or eradicated by eliminating freight conveyance. However, doing so would almost certainly result in economic damages that far exceed most conceivable terrorist attack scenarios. This realization, supported by national research discourse[1] that recognize the need for an open transportation system with reasonable levels of risk acceptance, forms the basis for developing security strategies and programs that address security concerns without undermining the viability of the trucking industry and the nation's transportation systems. An essential step in developing those security solutions is first understanding the operational characteristics and significant issues associated with the trucking industry.

The U.S. economy is the most complex manufacturing and distribution system in the world, moving billions of dollars of raw commodities and manufactured goods to domestic and international markets every day. In total, the country's freight modes represent 10 percent of the U.S. gross domestic product (GDP), with the trucking industry alone comprising nearly 90 percent of this value (See Figure 1).

In order to annually move more than 9 billion tons of manufactured goods to markets[2], the trucking industry has evolved into a large and complex system. In 2004, there were more than 675,000 for-hire carriers registered with the U.S. DOT, employing more than

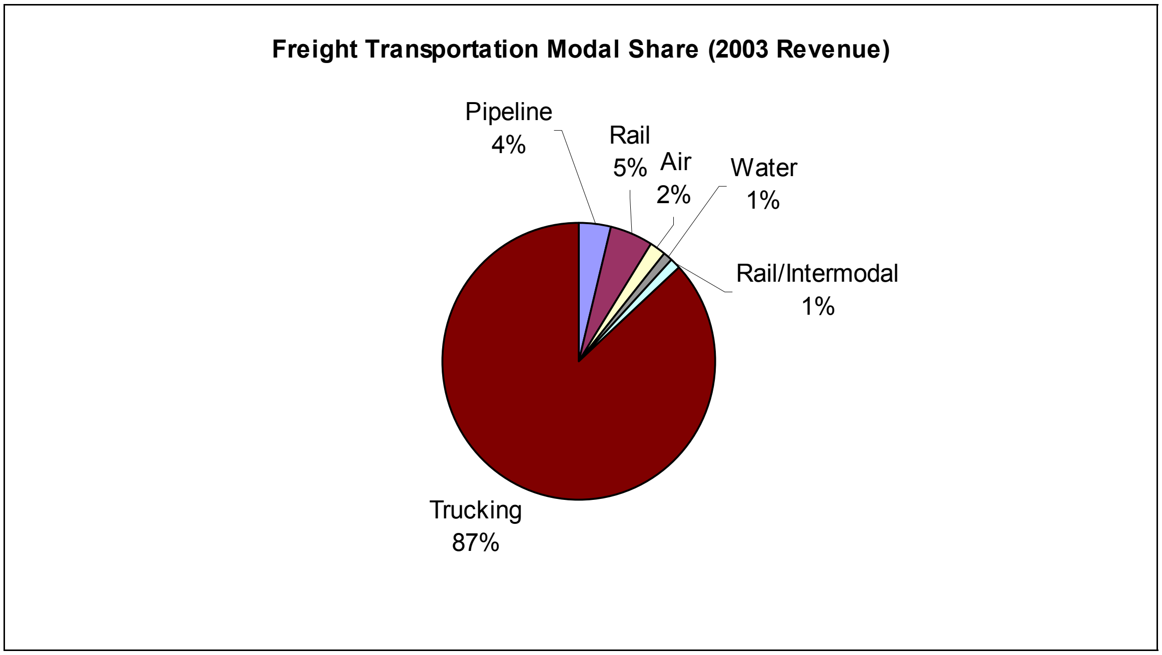
---

[1] Making the Nation Safer, NRC/TRB Special Report 270, 2002

[2] American Trucking Trends 2003; American Trucking Association, 2004

10 million people; 3.2 million of these were CDL-holding truck drivers. To manage the diverse flow of goods, unique sectors have developed within the industry including truckload, less-than-truckload, tank lines, specialized, small-package delivery services, household goods movers, agricultural movers, refrigerated produce haulers, hazmat and many others. Beyond these traditional sectors, numerous highly specialized carriers are emerging, often utilizing custom-built assets. In total, these sectors utilize dramatically different equipment designs, back-room and onboard technologies, and even driver compensation schemas.

Figure 1. Freight Transportation Modal Share



Source: *U.S. Freight Transportation Forecast to 2015*, ATA
Note: this report is available through the ATA Market Place: 800-282-5463

To simplify the organizational description of the trucking industry, the most common differentiation used is for-hire carriers and private fleets (see Table 1). The primary business service of for-hire carriers is provision of transportation services. For-hire fleets represent between 30 percent and 50 percent of all trucking firms, depending on the exact classification and designation of the fleets[3]. Common examples of for-hire fleets include Schneider National, Roadway Express, JB Hunt, Fedex and Overnite Transportation.

---

[3] Ibid, 2003

Private fleet transportation is typically a secondary support unit to a larger business entity, such as a manufacturing or retail operation. Examples of private fleets would include Walmart, General Mills, 3M and components of the US Postal service. Often times, businesses supplement their private fleet operations with for-hire carriers; much less common is the use of private fleets in limited for-hire situations.

Other carrier nomenclature exists as well. However, interstate and intrastate deregulation of the trucking industry in the 80s and 90s has made industry descriptors such as common carrier and regular-route carrier less meaningful.

Suffice it to say, the statistics that reflect the size and diversity of the industry are too numerous to mention here. Table 2 provides some of the industry's key operating statistics.

Table 1. Top Ten For-Hire & Private Fleets[4] (by revenue in $ millions)

For-Hire Carriers	Private Fleets
1. UPS Inc.	1. Sysco Corp.
2. FedEx Corp.	2. Wal*Mart Stores
3. Yellow Roadway Corp.	3. Ahold USA (US Foodservice)
4. CNF Inc. (Conway/Menlo)	4. Tyson Foods
5. Ryder Systems	5. McLane Company
6. Penske Truck Leasing	6. Kroger Co.
7. Schneider National	7. Safeway Inc.
8. Exel PLC	8. Halliburton Co.
9. JB Hunt Transport Services	9. Frito-Lay NA
10. Swift Transportation	10. Unisource Worldwide

---

[4] Transport Topics; 100 Largest For-Hire/Private Fleets, 2004

Table 2. CVO Transportation Statistics[5]

REVENUE…

- $610.1 billion in primary[6] freight shipment revenues, representing 86.9% of all freight revenue in 2003

TONNAGE…

- 9.1 billion tons of manufactured freight, representing 68.9% of total domestic tonnage in 2003.

COMPANIES…

670,000 interstate motor carriers on file with FMCSA in 2004

  - 87.3% operate 6 or fewer trucks
  - 95.9% operate 20 or fewer trucks

TRUCKS….

- 24.6 million registered commercial trucks in 2003 (excludes government)
- 2.6 million Class 8 trucks for business purposes in 2003
- 4.9 million commercial trailers registered in 2003

MILEAGE…

- 444.4 billion miles logged by all Class 3-8 business trucks in 2003
  - Represents 15.6% of all vehicle miles traveled
- 114.1 billion miles logged by Class 8 business trucks in 2003

FUEL CONSUMPTION…

- 49.8 billion gallons of fuel consumed by commercial trucks in 2003

TAXES…

- $31.3 billion paid by commercial trucks in federal and state highway-user taxes in 2003
- Commercial trucks represent 10.6% of registered vehicles, and pay 33.7% of all highway user taxes

---

[5] American Trucking Associations, Economic & Statistics Group, 2004

[6] Typically described as the first order of shipment on the primary bill of lading; secondary shipments include multiple and redundant shipments relating to new Bureau of Labor (BOL) documentation.

1.2 Industry Characteristics and Sectors

1.2.1 Industry Operating Characteristics: Fleet Size

Regardless of how it is classified or segmented, the trucking industry is complex and disparate. Fleet and company size is one example. While the 100 largest carriers move the majority of manufactured freight tonnage in the U.S., approximately 92 percent of all trucking companies have 20 or fewer trucks, with more than 87 percent having 6 or fewer trucks[7]. In fact, the large majority of registered trucking companies are owner-operators with operating authority and a single truck. The end result is that a single employee-owner may provide all standard trucking support services ranging from safety inspections and maintenance to driver management and technology investment decision-making. Aside from the impacts that interstate and intrastate deregulation had on carrier competition, the effects of relatively few barriers-to-entry but high operating expenses -- insurance, fuel, labor -- have resulted in a substantial increase in total registered trucking companies as well as a relatively high number of bankruptcies[8]. This makes access to, and management of, carriers a challenging task for public- and private-sector stakeholders.

1.2.2 Major Sectors: Truckload (TL) Carriers

The truckload industry, those carriers that typically focus on a dedicated movement of single loads between facilities or load centers, is the largest sector within the for-hire component.

---

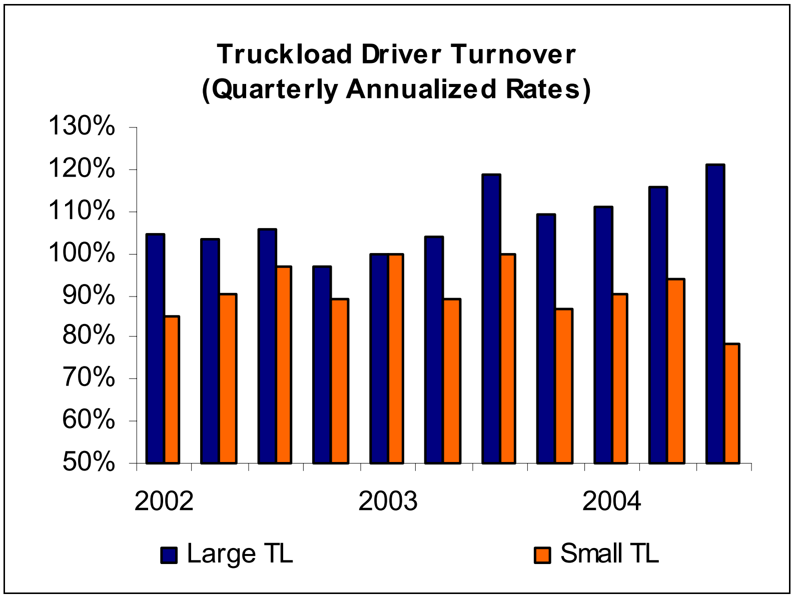
[7] U.S. Freight Transportation Forecast to 2015, 2004

[8] Standard Trucking & Transportation Statistics, ATA Economics & Statistics Group, 2004

Stereotypically, the truckload sector encompasses the long-haul, over-the-road, CB-toting[9] drivers often romanticized in song and movie. In reality, the truckload sector is possibly the most technologically advanced sector of the industry (with the possible exception of small package services such as FedEx and UPS). Truckload carriers were investing in satellite tracking systems in the mid-1980s, shortly after the Department of Defense released the GPS constellation system for civilian applications.

For numerous reasons, the TL sector is under considerable economic pressure, most notably in the area of driver turn-over. Recent statistics[10] indicate that annual driver turn-over exceeds 120 percent for large TL carriers (See Figure 2). Some experts speculate that the problem is due to compensation schema, whereas others believe the root cause stems from long periods of time away from home. Regardless of the cause, the growing economy is putting severe constraints on truckload capacity: many TL carriers were turning away business in late 2004 and early 2005 due to the unavailability of good drivers.

Figure 2. Truckload Driver Turnover



Source: *Trucking Activity Report*, ATA.

---

[9] ATRI-Gartner Study of Technology Applications indicates that 28% of trucks still utilize CB radios.
[10] Standard Trucking & Transportation Statistics, ATA Economics & Statistics Group, 2004

1.2.3 Major Sectors: Less-Than-Truckload (LTL) Carriers

The LTL sector typically provides business-to-business service with multiple pick-ups and delivery locations, utilizing various vehicle configurations and regional consolidation centers. The LTL industry is dominated by a number of larger LTL operations such as Yellow Transportation, Roadway Express, FedEx Freight and Overnite Transportation. One of the largest LTL operations in the nation, Consolidated Freightways, was dissolved in a bankruptcy filing several years ago. The LTL sector is also well known, albeit not exclusively, as the unionized arm of the truck driver population.

1.2.4 Major Sectors: Hazardous Materials Shipments

The movement of goods classified as "hazardous materials" transcends all sectors given the ubiquitous nature of US DOT-designated[11] HM shipments, which include everything from gasoline, caustic chemicals, explosives, and nuclear materials, a well as house paint and personal hygiene products. These shipments are moved in every possible operation and vehicle configuration; hence RSPA[12] now estimates that more than 1 million daily HM shipments were moved in 2003.

The HM industry and the management of HM goods is closely managed and/or regulated by multiple agencies including RSPA, FMCSA, TSA and EPA for safety and security purposes. Post 9/11, several major regulatory changes were made or promulgated to increase the security of HM shipments[13]. In addition, HM risk assessments, classified as security-sensitive information, have been conducted as part of several major initiatives. One well-known US DOT-sponsored initiative is the "Hazardous Materials Transport Field Operational Test" (HM FOT) which installed and tested a suite of integrated technologies to enhance the safe and efficient movement of HM goods.

---

[11] Code of Federal Regulations Title 49: Hazardous Materials Regulations & Motor Carrier Safety

[12] The Research and Special Programs Administration or RSPA ceased operations on February 20, 2005 as part of a U.S. Department of Transportation (DOT) reorganization. RSPA programs have moved to one of two new agencies, the Pipeline and Hazardous Materials Safety Administration (PHMSA) which incorporates Pipeline Safety and Hazmat Safety and the Research and Innovative Technology Administration (RITA).

[13] Code of Federal Regulations Title 49: See CFR Modifications 2002 - 2004

1.3 Strategic Operating Issues

There are myriad internal and external issues that continuously impact the safety and productivity of the trucking industry. In most cases, the ultimate impact is financial and given the slim operating margins of the industry – calculated across all sectors in 2004 at 4.09 percent[14], small fluctuations in operating margins can have dramatic, even catastrophic consequences to a company. Consequently major investments, even in ostensibly profitable assets or systems, are not made lightly. For example, equipment or technology investment decisions cannot be made solely on the basis of return-on-investment (ROI). Even with a positive per-unit ROI, carriers must have the total liquidity to purchase the system fleet-wide, the ability to train personnel and maintain equipment, and a holistic understanding of how the new equipment or system will impact legacy systems or processes.

The following strategic issues, in no particular order, are not inclusive of all factors that affect trucking operations, nor do they relate to every sector. But in general, the list highlights strategic issues that impact the livelihood of large groups of carriers, or ones that may have a macro-influence on the composition and design of the industry in general. These issues certainly have an impact on the decisions made by the trucking industry regarding investments in new technologies related to homeland security.

1.3.1 Highway Taxes & User Fees

Clearly, the trucking industry is a significant user of the nation's transportation system. Furthermore, while various government and academic studies debate the balance between the infrastructure impact of large trucks and their requisite financial contribution to maintenance, there is little agreement on axle-weight impacts of automobile vehicle-miles-traveled (VMTs) versus trucks VMTs. Lastly, large trucks pay a considerable portion of total highway user taxes: as a percentage of the total Federal Highway User Trust Fund contributions, trucks contributed 42 percent in 2003[15].

---

[14] Standard Trucking & Transportation Statistics, ATA Economics & Statistics Group, 2004

[15] American Trucking Trends; 2004

Many in the trucking industry believe that the component of transportation financing that has the greatest negative impact on the industry is toll projects and other creative financing tools. The three primary factors that raise concern are:

1) The ability of local toll authorities to raise tolls without major checks and balances. Consequently, carriers often cannot plan for, nor afford, unexpected and sometimes dramatic increases in fees. For example, in the mid-1990s, the Ohio Turnpike unexpectedly raised truck tolls by more than 80 percent;
2) The industry's opposition to double-taxation – state financing of highways is already supported by fuel taxes in addition to new and existing toll fees; and
3) The balkanization of the transportation system that may result from decentralized development of toll facilities throughout the country.

With the expected signing of the new six-year transportation bill in 2005, it is unclear how many new federally sanctioned creative financing initiatives may arise. The result is a trucking industry that is focused first on managing existing business expenses rather than focusing on new security programs and technologies.
SECURITY IMPLICATION: Unexpected financial impacts associated with alternative financing schemas will exacerbate the trucking industry's tight margins. The result is an inability to plan for new transportation costs and an increased unwillingness, or inability, to incorporate new security costs.

1.3.2 Driver Shortages

The driver shortage issue may reach crisis proportions in 2005-2006 when several major factors reach critical mass: an expanding economy, an entire generation of baby-boomer drivers on the verge of retirement, changes in driver-related safety and operating regulations, and increasing concern over the real or perceived level of driver compensation. As indicated previously, in 2004 the driver turn-over rate for large TL carriers exceeded 120 percent annually. In other sectors, it is less severe, but warrants attention. There is also a remaining question as to how much of the issue is true shortage versus a situation of drivers "churning" through employers.

SECURITY IMPLICATION: There is a basic assumption that truck drivers are the first or last node in trucking security management. However, when annual driver turnover rates are excessive, carriers must increase requisite training and compliance costs to ensure adequate driver training. The result is a labor-intensive and often unbudgeted expense for carriers; some estimates of standard (non-security-related) training costs are $4,000 to $6,000 per driver[16]. Qualitative research data[17] indicates that technology training and system maintenance expenses are often undocumented by vendors and suppliers. While some national programs such as the ATA Highway Watch program provide free or low-cost security training, high turnover rates will make it challenging to provide immediate training for all new drivers, particularly in the over-the-road (OTR) truckload sector.

1.3.3 Insurance Costs

As previously stated, the convergence of an economic recession and terrorist attacks in the early 2000s put considerable economic stress on the trucking industry. When unexpected insurance cost increases arose between 2001 and 2003, the industry was shaken financially. It was well documented that "safe" carriers (those with satisfactory FMCSA safety ratings) experienced premium increases ranging from 30-80 percent (See Figure 3).

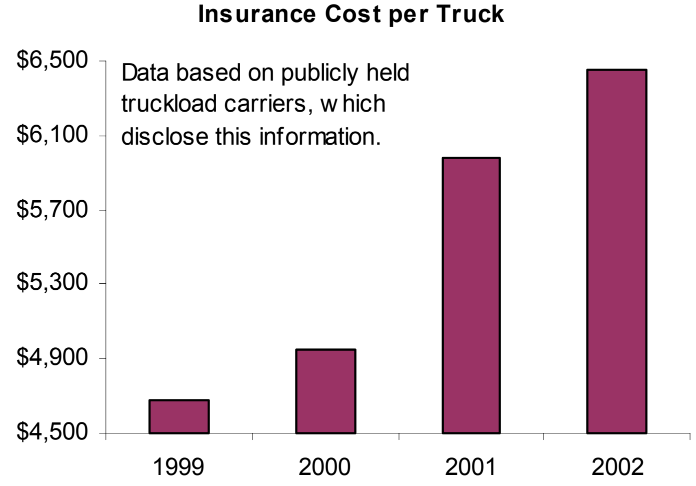
By 2003-2004, the rates had stabilized allowing carriers to budget for the higher rates. Nevertheless, insurance costs remain an area of great concern for most carriers.

---

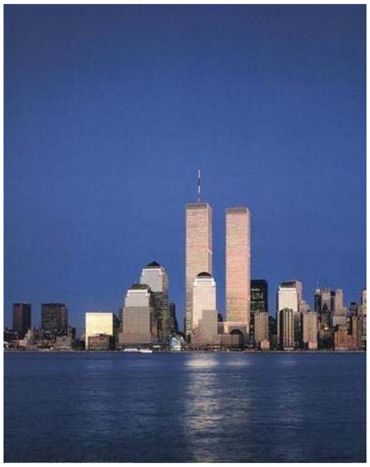
[16] Costs identified by large TL carriers during ATRI Driver Simulator Focus Group; February, 2005

[17] FMCSA-ATRI Safety Technologies Survey of 125 carriers; 2004

Figure 3. Insurance Pricing Survey Results



ATA Insurance Industry Survey, 2003

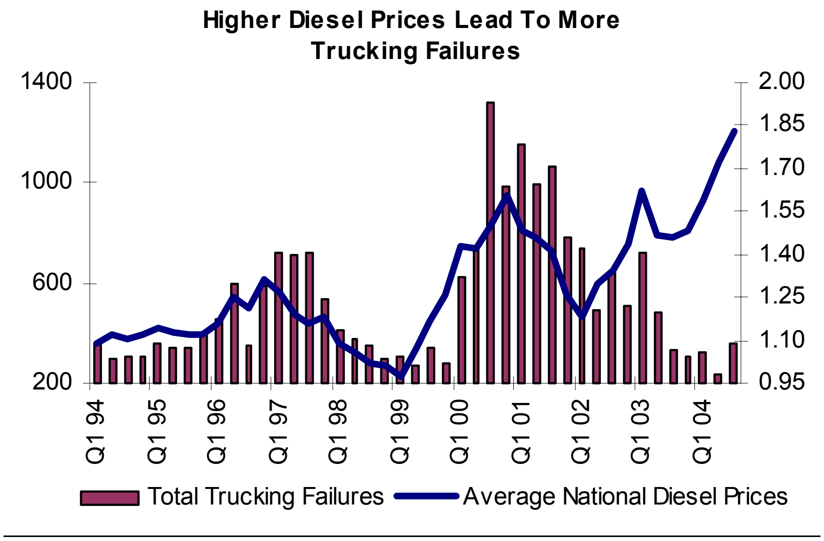


SECURITY IMPLICATION: Historically insurance costs have been closely associated with direct liability costs relating to accidents and other safety metrics. The premium rate increases that began in 2002 – occasionally described as market corrections – exceeded most carrier expectations, and presented a new degree of unpredictability in cost management. The recognition that any future terrorist attacks may dramatically increase existing rates above and beyond market corrections creates a fear of marketplace volatility. Another pressing question is whether security technology investments could result in lower premiums. Existing actuarial/risk assessment models typically require 3-5 years of field data, making any immediate insurance premium discount unlikely.

1.3.4 Fuel Price Volatility

It is no surprise that fuel prices have skyrocketed over the last 2-3 years, and that the trucking industry is a large consumer of both gasoline and diesel fuel. More specifically, the fuel increases have been recently calculated by the American Trucking Associations as costing the trucking industry at least $14 billion *more* in 2004 than it paid in 2003. By October 2004 trucking companies were consistently paying more than $2.00 per gallon. In relation to vehicles that attain five to eight MPG, the math is not promising. When fuel price increases are juxtaposed with business closure data, it is apparent that even small fuel increases can result in financial collapse (see Figure 4).

Figure 4. Business Closures & Fuel Price Increases



Sources: A.G. Edwards & ATA

The change in the price-failure relationship in late 2004 is likely attributed to: strong economic growth, new fuel surcharges in carrier contracts, and some reductions in carrier capacity due to previous failures and consolidations.

SECURITY IMPLICATION: Increasing fuel prices has the same two-fold effect on carriers as other unpredictable cost factors: it reduces total net revenue that might be used for other programs such as security, and it creates an air of cautiousness relating to new investments.

1.3.5 Hours-Of-Service

It does not seem likely that the new federally designated hours-of-service (HOS) regulations will have any direct impact on security programs and policies; however it is clear that the myriad changes relating to the new HOS, the related court challenge and stay, the congressional legislation and ongoing research have placed this issue at the forefront of industry concerns. While it is generally accepted that the HOS issues will be resolved by fall of 2005, the trucking industry will spend considerable time analyzing the safety and productivity impacts of the HOS. Furthermore, the national discourse involving the mandatory use of onboard recorders (OBRs) – both event recorders and electronic logbooks – will follow closely on the final HOS regulation.

SECURITY IMPLICATION: The potential long-term safety and productivity implications of revisions to the 60-year-old hours-of-service regulation makes this a prominent issue for the trucking industry. The related discussion regarding mandatory use of OBRs will continue to capture the policy and regulatory attention for several more years. The result is less attention applied toward proactive security initiatives.

1.3.6 Technology Utilization Issues

With technology utilization being the thrust of this report's focus, it warrants a large, detailed chapter (See Chapter 2). However, there are several issues relating to technology utilization that deserve some mention.

The first is the relationship between technology and information. The U.S. has become a highly litigious culture, and vast resources are expended to both file and defend individual and class action civil cases, reduce legal liabilities, lessen potential negligence, and lobby for and against state and federal tort and liability reform.

In all cases, the single most powerful evidence sought by legal practitioners and stakeholders is information. Unfortunately the primary and secondary output of all technology systems is information and rarely is information not stored or archived in some fashion or format by the simplest of technology devices. Hence, technology investment is often tempered by the potential dangers associated with possessing information that may create or document liability. Based on legal precedents associated with technology utilization and the requisite data retention[18], it is surprising how often technology vendors fail to build adequate data privacy protections into their systems.

---

[18] American Transportation Research Institute & Federal Highway Administration, Developing Tools to Enhance Data Privacy and Sharing, 2005

The data privacy concerns are particularly apparent at the state level where tort law – often described as Joint & Several Liability law – can hold defendants liable for up to 100 percent of financial damages defendants incur in instances where they're found to have as little as 20 percent responsibility in a case.

SECURITY IMPLICATION: Technologies that create or raise legal liabilities will not likely be received with favor by industries that have sensitivities to civil lawsuits. The primary alternatives are revisions to tort law or dramatic data protocol and technical changes to technology systems.

1.3.7 Congestion & Capacity

The US Department of Transportation has designated traffic congestion as one of the biggest challenges facing the U.S. transportation system.[19]. This is due directly to the dramatic increases in automobile ownership, vehicle-miles traveled (VMTs), and stagnant growth in new transportation capacity. New truck sales are also increasing (See Figure 5).

For the trucking industry, congestion delays are extremely costly; estimates for hourly CVO costs associated with traffic congestion range from $28.00 to $78.00 for every hour a single truck is delayed. The trucking industry has generally been able to accommodate the impact of congestion through two primary means:

1) incorporating expected (aka "recurrent") delays into travel times and routing and dispatching systems; and
2) Utilizing alternative routing.

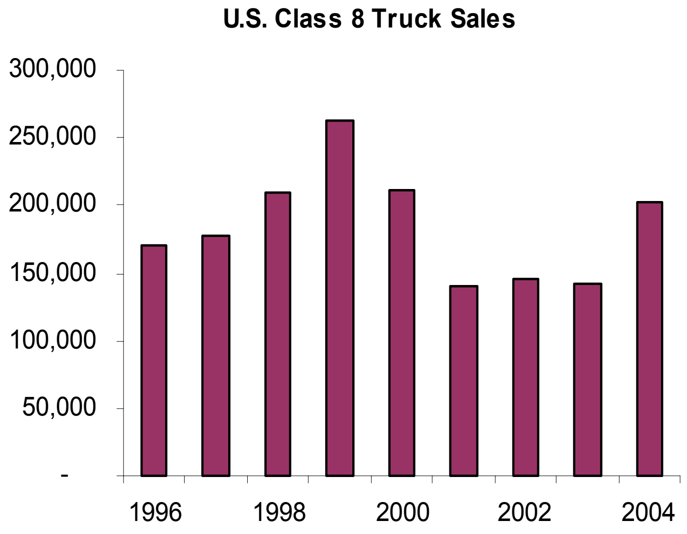
A growing trucking industry is a direct consequence of a growing economy. Increases in truck sales and truck VMTs reflects increased demand for freight services and increased cargo volumes. As one indicator of truck growth, new truck sales in the first quarter of 2005 were more than 50 percent higher than 2004 sales – which were approximately 25 percent higher than the previous year's (see Figure 5).

---

[19] http://www.fhwa.dot.gov/congestion

SECURITY IMPLICATION: The congestion consequence is that truck travel continues to expand beyond the classic interstate transportation system, resulting in increased truck trips on infrastructure that may not have originally been designed for larger, heavier trucks. Aside from safety and pavement wear issues, there may be new security concerns that congestion may push trucks closer to critical infrastructures and population centers.

Figure 5. New Truck Sales



Sources: Ward's Communications & ATA

1.3.8 Shipper-Carrier Relationships

It often surprises industry outsiders to learn that many operating characteristics of the trucking industry are defined by the shipper community. Shippers may dictate the routes and travel times of shipments to support "just-in-time" manufacturing processes; they may require companies to track shipments and calculate estimated delivery times, and they may require specific onboard technology systems to ensure the safe carriage of goods such as munitions or hazmat.

SECURITY IMPLICATION: Many security programs and regulations target trucking companies under the assumption that the trucking companies have the flexibility and control to make certain decisions that may, in reality, be dictated by shippers and/or consignees.

1.3.9 Maintaining a Safe Industry

From a safety management perspective, motor carriers are a leading stakeholder in transportation safety. Recent US DOT statistics show that the trucking industry's fatal accident rate decreased 22 percent over the last ten years while VMTs increased by 35 percent[20]. This dramatic safety improvement literally comes with a large, but necessary cost: over the last ten years the trucking industry has invested in:

- improved driver training;
- onboard safety systems;
- expanded state and federal safety enforcement programs; and
- more sophisticated vehicle components.

SECURITY IMPLICATION: Given the significant safety gains that have accrued over the years, it becomes more challenging – and more expensive – to find the incremental changes that will continue the downward trend of accident rates. Safety enhancements are often known commodities, resulting in documental declines in accidents, improvements in productivity, and reductions in costs such as insurance. Juxtaposed against theoretical terrorist attacks, safety will likely take precedent if/when discrete investment choices are presented.

---

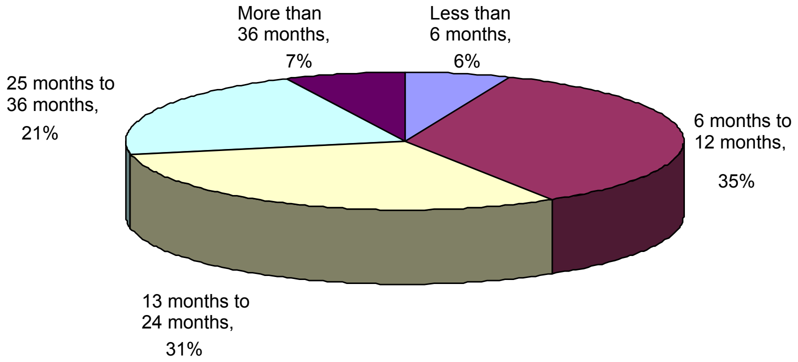
[20] US DOT Highway Statistics, 2003 & Large Truck Crash Facts 2002

CHAPTER 2. TECHNOLOGY IN TRUCKING

2.1 Investment and In-vehicle Technology Applications

From a technology perspective, the trucking industry is driven by immediate or short-term requirements on return-on-investment (ROI) (See Figure 6). A series of government- or industry-sponsored ITS/CVO cost-benefit studies conducted over the last eight years show that ITS investment by carriers must meet several requirements, including short-term ROI, manageable per-unit costs, and ease-of-use (to reduce labor and training costs). The primary objectives of these systems should be quantifiable benefits to operational efficiency and positive impacts on safety. With the events of 9/11, carriers now attempt to meld safety and security objectives into a single grouping. However, while certain safety technologies have proven value, their security benefits are unclear; the alternative is even more challenging: speculative (untested) security systems that propose safety or efficiency benefits. The bottom line is that industry profit margins rarely exceed 4 percent, often relegating security technology investment to some unclear point in the future (See Section 3.2.1 for more detailed information on technology ROIs).

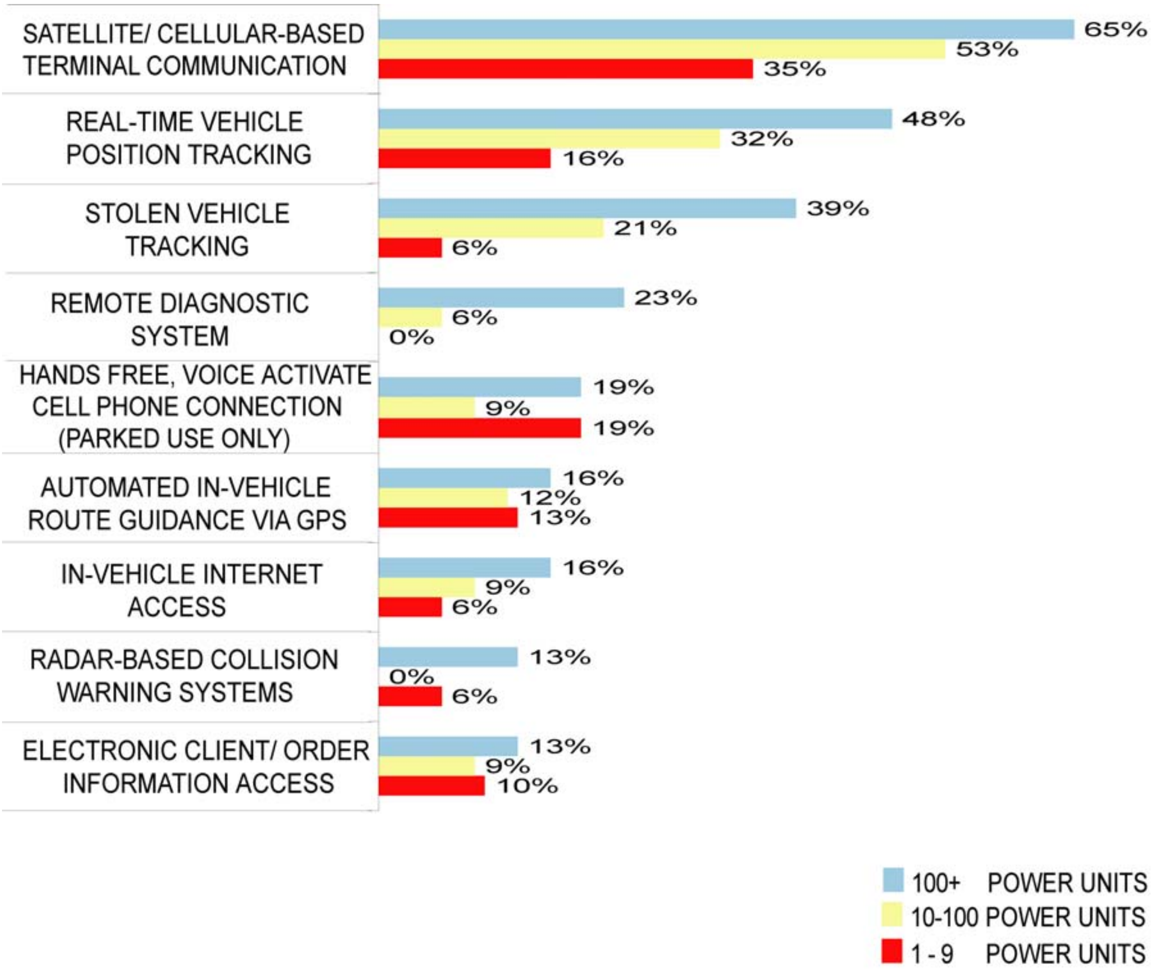
Figure 6. Maximum acceptable payback period for in-vehicle technology investments



From ATRI and GartnerG2, “Trucking Technology Survey”. © 2003.

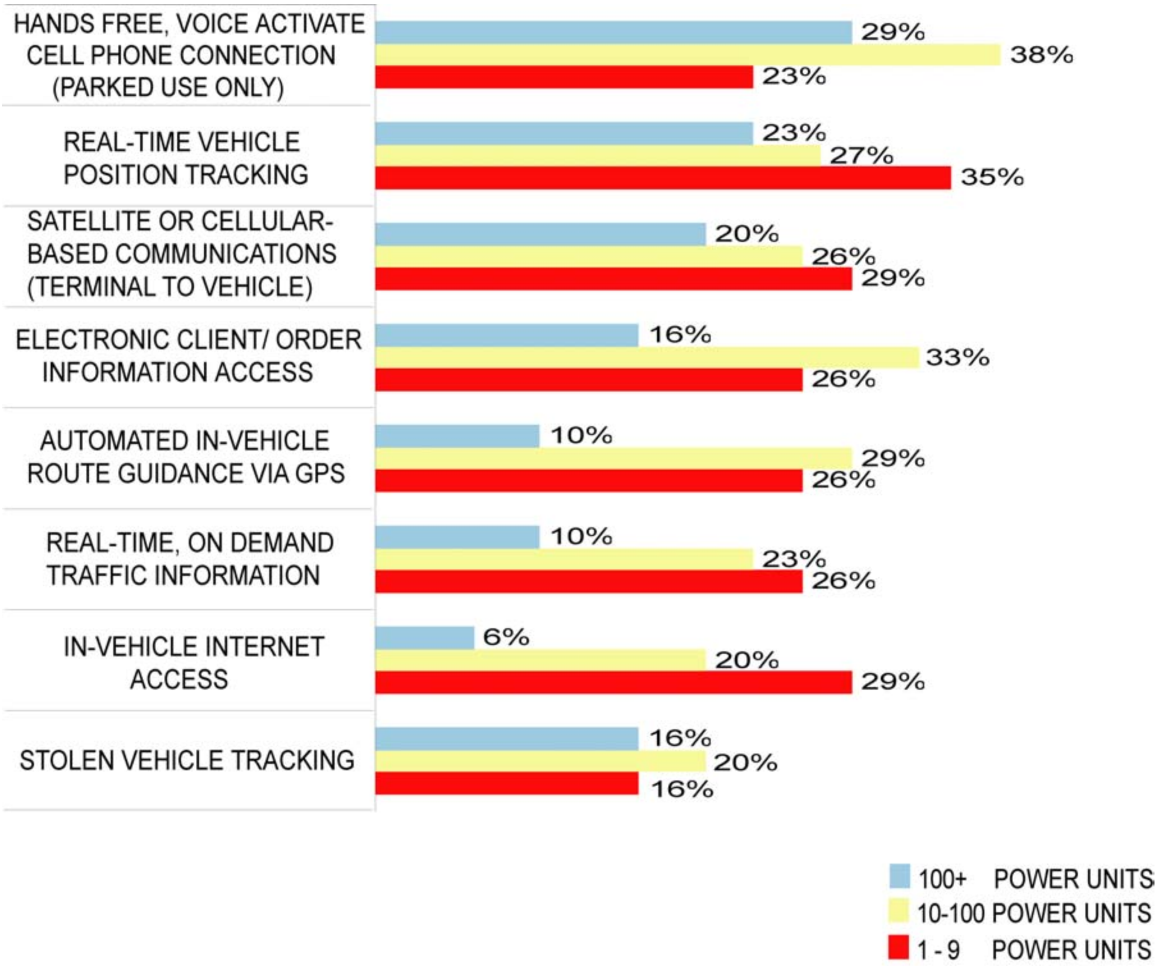
Large-scale ITS systems such as fleet tracking and communications, electronic data management, and advanced safety systems are often viewed as luxuries affordable only to large fleets. Research bears this out; smaller carriers are more risk-averse than larger carriers and often consider technology systems only after they've been fully tested by larger carriers and the production economies-of-scale are in motion (See Figures 7-9).

Figure 7. Most common in-vehicle applications now deployed by fleet size



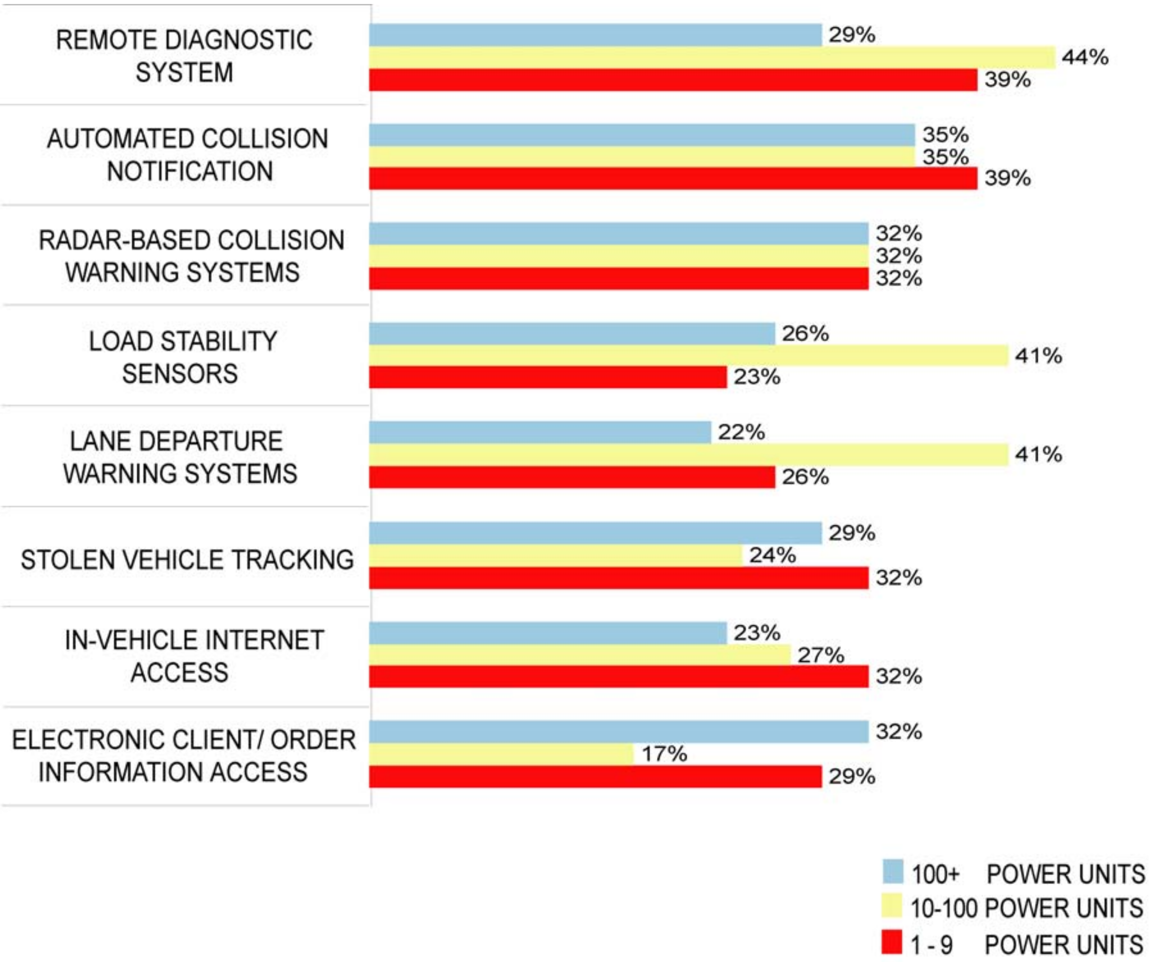
From ATRI and GartnerG2, "Trucking Technology Survey". © 2003.

Figure 8. In-vehicle applications most likely to be deployed into existing fleets



From ATRI and GartnerG2, "Trucking Technology Survey". © 2003.

Figure 9. In-vehicle technologies most likely to be deployed in future vehicles



From ATRI and GartnerG2, “Trucking Technology Survey”. © 2003.

2.2 Technology Investment Objectives

In the trucking industry, technology investments appear to be a reactive response to a specific operating objective. The industry’s small operating margins typically do not allow motor carriers to engage in speculative R&D, hence there are few tech labs and research centers housed within, or funded directly by carriers (industry original equipment manufacturers (OEMs) and vendors are of course an exception to this). Rather, technology investments are made in response to internal or external economic pressures that can most effectively be addressed through the productivity or safety benefits that technology offers. These are often discovered after non-technology solutions are considered and negated (at this point in development, many technology concepts are borrowed from other sectors and applications. For example, most driver simulator systems and experiments can trace their origin to military or aviation programs). In relation to onboard technologies, the objectives are relatively simple, although the technologies themselves are not: most onboard technologies focus on assisting the driver or the vehicle in managing information. With the former, the assistance focuses on reducing accidents and violations; with the latter, it reduces operating costs (less often, it increases revenue). Ultimately, only those technologies that reduce accident impacts or produce positive net marginal gains will be considered or maintained over the long run[21].

The following section – organized by functional design – describes applications and opportunities associated with technologies used in the trucking industry.

2.3 Technology Applications and Utilization

The depth and range of technologies used in the trucking industry is gargantuan in scope, although disparate across sectors and size of firms. The focus of this report is vehicle-based security issues so technology systems relating to "back-room" systems will be omitted. Suffice it to say however that technology issues faced in most areas of business exist within the trucking industry, including:

- The emerging role of the Internet and the impending conflict between EDI-based and XML-based transaction data;
- The policy and regulatory battles over whether technology enables the growth in regulations, or simply automates it;
- The high cost of emerging technologies and the quick product evolution that causes quick obsolescence of existing systems;
- The lack of technology standards and/or interoperability. It is not surprising to discover that some technologies have become nearly obsolete in the time period required to develop national or international standards (data, messages, interface

---

[21] Anecdotally there are myriad examples of motor carriers trial-testing and then uninstalling, in short time periods, technologies that did not deliver the proposed ROIs.

protocols, etc.). In other cases, the issue is not standards development but the willingness of vendors to provide system interoperability.

- Lack of education and awareness of freight issues. Based on the marketed attributes and potential solutions proffered by many technology vendors, there appears to be considerable ignorance of the operational characteristics of, and the internal/external issues faced by, the trucking industry. A comprehensive trucking industry training program, which may not exist today, would certainly be a worthwhile investment for any new technology provider that seeks to penetrate the trucking marketplace.

Focusing on technologies that relate directly to cargo, vehicles or drivers certainly does not dramatically reduce the universe of products or applications. Consequently, this section will discuss categories of technologies. There are numerous resources available that can offer system specifications for those that desire more detail.

2.3.1 Vehicle Communication Devices

By definition, 100 percent of en route communication devices are wireless, and there are numerous system configurations and wireless platforms. For simplicity, this report will categorize wireless communications in the following ways:

- Terrestrial versus satellite
- Driver communication systems versus vehicle positioning (tracking)
- Mobile versus installed units

Satellite Systems can typically be grouped by system attributes focusing on either driver communications or vehicle positioning. This is an important distinction because, while several systems offer both functions, dramatically different satellite systems and onboard processing is used. In general, the strength of GPS and communication satellite systems is the ubiquitous coverage provided by the satellite networks and, until the advent of digital terrestrial systems in the mid-90’s, satellite transmissions had a greater (at least perceived) degree of information security. The cons are few but significant in some instances.

While satellite voice/message communication has become much cheaper over the years, the bandwidth costs associated with large “data packet” transfers over communication satellites is still relatively expensive. Some believe this to be a function of the satellites being primarily owned by private communications companies. The other issue is more potentially problematic from a security perspective. Satellites require a “line-of-sight” position with the transceiver, which means that physical impediments such as buildings, mountains and metal antennae covers can interfere with, or completely eliminate signal reception. The urban canyons, associated with large cities, are the primary concern from a security perspective since these cities not coincidentally possess large concentrations of critical infrastructures and potential attack targets. In response, satellite service providers have begun developing communication parameters that allow carriers to manage satellite signal losses. For instance, carriers could utilize onboard systems that will provide some control over trucks that are no longer in communication with the satellites and/or carrier dispatchers.

For GPS-based technologies, the primary objective is vehicle positioning and tracking. There are also different methods and resolutions for processing GPS signals. It is generally safe to say, at least at the time of this printing, that the more detailed and granular the position information, the more expensive the technology.

An industry survey conducted by the American Trucking Associations one month before 9/11, 2001 found that approximately 42 percent of respondents used some form of satellite communications (GPS and non-GPS). However, among large carriers, this number exceeded 65 percent. Ninety-eight percent of carrier respondents included in this group indicated that their primary objective in using satellite systems was truck tracking. The group’s second most common objective was routing and dispatching (91 percent [22]). It is clear from more recent surveys that the use of wireless communications is increasing in the industry, for both satellite and

---

[22] Survey percentages are duplicative since respondents could check all applicable options

terrestrial systems. Whether this is the result of security concerns or other market-based factors is not clear based on available research.

Prior to 9/11, the major focus of these systems was cargo management; either to ensure that valuable cargos were visible or that essential just-in-time product components reached manufacturing facilities within hours or minutes of their scheduled assembly facilities. Post 9/11, vehicle positioning became vehicle tracking and was described as essential to ensuring that trucks and cargos were not used as weapons. Several government sponsored studies have indicated that the GPS system itself is relatively immune from spoofing and direct attacks. However, the same line-of-sight requirement exists with GPS systems and a loss-of-signal effectively makes the vehicle invisible to a dispatcher or enforcement agency.

Terrestrial communication systems can take several forms including CB radios and short-range radio systems, but this section focuses on cell-based communications. First and foremost it is important to note that most onboard (installed) terrestrial communication systems utilize GPS signals for positioning. It is possible to develop positioning from cell tower triangulation, but it is both complex and somewhat inaccurate. The same pre-9/11 ATA survey shows that more than 61 percent of carriers use some type of (non-CB/non-pager) terrestrial communication system. Of these, 73 percent were hand-held cell phones and the rest were either installed systems or hybrids. Terrestrial systems have grown quickly over the last five years, possibly based on their market position as low-cost alternatives to satellite. Like satellite, terrestrial systems have inherent problems including poor coverage in some sparsely populated areas where trucks must nevertheless still travel, and lack of interoperability across proprietary systems.

The last wireless communication system described here is the hand-held cell phone – which deserves some attention now that improved functionality is becoming commonplace. More and more cell phones now incorporate GPS positioning which makes these devices useful as a mobile (vs. installed) fleet management system or as a combined personnel/vehicle system. Most cell phones now possess some type of WAP-related internet browser, allowing drivers to access e-mail. Again, the shortfalls include coverage, damage and loss. One of the more interesting developments in this grouping is the ability to add bar-code and Radio Frequency Identification (RFID) readers to the phones. A biometric reader attached to a cell phone as a driver validation system has also been tested.

2.3.2 Personnel Management

Today there are few technology-based driver identification tools in the trucking industry, and far fewer that utilize onboard applications. The most common is an electronic driver log-in system used by several onboard communication systems. Several additional onboard driver validation systems have emerged post-9/11 including at least one tested by a truck OEM.

While driver passwords are most common, they will be vulnerable to the same identity theft issues associated with credit card PIN numbers. Biometrics as an identification system can't be lost, stolen or forgotten, but certainly can still be used against the person's will in some scenarios.

2.3.3 Vehicle Management

Vehicle management can and does refer to many different objectives, functions, and technologies. In some instances, vehicle location information itself qualifies; on the other end of the continuum, intelligent control devices are built into the engine and power systems allowing for remote management and control of most major vehicle systems. It is relatively easy for trucking managers to "conduct" engine diagnostic checks from distant locations using wireless connectivity to sensors and onboard diagnostic systems. The US DOT-sponsored "Hazmat Field Operational Test" included a vehicle-control component that had various control parameters and mechanisms, whereby a vehicle "limp mode" could be activated by drivers, remote dispatchers, even the vehicle itself if certain parameters were exceeded or events occurred. In this test, the vehicles were equipped with a vehicle inhibitor device that provided a bypass of the throttle and cruise control circuits, while still allowing braking and power steering functions, thus rendering the tractor to idle mode.

The University of Minnesota has demonstrated the potential of integrating wireless systems with vehicle control on truck tractors, snowplows and buses. For example, their Technobus provides lane assistance to the driver to help steer a nine-foot-wide bus in a ten-foot-wide bus-only shoulder[23]. Steering controls are integrated with high accuracy enhanced digital maps and differential GPS transceivers and provide feedback to the driver visually and haptically (through the steering wheel and/or the seat). These steering systems enable lane departure warning, but can also provide for full steering automation if needed. In a public demonstration at the MnROAD test facility several years back, a system was shown to be capable of automatically steering a truck tractor off the road to a safe spot on the shoulder and bringing it to a complete stop, if the system sensed that the driver was incapacitated[24].

Vehicle Management can also be placed in the hands of the drivers using short-range wireless devices similar to keychain-based car alarm remotes. The objective of these devices is generally to thwart vehicle theft when the driver is within range of certain RF bands. Another viable application would be to foil a vehicle hijacking with the driver present, although that may present new dangers to a driver's personal safety.

The vast majority of vehicle management systems are tractor-based since this configuration provides a power source and driver access and management. However, an interesting asset management device that continues to evolve is the trailer tracking system that may either be wired to the tractor and its related management systems or "untethered", with its own power and management systems and position-location system. The logical thought behind trailer tracking devices, at least from a security perspective, is that the danger of truck-based terrorist attacks comes from the cargo within. If the trailer is not attached to a tractor or is attached to a tractor without a communication system, then it is ostensibly invisible to interested parties. Untethered trailer tracking devices may provide some counter-measure in this regard. The US DOT has conducted several different field tests of untethered trailer tracking systems. Several large fleets within the trucking industry have also invested in these systems, mostly as an attempt to manage thousands of trailers – loaded and unloaded – that otherwise may go missing.

---

[23] L. Alexander et al., "Bus Rapid Transit Technologies: Assisting Drivers Operating Buses on Road Shoulders," Volume 1, Report No. CTS 04-12, 2004.

[24] L. Alexander and M. Donath, "Differential GPS Based Control of Heavy Vehicles," Minnesota Dept. of Transportation, Report No. 2000-05, January 1999. Also L. Alexander and M. Donath, "Differential GPS Based Control of a Heavy Vehicle," Proceedings of the IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems, Tokyo, Japan, pp. 662-7, October, 1999.

2.3.4 Cargo Management Devices

Outside of security, technology is used more and more to manage cargo. It can take the form of more basic package- and pallet-based bar-coding or RFID tags. Bar-coding is extremely common, with "2-D" bar-coding offering slightly improved data security. RFID tags, recently promoted by large retailers as a method for managing inventory and supply chain visibility, may have some security applications in trucking but only when certain requirements are met, including:

- Improved quality control. Recent internal industry testing indicates tags work at different levels of effectiveness;
- Integration with large management systems. By themselves, RFID tags have limited benefits as a data storage system unless more sophisticated components are included.
- RFID standards are developed that would provide some symmetry between the many different tags that may enter the marketplace.

Smart Containers. One of the most notable areas of cargo management attention relates to the development of "smart containers". Four of the factors driving this effort are 1) containerized intermodal traffic is now the fastest growing sector of freight movement, 2) over the last decade the U.S. has experienced massive increases in foreign product imports, 3) there is clear evidence that malefactors have considered and/or tested the use of containers for illicit purposes, and 4) the number of containers that are manually inspected is approximately 5percent, and large increases in this inspection rate would come at considerable expense.

For these reasons, there have been various tests of different container security and tracking systems, particularly between southeast Asian ports and the U.S. west coast ports. These systems have incorporated various sensors and devices for the purposes of detection, deterrence and tracking. For example, GE has tested a small container-based device that creates and monitors a magnetic field. When the field is disturbed, the device documents the event and relays it to wireless readers.

The unfortunate weakness of any reasonably priced container-based security system is that the wired or wireless communication reader often resides at the destination port – which is almost always located in highly dense population centers. It is an unfortunate reality that identifying Trojan horse containers housing WMDs at the destination port will not likely offer much advance interdiction.

There are myriad other cargo management devices, particularly focusing on trailer-installed systems. The sheer number and attributes of these systems cannot be described in the confines of this report, but they include detectors and sensors such as:

- Infra-red
- Motion
- Radiation
- Direct-Contact Switches
- Temperature Sensors
- Density Sensors
- Magnetic Fields

2.4 Safety Technologies

The trucking industry is extremely safety conscious, motivated by both safety stewardship and economic benefits that come from strong safety ratings, few accidents and lower insurance premiums. The most telling indicator of this is the truck-involved fatal accident rate which has fallen nearly 40 percent in the last 10 years. That being said, most carrier-based safety programs have favored driver training over onboard technology investment, partially because of the dearth of field-tested onboard safety systems. However, over the last few years a number of new or improved systems have found interested buyers. As vendors can attest to, moving safety technologies from idea to tested reality is not a small undertaking.

Safety technology development, which requires design, funding, testing and evaluation, occurs along all parts of the industry continuum from truck OEMs and carriers to academic institutions and government. Even consulting and insurance companies are involved at various points in some systems' development. An excellent example of the broad partnerships that are involved in safety technology development is the

US DOT-sponsored Intelligent Vehicle Initiative (IVI) which provided funding and program management to a series of IVI design and deployment teams that included OEMs, carriers, after-market vendors, industry associations and academic institutions. The deployment tests were evaluated by equally robust teams of consultants, research institutes and government experts. The results of the IVI program included field-testing, human factor analyses, and systematic documentation of cost-savings associated with certain types of technologies, or new applications of "commercial off-the-shelf systems (COTS).

Somewhat related to the IVI program, the newest public-private ITS initiative is the large-scale Vehicle-Infrastructure Interface (VII) which attempts to develop intelligent communication and processing between on-road vehicles and the transportation system itself using readers, transponders and myriad embedded sensors throughout the VII system. Much of the initial VII work has focused on automobiles, but in many ways trucks are better equipped to participate given their present utilization of wireless communications. Here again, resolving data privacy and institutional issues is a far greater challenge than developing and installing the technologies.

On the public sector side, FMCSA has taken the lead sponsorship role in managing safety technology development, including the IVI program. Other related initiatives are calculating the safety and financial benefits of different safety technologies and what types of incentives might motivate industry stakeholders to invest in, and use, onboard safety technologies. Three of the technologies that are presently being analyzed include:

- Roll-Stability: Roll stability devices sense the center of gravity of the vehicle and are activated when lateral forces reach a specific threshold (i.e. when the vehicle begins to tip to one side). When alerted, the device automatically reduces speed using brakes and engine adjustments in order to prevent the vehicle from rolling over or departing from its lane on sharp turns.
- Forward Collision Warning Systems: As the name implies, forward collision warning systems use a radar mounted on the front or sides of the vehicle to detect when a truck is too close to the vehicle in front of it, or is in a situation that may cause a collision (i.e. moving at a closing rate relative to the vehicle in front of the truck). When the device detects a threatening situation the driver is given an

in-cab warning sound, indicating that he or she should slow down. This device is especially useful in situations where visibility is limited, such as in fog. The device can also be configured to reduce speed or provide a haptic shake to the steering wheel if the driver fails to act.

- Lane Departure Warning Systems (LDWS): sense and alert the driver audibly when the vehicle is drifting from its lane. This is generally useful in all situations, but especially for fatigued drivers.

CHAPTER 3. CVO SECURITY APPLICATIONS & RESEARCH

3.1 Biometrics, Smart Cards and Cryptography

Biometrics, smart cards and cryptography technologies continue to evolve as does the integrated application of the three to produce the high assurance identity management solutions which are now being considered for use by government and commercial customers.

For the trucking industry, the blending of identity management solutions requires an intimate understanding of the technologies' technical aspects as well as industry user requirements. Given the potentially diverse transportation applications that technologies such as biometrics and smart cards offer, basic security objectives and industry operational impacts must first be determined at both the carrier and industry level. At that point, industry requirements can be selected and assessed against technology attributes. Ultimately, the correct level of functionality must be selected from each technology and integrated in order to produce the best overall solution.

Recent government actions such as the signing of Homeland Security Presidential Directive 12 (HSPD-12) and government sponsored programs like the Transportation Workers Identification Credential (TWIC) have significantly accelerated the process of combining biometric, smart card and cryptographic technologies in search of high assurance identity management systems. No single technology provides all the functionality needed to support the high assurance identity requirements promulgated by HSPD-12 or the TWIC program. HSPD-12 requires, at a minimum, smart cards with contact and contactless chip interfaces, digital left and right index fingerprints, public-key infrastructure certificates (PKI) and a cryptographic algorithm. An integrated combination of biometrics, smart cards and cryptographic technologies will accomplish this goal.

3.1.1 Biometrics

3.1.1 A. Technology Attributes - Biometrics

Biometrics is the measurement of certain physical or behavioral characteristics of an individual used to create a unique identifier which can then be electronically stored, retrieved, and compared for positive identification purposes.

Physical Characteristics	**Behavioral Characteristics**
— Fingerprint	— Keystroke Dynamics
— Hand Geometry	— Dynamic Signature
— Facial Features	— Lip Movement
— Iris	

There are three basic processes associated with biometric: enrollment, verification, and identification. *Enrollment* is the process of collecting and adding a biometric identifier to a database. *Verification* is the process of matching a live scan against a single record, or a one to one match, answering the question “Am I who I claim to be?” *Identification* is the process of matching against all the records in the database, or a one-to-many match answering the question “Who am I?”

The components of a biometric system are a capture device, a processing algorithm, and a repository. The biometric capture device is a sensor which can capture the biometric, e.g. a person’s fingerprint, voice or iris. The biometric algorithms are needed to process the feature extraction and perform the matching functions. The repository is required to provide a protected sector to store the enrolled biometric identifiers for later comparison.

Two terms are commonly used when describing the accuracy of biometric systems: false rejection rate and false acceptance rate. False rejection rate (FRR) measures how often an authorized user, who should be recognized by the system (granted access), is not recognized, i.e., this person was falsely rejected by the system. False acceptance rate

(FAR) measures how often a non-authorized user, who should not be recognized by the system, is falsely recognized (and granted access). In other words, this person was falsely accepted by the system. The values for FRR and FAR will vary based on the type of biometric employed, the specific software employed, and the matching thresholds established by the implementing agency.

3.1.1 B. Biometric Characteristics

Fingerprint

Fingerprint biometrics are the most commonly used biometric with the pattern of the friction ridges on the finger establishing a unique measurable physical characteristic. The fingerprint device captures either an image of the ridge pattern or develops a minutiae-based numeric identity from the print. Software is then used to analyze the pattern or ID number and compare it to an enrolled version of the fingerprint.

Fingerprint identification has a one-hundred-year history in criminal investigations. Because of volume of use and innovations to the technology, fingerprinting is generally the lowest cost option. Enrollment consists of presenting each finger several times. A moment of training is typically required for proper fingerprint placement.

Pros

- Mature and proven technology
- Deployed in a wide range of application and environments with high level of accuracy.
- Enrollment of multiple fingerprints can increase system accuracy.

Cons

- Most devices cannot enroll a small percentage of the population
- Fingerprint can deteriorate over time and with some occupations.
- Associated with the processing of criminals.

Hand Geometry

Hand Geometry devices measure several dimensions of the hand such as the length of fingers between joints and the width of fingers; it effectively establishes uniqueness.

This solution has been widely deployed for access control applications in challenging environmental conditions. On a per-unit basis it is considerably more expensive than fingerprint technology. As with most physical biometric enrollment processes, there is some behavioral component required for the proper presentation of the physical element. With hand geometry a moment of training for proper hand placement improves system performance.

Pros

- Operates in challenging environments.
- Established, reliable core technology that is widely deployed.
- Based on relatively stable characteristics

Cons

- Limited accuracy
- The large form factor and relative cost limits the scope of application.
- Certain populations cannot use the technology because of disabilities.

Facial Recognition/Features

With this technology the system recognizes visible features of the face, conceptually similar to how people recognize each other. Several facial features are measured, such as the distance between the eyes relative to the size of the nose and the distance between the nose and mouth.

This technology can have lower deployment costs if existing camera technologies are used for image capture. Enrollment feels comfortable to most users, similar to posing for a photograph.

Pros

- Can be used by existing image equipment
- Can be used to search static databases such as driver licenses databases
- Can operate without user cooperation

Cons

- Changes in acquisition environment, such as lighting, can reduce matching accuracy.
- Changes in grooming and weight can affect matching accuracy.
- There is a potential for privacy abuse because of the potential use of the technology without the knowledge and cooperation of the user.

Iris

The human iris has a unique pattern for each individual. With appropriate imaging technology, the system can focus on the iris, capture the image and categorize the uniqueness.

Iris scans has been traditionally more expensive than fingerprinting and other technologies. However a long-standing patent expires this year and it is predicted that the resulting competition will result in lower prices and more choices. Most iris scan systems require users to learn how to respond to system feedback in order to place the eye in proper focus.

Pros

- Potential for exceptionally high levels of accuracy.
- Capable of reliable identifications as well as verification.
- Iris patterns are very stable over a lifetime

Cons

- Current technology requires training and attentiveness to use.
- Lighting and corrective lenses can negatively impact user experience.
- Users are reluctant to use eye-based technologies.

Keystroke Dynamics

As a behavioral characteristic, Keystroke Dynamics measures the user's distinctive typing patterns of the use of the keyboard. This biometric has been effectively used in long-term user identification such as controlling Internet access. It can also be combined with passwords.

This is primarily a software solution working with existing hardware, and can be very low cost to deploy. Use and enrollment are not separated; most products continually enhance the reference template as the system is used.

Pros

- Leverages existing hardware.
- Uses common processes.
- Password can be changed as necessary.

Cons

- Retains many flaws inherent to password-based systems.
- Adds only security, not convenience of quick capture of other biometrics.

Dynamic Signature

The old fashioned signature can be automatically captured as a series of separate, distinct strokes. The combination of these strokes creates a unique pattern.

Signature tablet hardware is becoming ubiquitous at the retail point of sale. Most behavioral biometrics such as this requires users to perform consistently throughout their use of the product, which may require practice before enrollment and frequent use.

Pros

- Resistant to imposters.
- Leverages existing processes.
- Long tradition of using signature for authorization.

Cons

- Inconsistent signatures lead to increased error rates.
- Can be affected by behavioral factors (stress, distractions).
- Limited applications.

Voice Print

In contrast to speech recognition where the computer attempts to understand words, voiceprint technology analyzes the tonal characteristics that establish a unique pattern among individuals.

Pros

- Capable of leveraging telephony infrastructure.
- Effectively layers with other processes such as speech recognition and verbal passwords.
- Lacks the negative perceptions associated with other biometrics.

Cons

- Potentially susceptible to recorded playback attack.
- Accuracy can be impacted by the quality of capture devices and background noise.
- Can be affected by illness or stress.

3.1.1 C. Current State of Biometric Technology

The newest ID security developments are the availability of standards-based biometric products and their increased usage in large credentialing and identity management systems. Biometric technologies continue to evolve and mature with real progress being made in the standards area.

Several large, active, high-assurance identity management programs are now utilizing biometrics. The US-VISIT program has generated genuine market acceleration for biometrics. The use of biometrics in passports has played a role in the acceleration of biometric use in the United States as well as in the European Union, Australia, New

Zealand, and Japan – all of whom have committed to or begun the process of developing biometrically enabled passports.

Individual biometric technologies such as iris scanning are seeing renewed interest based on the fact that Iridian's patent control in the marketplace with the original iris recognition concept patent is expiring in the United States in 2005 and in Europe and Japan in 2006.

In addition, the biometric industry is producing more products that conform to industry standards, thus assuring the availability in the marketplace of multiple sources for comparable products. Standards-based products typically foster wider spread utilization of the technology, reduced time to market, reduction of vendor "lock-in" effect, and reduced risk to integrators and end users.

3.1.1 D. Biometric Standards

Since 9/11, security imperatives have created an explosion of activity in the biometrics standards area both in the United States and internationally resulting in an acceleration of the standards process. In the United States the International Committee for Information Technology Standards (INCITS) is the organization responsible for biometrics standards. M1 is the INCITS committee for biometrics and represents the United States in international biometric standards development.

The creation and approval of the data interchange format standards and the continued progress in creating international standards for biometric application program interfaces (BioAPI) and for the Common Biometric Exchange Formats Framework (CBEFF) have been important developments for 2005. Data interchange format standards allow biometric data which has been enrolled using vendor A's technology to be processed using vendor B's technology.

INCITS is now fast-tracking version 1 of the BioAPI specification (ANSI/INCITS 358, available at www.ncits.org) which defines an open system standard application program interface (API) that allows software applications to communicate with a broad range of technologies in a common way. BioAPI provides:

- Simple application interfaces
- Standard access methods to biometric functions, algorithms, and devices
- Robust biometric data management and storage
- Standard methods of managing biometric data and technology
- Support for biometric verification and identification in distributed computing environments

INCITS is also fast-tracking a revised version of the CBEFF. CBEFF describes a set of data elements necessary to support technologies in a common method and format. CBEFF provides the ability to exchange biometric data in nonproprietary format among multiple vendors/applications (www.nist.gov.cbeff).

Internationally, INCITS represents the United States in subcommittee 37 of the Joint Technical Committee 1 JTC1. SC37 was established by JCT1 in June 2002 as a formal international standards forum (www.jtc1.org/sc7/default.asp). Activities in SC37 in general mirror those of M1 with the international approval of BioAPI and the CBEFF standards as the United States highest priority.

3.1.1 E. Biometric Vendors

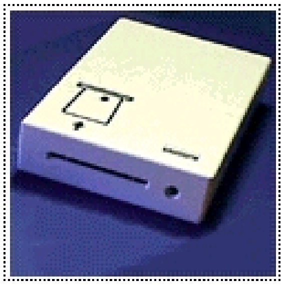
Like most industries, the biometric vendor community has experienced consolidations, failures and new start-ups. An incomplete listing of major biometric suppliers is attached as Appendix C. Since the report authors are not positioned to test or validate each system’s attributes or claims, the information included is derived from each vendor’s marketing material or website.

3.1.2 Smart Cards

3.1.2 A. Smart Cards – An Overview

A smart card is a credit card size plastic card which contains one or more integrated circuits (computer chips) and a contact or contactless communications capability. The computer chips can either provide memory (data storage capabilities) or micro-processing functions which combine memory and data processing capabilities. A microprocessor computer chip is very similar to those found inside all personal computers and, when implanted in a card, manages data in organized file structures using a card operating system.

Beyond data storage and management, smart cards use either a contact or contactless communications interface. Contact smart cards use a smart card reader, requiring physical contact with the reader to communicate. Contactless smart cards have an antenna embedded inside the card which enables reader communication without physical contact. Hybrid smart cards contain two chips in the card, one supporting a contact interface and one supporting a contactless interface. The chips contained on the card are generally not connected to each other. Dual interface smart cards contain a single chip which supports both contact and contactless interface. Dual interface cards provide the functionality of both contact and contactless cards in a single-form factor, with designs that allow the same information to be accessed via contact or contactless readers.



There are three basic components of a smart card system: the card itself, the card operating system, and the card management system. The basic foundation of a smart card system is of course the card itself; these can take a variety of forms, including contact or contactless and variations in the storage or microprocessor on the card. If the smart card does have a microprocessor unit, the card will require a resident software operating system. Finally, the cards themselves will need to be managed using a card management system. The card management system provides for the creation, tracking and revoking of cards to personnel.

3.1.2 B. Current State of Smart Card Technology

The increased availability of dual interface smart cards and the use of match-on-card processing are important new developments. Again, dual interface cards are smart cards which contain one computer chip which has both a contact and contactless communication capability. Match-on-card technology refers to smart cards which have the memory and processing power to not only store biometric data on the cards but also perform biometric one-to-one verifications against a live scan in the card. The match-on-card capability can provide a very secure method of verifying identity as part of a high assurance management system.

Neither the dual interface cards nor standard smart cards that perform match-on-card functionality are widely used in the United States at this time. As is the case with biometrics and cryptography technologies, the cost of sophisticated smart card systems increases based on the level of sophistication and functionality it is asked to provide. For this reason, dual interface cards are not being produced in large enough quantities world wide to achieve economies-of-scale cost reductions. However, some large programs are in the works in other parts of the world such as in Malaysia where by the end of 2005, all citizens over the age of 12 will be carrying a dual interface contact/contactless smart card as their national ID. In the United States we will likely see the increased use of hybrid smart cards until the cost of dual interface cards drops.

Similarly, smart cards which can support biometric match-on-card capabilities require higher levels of memory and processing power than found on the most widely used cards today. The combination of the higher cost associated with the memory and processing power requirements and the availability of testing results will slow the introduction of the match-on-card capability.

3.1.2 C. Smart Card Standards

The creation and signing of Security Presidential Directive 12 (HSPD-12) and its impact on the Smart Card standards efforts has renewed the attention on smart card standards and usage. Specifically, it has motivated the smart card industry to refocus on GSIC 2.1 protocol to better conform to the requirements of HSPD-12.

The Government Smart Card Interoperability Specification (GSC-IS) was issued by National Institute of Standards & Technology (NIST) with assistance from the public and private sector. GSC-IS was built upon existing ISO/IEC standards with the goal of migrating the specification to becoming a formal international standard (www.smartcard.nist.gov/gscis.html).

HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standard (FIPS) to define a common identification credential. "FIPS 201: Personal Identity Verification (PIV) for Federal Employees and Contractors" has been released in draft format and is going through a final approval process (www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf). However, much of this critical activity can be credited to the U.S. military's use of smart cards: Since 2002, more than three million members of the U.S. armed forces and Department of Defense civilian employees have been issued smart cards, providing access to buildings and computer networks, and enabling workers to encrypt and send e-mail.

Smart card standards development efforts are structured similarly to biometrics standards efforts. There is a United States group which is part of the International Committee for Information Technology Standards (INCITS), the organization responsible for identification cards and related devices standards. Like M1, B10 is the INCITS committee responsible for standards regarding identification cards and related devices, and represents the United States in international biometric standards development (www.ncits.org/tc_home/bio.htm).

The International Standards Organization (ISO)/International Electrotechnical Commission (IEC) is the international standards-setting body for smart card technology. Since smart cards have been around longer than biometrics, they have a rather large set of international standards governing all aspects of the technology. ISO/IEC standards 7816, 14443, and 7501 (www.iso.org) are just a few, governing everything from the physical characteristics of the cards, to the communications interfaces and standards for machine-readable travel documents. Unfortunately, ISO/IEC standards include many options and tend to leave some issues unaddressed -- so conformance to ISO/IEC standards alone does not guarantee interoperability.

Internationally INCITS represents the United States in subcommittee 17 Cards and Personal Identification, of the Joint Technical Committee 1 JTC1. Activities in SC17 in general mirror those from B10 with the international approval of the GSC-IS standard as the United States' highest priority.

3.1.2 D. Providers

The following is a list of leading providers of smart cards operating in the United States as of this writing. These vendors offer various levels of smart card technology and services, but at the very least provide the basic personalizing of a card with an embedded microchip.

- Axalto (formerly Schlumberger): headquartered in Austin, TX with a manufacturing plant just outside Baltimore; heavily involved in smart card software as well and has been extremely successful in selling cards to the DOD for CAC cards
- Gemplus: Headquartered in Gemenos, France with US offices in Montgomeryville, PA, where they have a large manufacturing plant. The largest smart card manufacturer by volume in 2004. They provide end-to-end credentialing solutions using components from other manufacturers. They are strongest in banking and telecommunications applications.
- Oberthur: French company with US offices and manufacturing in Louisiana and Pennsylvania. They have a large service bureau (which personalizes cards and creates mailers, etc.) in Chantilly, VA. They are currently selling cards to the DOD for CAC. Oberthur is also involved in other business lines, specifically secure printing.
- G&D (Giesecke & Devrient); Headquartered in Munich with offices in Dulles, VA and Toronto; they have manufacturing facilities in Cleveland and Toronto. They are just entering the government market, but are strong in telecommunications.

3.1.3 Cryptography

3.1.3 A. Cryptography – An Introduction

Cryptography is the technology that provides data security. It involves a method of converting data from a human readable form to a modified, encrypted form, and back again to its original readable form. Cryptography is utilized to ensure data privacy, data integrity (protecting data against manipulation), and authentication (providing the identity of the parties), and non-repudiation (the party did participate in the transaction). The process of converting the unencrypted data is called encryption. The process of converting encrypted data to unencrypted data is called decryption. Digital signing is the validation process that provides data integrity, authentication, and non-repudiation.

In order to convert data, an encryption algorithm and key are needed. If the same key is used for both encryption and decryption, that key is called a secret key and the algorithm is called a symmetric algorithm. If different keys are used for encryption and decryption, the algorithm is called an asymmetric algorithm. When using two different keys, one is a public key, designed to be shared, and one is a private key, which must be protected. These keys are complementary, in that if something is encrypted with the public key, it can only be decrypted with the corresponding private key.

The use of public-key cryptography requires an infrastructure to support its use. PKI or Public-Key Infrastructure provides the capability to easily publish, manage and use public keys. It consists of an operating system and application services, i.e., software to support the creation, management and use of the public keys. Public keys are most often packaged as digital certificates[25]. Digital certifications most often contain the public key and a set of attributes which relate to the holder's identity, what they're allowed to do, and under what conditions the certification is valid.

3.1.3 B. Current Status of Cryptography Technologies

In 2005, the movement away from the Data Encryption Standard (DES) and Triple-DES towards the Advanced Encryption Standard (AES) and other cryptographic systems such as those based on RSA and the elliptic curve will continue. Two developments are evolving: the movement from DES which was an early standard for private key cryptography to AES which defines the next generation of private key algorithms, and the movement from symmetric or private key systems to an asymmetric or private public key combination cryptosystems.

---

[25] Digital certificates are electronic documents that offer secure commerce transactions, identity verification, and trust between distant supply chain partners. The certificate itself is issued by an authorized issuing agency, and provides the bearer with a secure number and means of identifying themselves electronically. This offers many government entities the ability to accept electronic documentation from importers and to verify their identities. The importer benefits through its ability to identify itself and declare cargo efficiently and securely, before arriving at port.

The Data Encryption Standard (DES) was developed during the 1970's by IBM and NBS -- a forerunner to NIST. This algorithm has been the standard since 1977. There is general consensus that DES is no longer strong enough for today's encryption needs. Triple-DES is a method of using DES to provide expanded security. This method can use up to three keys, hence the name triple DES.

Advanced Encryption Standard (AES) specifies a Federal Information Processing Standard- (FIPS) approved cryptographic algorithm that can be used to protect electronic data. AES supports key sizes of 128-bits, 192-bits, and 256-bits, in contrast to the 25-bit keys offered by DES.

As an aside, RSA is a public-key cryptosystem that offers both encryption and digital signatures[26] developed by Rivest, Shamir, and Adleman in 1977. RSA was based on a mathematical algorithm, and patented and licensed in earlier years.

Elliptic curve systems were first proposed in the 1980s based on mathematical algorithms associated with elliptical curves. Elliptic curve cryptosystems have emerged as a promising area in asymmetric cryptography in recent years due to their potential for offering similar security to private public-key systems but with reduced key sizes.

When evaluating cryptographic technology for use in identity assurance management systems, the cost of the system is directly related to the level of security required by the user. It will cost considerably more to produce a highly secure system utilizing high-end cryptographic algorithm technology and a private-public key architecture, especially when the cost of the PKI infrastructure is included, then a less expensive private key solution.

---

[26] A digital signature is an electronic authorization that can legally replace physical signatures used for freight transactions. When filling out paper work on imported cargo, for instance, a shipper can use the digital signature to legally authorize the paperwork he or she has filled out. This is especially useful for members of the supply chain such as freight forwarders, shippers, customs and even banks who fund members of the supply chain. Papers that have standard signatures must be transferred by courier, and thus taking several days for completion. Digital signatures, however, offer the efficiency of having electronic paperwork pass between entities instantly; the speed at which the document moves through the system depends only upon how quickly electronic information is opened, electronically filled out and digitally signed, and transferred to the next party. Digital signatures can be authenticated with far greater accuracy than a standard signature.

3.1.3 C. Cryptographic Standards

The history of cryptographic standards does not quite follow the same format as the biometrics and smart card standards. A United States group which is part of the International Committee for Information Technology Standards (INCITS) called X9 (www.x9.org) has a corresponding group at the International Standards Organization (ISO)/International Electrotechnical Commission (IEC) level SC27, but these organizations are mainly focused on banking security issues.

The National Institute of Standards and Technology (NIST) plays a large role in the use of cryptographic technology in the United States through its development of the Federal Information Processing Standard (FIPS) FIPS-140 standards (www.src.nist.gov/publications/fips/index.html). The FIPS-140 standards are the documents which define the US government-approved cryptographic algorithms and rules for key management required to protect U.S. government electronic data. There are four levels of security from level 1 (lowest) to level 4 (highest) defined in FIPS-140. These levels are intended to cover the wide range of potential applications and environments in which cryptographic technology may be deployed.

FIPS 140 standards are continually being revised as cryptological technology advances along with the ability of people to break cryptological security protection.

3.2 Integrating Biometrics, Smart cards & Cryptography

The use of biometrics, smart cards and cryptographic technologies together can provide many synergies. The following benefits are typically sought and achieved by using an integrated approach:

- ☐ Biometrics use Smart Cards to provide portable/secure template storage.
- ☐ Biometrics use Smart Cards to provide claimed identity.
- ☐ Biometrics use Smart Cards to provide a second authentication factor.
- ☐ Biometrics use Cryptography to secure templates during transmission/storage.
- ☐ Biometrics use Cryptography to digitally sign templates.
- ☐ Biometrics use Cryptography to digitally sign components.
- ☐ Smart Cards use Biometrics to provide access control to card.
- ☐ Smart Cards use Biometrics to unlock data on the card.
- ☐ Smart Cards use Biometrics to verify the cardholder as the card owner.
- ☐ Smart Cards use Cryptography to secure data on the card.
- ☐ Smart Cards use Cryptography to secure smart card reader interface.
- ☐ Smart Cards use Cryptography to mutually authenticate smart card applications.
- ☐ Cryptography uses Biometrics to protect access to private keys and digital certificates.
- ☐ Cryptography uses Biometrics to enhance non-repudiation.
- ☐ Cryptography uses Smart Cards to provide portable/secure key/certification storage.

3.2.1 System Example - Transportation Worker Identification Card

One recent example of integrating biometrics, smart card and cryptological technologies to provide a high-assurance identity management system is the Transportation Worker Identification Card (or Credential; TWIC) Program. The TWIC program utilizes a hybrid smart card, which has both a contact and contactless communications capability using two separate computer chips. The smart card is used to store the biometrics of the individual to whom the card is issued. The data is stored in the newly approved data interchange format standards ANSI 377 – finger pattern, 378 finger minutiae, and 385 face recognition data interchange formats. The card stores the biometric data using cryptological technology to protect the data stored on the card as well as the transmission of that data.

3.2.2 System Example - The Hazmat Field Operational Test

Outside of the TWIC program, biometric, smart card and cryptographic technology integration is moving forward in other security arenas. The following provides a scenario overview of a hazardous material driver identification pilot which was recently conducted by the US DOT. The HM pilot included a high assurance method for the identification and verification of hazardous material drivers by the shipper, the vehicle, dispatcher, and receiver. The technology platform was a biometric smart card with information stored on the card and protected by cryptography.

3.2.2 A. Driver Identification and Verification by Shipper

In order for a driver to pick up a hazardous material load from a shipper, the driver was identified and verified by the shipper prior to receiving the load. This was attained when the driver presented a smart card containing the driver's biometric fingerprint template and having the biometric data verified against a live scan of the driver's fingerprint.

The shipper was equipped with a computer or dedicated biometric verification system containing a smart card reader and fingerprint scanner at the pickup site. Upon successful verification of the driver's live scan biometric, a message was displayed denoting a successful validation.

3.2.2 B. Driver Identification and Verification by the Vehicle

Furthermore, the vehicle was equipped with a biometric verification unit partially designed to satisfy the environmental and usage characteristics required for installation in a long-haul trucking rig. The biometric verification unit consisted of a CPU (central processing unit) which controlled an attached smart card reader and fingerprint scanner, and which performed biometric verification.

In order to operate the truck, the driver was required to place his/her smart card into the slot of the biometric verification system. The system attempted to obtain a live-scan of the user's fingerprint, and then compared this print with the reference template on the smart card. If they match, the biometric verification system checked an approved driver's list. If the driver was on the approved driver's list the system allowed the driver to operate the vehicle.

Drivers who left the vehicle for any reason, were required to remove the smart card. The system sends a message to Change the Driver Status to Inactive.

3.2.2 C. Driver Identification and Verification by the Dispatcher

In this scenario, the dispatcher could issue a message at any point to the driver to log in to the system. This command would be directed to the vehicle via standard wireless communications links. The identification/verification device in the vehicle would then notify the driver of a login request. The driver would insert or re-insert the smart card into the system card reader and place his/her finger on the live scan device. The biometric system would attempt to obtain a live-scan biometric for comparison with the reference template on the smart card. If the two matched, the system would allow the driver to continue operating the vehicle. If they did not match, the system could put the vehicle into a disabled "limp" mode until the driver and/or dispatcher resolved the issue.

3.2.2 D. HM Driver Identification and Verification by the Receiver

Upon arrival at the destination, the driver was required to present his/her smart card to the receiver/consignee. The receiver had a dedicated biometric verification system containing a smart card reader and fingerprint scanner at each facility in the test. Upon successful verification of the driver's live-scan biometric, a message was transmitted denoting a successful validation, thus allowing driver and cargo access and delivery.

3.2.2 E. HM FOT Cost-Benefit Analyses

The HM FOT tested a variety of different technologies and developed cost-benefit analyses for both individual and integrated technologies. The project also differentiated costs and benefits in several ways: by beneficiaries and payers, and by security and efficiency outcomes.

The different groupings of technologies were developed based on the design of the industry sector and the risk sector assessments that were developed as part of a separate security-sensitive information (SSI) Report. The different technology groupings or suites ranged in cost from $800 to $3500 per vehicle.

The project's Independent Evaluator applied a range of different research and statistical methods to calculating costs and benefits. Because the project was based on theoretical security scenarios and attacks, the research evaluation was built fielding testing results, qualitative data, and operational assumptions that were vetted through an expert panel.

In summary, the communications and tracking technologies provided the greatest security and productivity ROIs for almost all sectors of industry. In the LTL environment the communication and security benefits were somewhat lower given the complexity of the LTL operating environment.

Overall, the different technology suites provided security reductions of 17 percent to 32 percent, depending on the configuration and scenario. From an efficiency standpoint, the communications and tracking systems were the only technologies that provided tangible ROIs. However, the FOT itself had limitations that may not have fully documented efficiency benefits for the other technologies. Nevertheless, a major trucking company assisted the evaluators with the ROI on wireless communication systems, and discovered a positive ROI of $1,920 to $5,800 – depending on sector design – per truck per year.

For more information on this project see Battelle (2004) and Science Applications International Corporation (2004) or to view the publicly available documents, please visit: **www.safehazmat.com** .

3.2.3 Section Summary

The selection of biometrics, smart card and cryptographic products continues to evolve. Each technology now offers a range of security solutions. When reviewing the technical capabilities of biometrics, smart cards and cryptography, it quickly becomes apparent that each technology provides a wide range of functionality which can be applied to secure identity management systems. The first challenge however is to select the correct level of operational functionality needed by stakeholders. Just as there is no single best biometric technology, for any specific application there is no single combination of biometric, smart card and cryptography technologies that meets all needs. Only by carefully evaluating the level of security required and utilizing the technology which best meets those requirements can the best solution be produced.

CHAPTER 4. ELECTRONIC CARGO SEALS

4.1 Overview

Electronic cargo seals, also known as e-seals, use a combination of manual seal elements and electronic components to provide cargo containers with several aspects of security and efficiency. E-seals are clearly different from the standard trailer and container seals used by freight carriers today. Often called mechanical seals, the two primary types of seals used in the industry now are indicative seals and barrier seals. While neither type provides certainty that the container won't be violated, they do provide two levels of security:

- ☐ Indicative seals offer a low-cost tool for identifying tampering, either through physical or chemical means.
- ☐ Barrier devices in the form of bolt seals and cable seals provide deterrence in that they offer some protection from container penetration.

While neither is highly secure, both have high levels of usage in industry for two primary reasons: 1) the unit costs are extremely low, typically pennies a piece; and 2) for everyday low-vulnerability operations they have provided adequate protection.

There are two major parts of an electronic cargo seal system: the seal, which transmits data and manually locks a container, and the reader, which is the communication link between incoming or retrieved seal data, and those persons and computer systems that understand, and in some cases react, to the data. The capabilities of these devices often include automatic detection mechanisms in combination with the ability to identify cargo containers (e.g. who is the shipper, what is being shipped, what is the origin and destination of the cargo), reporting on location and tamper status, and collection, storage and dissemination of a variety of other electronic data.

This combination of attributes may offer a barrier to cargo theft, tampering, or sabotage, and could also act as a barrier to the introduction of illegal cargo into shipping containers while en route or at distribution centers. For purposes of national security and efficient movement of freight across borders, this technology proposes potential security benefits along multinational routes. An example of this can be found in a scenario where an e-seal is attached to a cargo container in Nation A, and the container travels on land through Nation B to its final destination in Nation C. Through this process, goods can theoretically move efficiently (avoiding multiple inspections) across several international borders while at the same time ensuring that no items are removed from or introduced to the cargo container before the final destination is reached. Thus many forms of illegal activity, including those with national security consequences, may be avoided. In reality, while e-seals may have some ability to improve efficiency and security in cargo movement in an appropriate application, the quality and extent of these attributes have not been measured or proven in the trucking industry to a large degree.

Most, if not all, manufacturers of electronic cargo seals claim that vulnerabilities associated with their product are minimal. There is evidence, however, that e-seals can be circumvented to allow the introduction or removal of items from a cargo container without detection. For instance, trailers and containers can be penetrated from other non-door points; in this case, additional systems would be needed such as motion detectors or other cargo management or intrusion-detection sensors. Two major areas that convey the challenges and/or vulnerabilities of the current technology have been identified.

First, concerns lie with the lack of standards and interoperability of e-seal products. The International Maritime Organization's (IMO) Maritime Safety Committee found that no universal standards exist for electronic cargo seals. The IMO also concluded that while there are several technologies on the market today, "the ultimate end state for container seals are active electronic seals capable of storing and transmitting sufficient amounts of data for all shipping needs"[27]. This end state will only exist after a series of advances in technology as well as system

---

[27] Maritime Safety Committee, *Prevention and Suppression of Acts of Terrorism Against Shipping: Container Security.* 2002.

cost reductions. Thus, the current state of e-seals may not have broad utility until such standards and functionalities are developed and adhered to by manufacturers and those who purchase the technology.

The Economic and Social Council, part of the United Nations, agrees with this conclusion.[28] They find that, beyond a deficiency in standards for e-seal manufacturers, very little guidance exists for the end user, thus allowing for potential increases in cargo seal vulnerabilities. The end user does not have access to guidelines on purchasing electronic seals, including a guide for best practices for different containers and shipping methods. Secondary research indicates that manufacturers often do not provide sufficient information on the appropriate applications and effectiveness measures for their products.

Second, the Economic and Social Council also states that almost all electronic cargo seals can be bypassed. This is based on the findings of the Los Alamos Vulnerabilities Assessment Team, which was able to defeat 213 types of electronic cargo seals using methods that varied in cost, duration of time, duration of planning and number of participants.[29] The defeated technologies were chosen from an estimated 5,000 different types of e-seals available for use. Johnston also indicates that there are 11 separate categories of attack, including the following which can result in undetected electronic cargo seal bypass:[30]

- Unsealing: E-seals often can simply be opened, and then repaired in a manner that hides evidence or damage to the seal.
- Tampering with Seal Data: It is possible to change electronic reports, interpretations and serial numbers.
- Sabotage: Either an insider or outsider can compromise the process of sealing the container so that it can be circumvented in an undetectable manner at a later time.
- Backdoor: A defect can be placed in the seal prior to its use, thus making later exploitation possible. This can occur during manufacturing, while the product is shipped or stored, or even as the product is being put into use.

---

[28] Economic and Social Council, *Customs Convention on the International Transport of Goods Under Cover of TIR Carnets (TIR Convention 1975): Section - Tamper-Indicating Seals: Practices, Problems, and Standards.* 2003.

[29] Johnston. *Efficacy of Tamper-Indicating Devices.* 2002

[30] Johnston, *Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste.* 2001

- Electronic: Sophisticated malefactors can bypass the seals by manipulating certain sensors, signals or power sources electronically.

4.2 E-Seal Design

There are typically four types of electronic cargo seals: RFID, Infrared Seals (IR), Contact Seals, and Remote Reporting Seals. The distinction between these four is found in the technical and functional means used by the seal and the reader to communicate with each other.

4.2.1 Category One: RFID

Radio Frequency Identification, or RFID, is the most common of the four e-seal categories. The seal itself consists of a manual locking mechanism with an attached RFID transponder. There are two categories of RFID seals: active and passive.

Passive RFID seals are unable to initiate transmissions and are only activated when interrogated by a reader. When communication is initiated by the reader, the seal can send identification and determine its own integrity, along with other similar functions. A "pure passive" tag refers to a seal that does not have an onboard energy source. However, passive RFID seals sometimes carry batteries in order to boost reflective signal strength, aid in communication, and/or provide an energy source so that functions can be performed beyond the range of the readers.

Pure passive RFID tags are relatively simple in design, inexpensive, and often disposable. When an energy source is added to a passive RFID tag, the range in which the seal can be read has the potential to increase to over 30 meters. From a security and productivity standpoint, there are industry issues relating to the limited capabilities and effectiveness of the purely passive seals, however.

Active RFID tags are able to respond to interrogation in the same manner that passive tags are, but they also have the capability of initiating data transmissions. The term 'active RFID' generally implies the use of an onboard power source, which in many cases gives the e-seal the following capabilities:

- Continuous monitoring of seal integrity within certain proximities.
- Capturing and logging time data when the seal recognizes an event or break in integrity.
- Omni-directional communications.
- Longer communication ranges than found in passive RFID e-seals.
- Real-time tampering reports.

Active seals are more expensive than passive seals due to the power source, and the technologies that initiate communications and offer improved communication ranges. RFID readers and the RFID tags themselves can use external booster systems to dramatically enhance the range of communications. In highly sophisticated conceptual scenarios, retailers could track product use within a consumer's home and ship additional goods as needed.

The usefulness of RFID e-seals in real-world applications can be greatly impacted by regulations involving international movement of cargo, and certain operating environments which can impose physical limitations on the power and range of the seal.

4.2.2 Category Two: Infrared Seals (IR)

Infrared seals essentially require line-of-sight communications capabilities (i.e. communications are blocked by any physical barrier between the seal and the reader.) Thus the effectiveness of infrared seals is limited to situations when readers and seals are within close range of each other. As is the case with most e-seals, the lack of infra-red seal standards may be problematic.

4.2.3 Category Three: Contact Seals

Contact seals require a physical link between the reader device and the seal for communications. This link is often a cable that can plug into the seal and retrieve data, including information such as identification and events. It is applied to the container much like a wire bicycle lock. These types of devices are generally not reusable.

4.2.4 Category Four: Remote Reporting Seals

A remote reporting seal uses a communications platform, such as satellite or cellular, to provide a high-level of shipment visibility while en route, and also offers users the ability to generate real-time event reports. Remote reporting seals, which are manually attached to containers or trailers, are relatively more expensive than other seal types but, like most commodities, could decrease in price as production becomes more widespread and product applications increase.[31] A benefit of this type of device is the user's ability to remotely identify problems with the seal in real time. As a GPS and wireless device, this type of seal can be read throughout much of the world.

4.3 Economic Considerations

Since e-seals can be disposable, reusable or permanently installed on a container, each option could have different economic ramifications on the return-on-investment. A disposable seal will generally have a lower purchase price, with a much greater cost per use. The obvious benefit of such a device is operational simplicity for carriers but also implies that the device is not as complex as a reusable seal. Reusable seals generally will have a high purchase price but the expense can be offset by effective management and reuse which can lower the cost per use. Permanent installation implies a longer device lifespan with an associated lower cost per use. As e-seals gain a proven track record, permanent installations of electronic cargo seals will likely grow in usage while the percentage use of disposable and portable reusable devices will fall.

4.4 E-Seal Field Testing

The WSDOT Northwest Trade Corridor study[32] evaluated the use of an electronic cargo seal for its ability to automatically detect and positively identify a sealed container at several points along I-5 of the Northwest Trade Corridor. After much initial system design work, results from the test indicated that a sealed cargo container can reliably be detected after passing a reader site in the designated traffic lane at speeds of up to 45 MPH. It is important to note that reader sites such as those used for this study are placed

---

[31] Stromgren, *Program Sector: Agile Port and Terminal Systems Technologies; Report on Electronic Container Seal Technologies (Task 2).* 2002

[32] Transcore, *Northwest Trade Corridor.* 2001

along specific, known routes. These sites included: two weigh stations along I-5, the gates at freight facilities, and at a border-crossing location.

The study concluded that there is a considerable amount of potential to control the read zone through antenna attenuation for discriminating between lanes at very low speeds. However, the study mentioned that further testing is needed. Two additional research topics that were identified include: confirming that a cargo and container identification information can be incorporated into an e-seal and be read from the e-seal through its base reader, and determining the effectiveness and reliability of tamper detection features and battery life of an activated seal.

The Alameda Corridor Test Report[33] evaluated the performance of electronic cargo seals and readers in a railroad freight environment. The test involved the detection of the sealed cargo containers along with the seal's status as it traveled past the base readers located at strategic points along the rail corridor. The test was conducted using three separate train speeds along the test location. According to the study, each of the first electronic seal tests was successful, i.e. the e-seal reader was able to collect data from the e-seal as they came into close proximity to each other. In subsequent tests, however, one e-seal was not read. While the research team demonstrated that electronic seals can be used in a rail line environment, additional testing was recommended by the report in order to achieve more statistical significance and add verification and refinement to the system design, thus providing a better indicator of strict performance.

As mentioned earlier, a study which tested 213 different electronic seals demonstrated a quick and often effortless ability to defeat e-seal devices.[34] The seals studied include both commercial and government seals, and ranged from inexpensive low-tech seals to highly sophisticated and expensive ones. The results of this study indicated that high-tech seals were not automatically superior to low-tech seals. Reasons for this are said to possibly include the following:

- Physical components of electronic seals leave them susceptible to simple attacks.
- Developers erroneously focus only on high-tech electronic attacks.

---

[33] Transcore, *Alameda Corridor Test Report,* 2002

[34] Johnston. *Efficacy of Tamper-Indicating Devices.* 2002

- Developers lack real-world knowledge of detection issues and/or physical attacks.
- Greater device complexity creates more options for an adversary to attack.
- There exists overconfidence in seal technology.
- High-tech seals usually require more hands-on inspection and handling.

This study emphasized the security and societal opportunities of tamper detection and suggests that there is a need for the following:

- More effective seals (i.e. e-seals that are less vulnerable).
- More use of optimal standards.
- A greater awareness of seal vulnerabilities.
- Better education and training for seal users.

The WSDOT Intermodal Data Linkages ITS Operational Test Evaluation study[35] researched an electronic container seal prototype system that tracks intermodal cargo containers with disposable electronic seals. The test represented a two-and-a-half year effort and was conducted in Washington State and British Columbia, with a supply chain link to Asia. Towards the latter months of the Field Operational Test, the system approached a 100 percent read rate and validated the e-seal operational concept. The evaluation of this test identified a series of technical challenges that would need to be addressed before full system deployment. These are as follows:

- Operating frequencies of the seal requires further examination.
- Compatibility issues associated with the seal and the Commercial Vehicle Information Systems and Networks (CVISN) AVI truck transponder technology.
- Labor-intensive problems related to the multiple screens of the hand-held readers.
- An inadequacy of the battery life of the hand-held units.

Even though security was not the primary focus of this test, the evaluation identified several security-related concerns that should be addressed in future electronic cargo seal discussions and research projects. These concerns included:

- An apparent inability of a seal to broadcast in real-time.

---

[35] SAIC. *WSDOT Intermodal Data Linkages Freight ITS Operational Test Evaluation.* 2002

- If the seal has been compromised, that information can only be transmitted within a certain proximity to a reader.
- The seal is unable to define the contents of its load.
- Frequency standards have not been fully addressed.

The Container Seal Technologies and Processes Phase I Report[36] is an overall assessment of the current state of e-seal technologies and their readiness for wide-scale deployment. The authors indicate that e-seals are relatively mature in certain applications and are based on technologies that have been proven effective in other settings. Even though RF-based e-seals operate under the same basic technology, differences among e-seal manufacturers create different communication frequencies, protocols, reader infrastructure hardware, and tamper detection methods. The report emphasizes the need for standards in the area of electronic seal design and operations. The report also recognizes that any electronically sealed container can be bypassed by simply accessing the container through the walls or the ceiling, and that an electronic seal DOES NOT provide any real-time indication of all types of security breaches. Therefore, while it is designed to indicate tampering through the door which it seals, it could only be described as an incomplete or partial security solution. For this reason, simple low-cost steel bolt seals (many with numeric IDs) continue to represent the vast majority of the container seal market.

A list of available e-seal technology vendors follows in Table 3.

---

[36] SAIC. *Container Seal Technologies and Processes*. 2003

Table 3. Electronic Seals and CSDs – Vendor and Product Table[37]

Manufacturer	E-Seal / CSD Model	Application	Type of RFID Technology
AllSet Tracking/ GE Security	AllSeal	ISO Containers, Trucks	Active
Bulldog	RB-100	ISO Containers, Trucks,	Active
	RB-200	ISO Containers, Trucks	Active
	RB-210	ISO Containers, Trucks	Active
	RB-300	ISO Containers, Trucks	Active
Canberra – Aquila	DataSeal	ISO Containers, Trucks	Active
	VACOSS 5	ISO Containers, Trucks	Active
CGM Security Solutions	Navalock MKIIIA	ISO Containers, Trucks	Contact Passive
	Navalock MKIIB	ISO Containers, Trucks	Contact Passive
Container Security Corp.	Sciguard2000	ISO Containers, Trucks	Active
Crown Agents	I-Seal	Cargo Containers and Goods Vehicles	Infrared Active
E. J. Brooks/ Telematic Wireless	E-Seal	ISO Containers, Trucks	Active
GE Infrastructure Security	CommerceGuard CSD	ISO Containers	Active
Hi-G-Tek	IG-BR-40-916	ISO Containers	Active
	IG-BR-40-433	ISO Containers	Active
	IG-BLT-40-916	ISO Containers	Active
	IG-BLT-40-433	ISO Containers	Active
Microraab		ISO Containers	Passive
NewTrax Technologies	Advanced Container security Device	ISO Containers, Trucks	Wireless Sensor Network
Porter Technologies	Intrusion Detection Device (IDD)	ISO Containers, Trucks	Infrared Active
RFTrax	r^3Sensors	ISO Containers, Trucks	Active
Savi Technology, Inc.	Savi Sentinel	ISO Containers, Trucks	Active
Telematics Wireless	FP100SA	ISO Containers, Trucks	Active
	E-Seal	ISO Containers, Trucks	Active
Unisto - Encrypta	Crypta Data Tag	ISO Containers, Trucks	Active
Universeal	I-Seal	ISO Containers, Trucks	Infrared Passive

---

[37] North River Consulting Group and Homeland Security Research Corp, 2004. Table 12 *2004 Maritime Smart Containers Product Comparison Report*.

CHAPTER 5. SECURITY PROGRAMS & LEGISLATION

There are many security programs that have been proposed and/or initiated since the 9/11 terrorist attacks. While legislative descriptions and federal security programs are separated here for improved understanding by the reader, they are closely inter-related since many programs have been congressionally mandated. The result is some recognized but useful redundancies in the information provided. The range of these programs, all of which have some direct or indirect nexus to the trucking industry, covers everything from the development of security programs; the management of personnel; the tracking of vehicles or cargo – sometimes by specific commodity; or the reporting of security-related information.

5.1 Security Legislation

5.1 A. US PATRIOT Act

(develops a range of trucking security programs including the truck driver CDL hazmat endorsement background check)

5.1 B. The Trade Act of 2002

(advance electronic notification of cargo information)

5.1 C. Maritime Transportation Security Act

(creating strengthening of CTPAT, developing a "Secure System of Transportation"),

5.1 D. Border Security Act

(strengthening border agencies resources, requiring close coordination among them),

5.1 E. Bioterrorism Act

(Food and Drug Administration (FDA) rules on facilities registration handling regulated cargo, import notification and recordkeeping rules)

5.1 F. Safe Explosives Act

(establishing criteria disqualifying drivers from transporting explosives, also used as criteria under HME rule)

5.1 G. Aviation Transportation Security Act

(requiring security plans and security threat assessments of indirect air carriers, among others).

5.1 H. **HR 168:** Goods Movement Act of 2005 that calls for investment to expand the freight transportation gateways in this country, including expanding security considerations, but no mention of any technologies.

5.1 I. **HR242** and **HR 243:** Surface Transportation Research and Development Act of 2005 requests appropriations for increased research into areas of construction materials, methods, and expansion of existing surface transportation infrastructure.

5.1 J. **HR 163:** Secure Domestic Container Partnership Act of 2005 calls for the establishment of an 'empty shipping container sealing pilot program' to ensure that empty shipping containers are made secure in their transshipment after delivery of goods. This may offer utilization of smart card technology, but it is not called for in the legislation.

5.1 K. **HR 153:** Rail and Public Transportation Security Act of 2005 addresses appropriations for improvements in rail and public (buses, etc.) transportation facilities, but does not directly address surface transportation involved with cargo or supply chains.

5.2 United States Department of Agriculture

The USDA has a number of security initiatives underway to ensure the security and integrity of the nation's food supply. Some of these efforts are done in concert, or led by, the Food & Drug Administration. In 2004, ATRI completed a study of food transport security issues and practices. The research results were based on a survey of more than 10,000 agriculture and food transport carriers. The results of the research showed that there are real security concerns (see Figure 10 and Figure 11), but that certain solutions may be low-tech in nature. In addition, carriers ranked compliance and added regulations are being equally problematic from an economic impact perspective.

Figure 10. Ag/Food Transport Security Impact Concerns

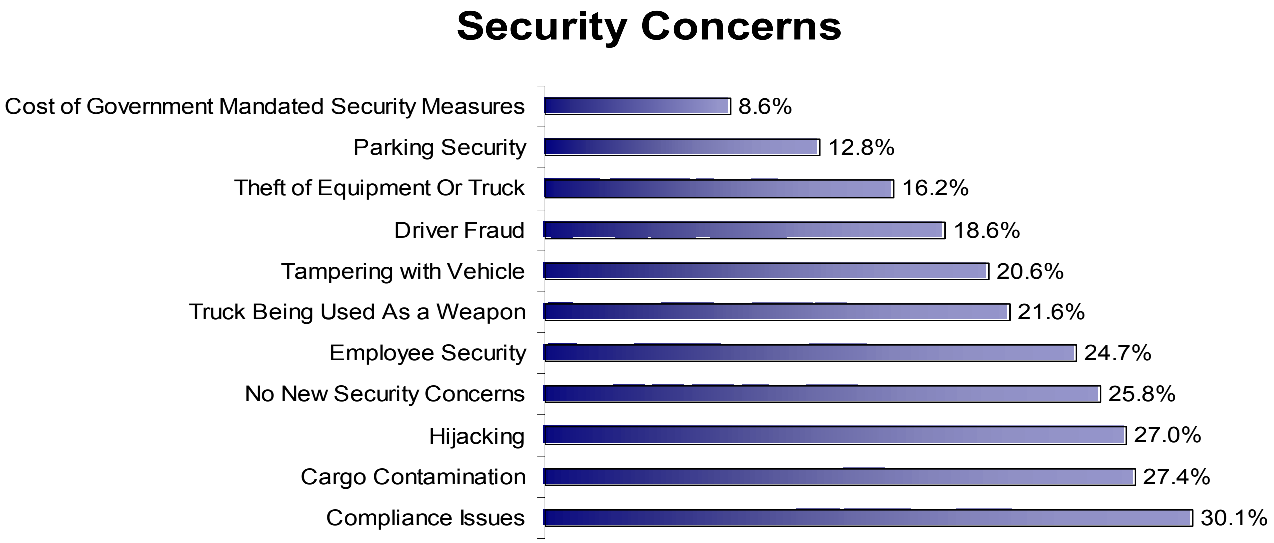
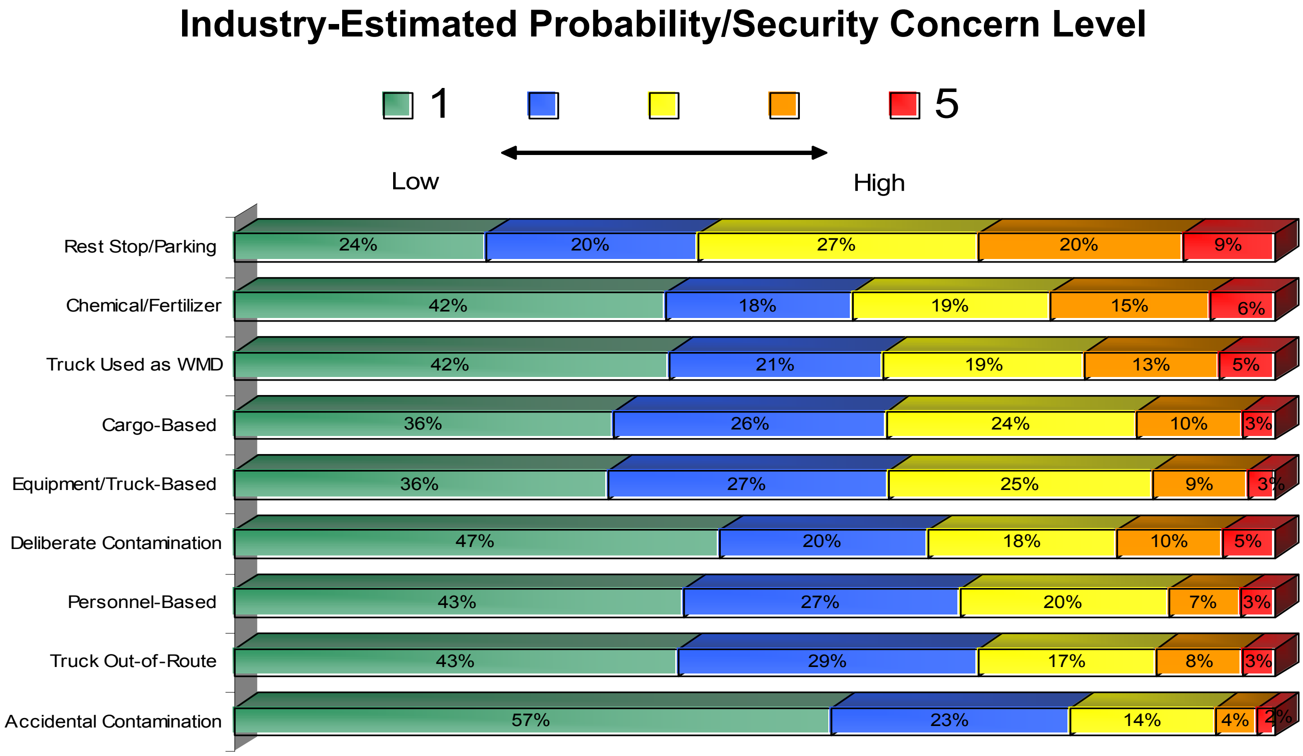


Figure 11. Security-based Concerns



5.3 Department of Homeland Security Programs

5.3.1 Customs Trade Partnership Against Terrorism

Customs Trade Partnership Against Terrorism (C-TPAT) is a voluntary government-private collaborative program designed to enhance security and facilitate legitimate trade. The objective of the program is to prevent and deter terrorists from utilizing the commercial supply chain system for terrorism-related activities. Stakeholders join the C-TPAT program by following a four-step security and verification process - which includes: submitting an agreement to participate in C-TPAT, conducting a security review and submitting a profile, undergoing a validation of the security profile, and completing an annual security review and profile update. Certification of companies in C-TPAT allows the government more time to focus their efforts on high-risk parties and cargoes along the supply chain. Stakeholders benefit from an expedited release of cargo and/or a reduced number of cargo examinations when crossing the border.

5.3.2 Free and Secure Trade

The Free and Secure Trade Program (FAST) is a joint initiative of the United States, Canada, and Mexico that aims to increase the security of the supply chain system by offering expedited clearance through U.S. land ports of entry to carriers and importers enrolled in the C-TPAT or Canada's Partners In Protection (PIP) program. It is the first completely paperless cargo release mechanism implemented by CBP and is achieved through electronic data transmissions and transponder technology. The qualify for FAST lane processing, the following conditions must be met: the shipment must be1) destined for a U.S. C-TPAT importer, 2) have originated from a C-TPAT-certified manufacturer (Mexico-U.S. moves only), 3) consigned to a C-TPAT motor carrier, and 4) hauled by a FAST-approved truck driver. Certification of companies in FAST allows the government more time to focus their efforts on high-risk parties and cargoes along the supply chain. Companies benefit from a reduced number of examinations at the border and, where available, the presence of dedicated FAST lanes to increase the speed and efficiency of transborder shipments.

5.3.3 Container Security Initiative

The Container Security Initiative (CSI) is a reciprocal government-to-government security program implemented on a voluntary basis. The program seeks to target and examine potentially high risk container shipments at ports of participating countries prior to the shipment being loaded onto U.S.-bound vessels. CSI has four core elements: establish security criteria to identify high risk containers, pre-screen containers before they arrive at U.S. ports, use technology to pre-screen high risk containers, and develop and use tamper-evident container technologies. In theory, cargo containers pre-screened at a CSI port should receive expedited clearance upon arrival into the U.S.

5.3.4 The 24-Hour Manifest Rule

This rule is aimed at cargo information from carriers and/or automated NVOCCs and requires that a cargo declaration be submitted to CBP 24 hours in advance of a container being loaded onto a U.S.-bound vessel.

5.3.5 Automated Commercial Environment

The Automated Commercial Environment (ACE) is a CBP Modernization program to automate the systems that support CBP operations for all goods and people crossings at U.S. borders. ACE will be a consolidated release program that will expedite the release process for carriers and shippers that have pre-filed, been approved, and been subject to enforcement prescreening and targeting.

When truck carriers file their FAST Manifest 30 minutes prior to their arrival at the border, the manifest will be sent to ACE along with FAST selectivity information. Once the truck reaches the border, the ACE system will display all the relevant information on the primary booth portal screen. It is then up to the discretion of the primary Customs officer to decide whether or not to release the trip or refer the truck for further inspection. ACE has been described as the system that will support border security programs like C-TPAT and CSI.

5.3.6 Carrier Initiative Program

The Carrier Initiative Program (CIP) is a training program by the CBP in cooperation with carrier companies to prevent commercial conveyances from being utilized to smuggle narcotics. Carriers voluntarily sign agreements with CBP and agree to take every precaution in order to secure their facilities and conveyances. The objectives of this program are to; promote a shared sense of responsibility of stopping the flow of illicit drugs, prevent smugglers from using commercial carriers to smuggle drugs, and to promote a heightened sense of awareness of the security concerns associated with the threat of drug smuggling.

5.3.7 Transportation Worker Identification Card/Credential

As previously mentioned, the Transportation Worker Identification Credential (TWIC) is a government initiative to improve security by establishing a system-wide common credential that could be used across all transportation modes for use by transportation workers to allow access to secure areas of the national transportation system. The card is being developed to remedy various threats and vulnerabilities currently present in the transportation system.

The program ostensibly will utilize one or two biometric identifiers – expected to be fingerprints and iris scans – on a dual-use smart card for both contact and contactless ("proximity cards") applications. The smart cards are likely to include 32K to 64K in chip capacity.

The TWIC Program completed the Technology Evaluation Phase, which was an evaluation of access control technologies at regional pilot sites in the Philadelphia/ Delaware River and Los Angeles/Long Beach areas.

The successful completion of this phase involved various transportation modes on the East and West Coasts including ports, airports, trucking, rail, and pipeline facilities. The participants consisted of a broad array of transportation workers. In each area, TWIC Program personnel participated in region-wide stakeholder working groups to identify and resolve issues, and refine requirements, processes and procedures. Within the next three months, TSA plans to finalize the roll-out of the prototype to 34 other sites within six other states enrolling 200,000 users. The data that is being collected from the rollout of the prototype includes:

- Access Control Logs
    - Entry/Verify Fails
- Voluntary back-ground checks

According to the TSA timeline, the preliminary final report of the prototype phase is due by the end of May 2005.

5.4 U.S. Department of Transportation

5.4.1 Cargo Handling Cooperative Program

The Cargo Handling Cooperative Program (CHCP) is a public-private partnership sponsored by the Maritime Administration. The mission of the program is to actively pursue innovative cargo handling developments that will increase productivity and improve customer service.

5.4.2 Operation Safe Commerce

Operation Safe Commerce (OSC) is a program launched by the DOT and Customs to fund business initiatives that seek to enhance container cargo security while in transit throughout the international transportation system. The objective of the program is to test new security techniques that may greatly enhance the security of container shipments and ultimately recommend the most successful techniques for full system-wide implementation.

5.4.3 Electronic Supply Chain Manifest Initiative Field Test

Electronic Supply Chain Manifest (ESCM) was a cooperative effort between the American Transportation Research Institute; the Federal Aviation Administration; the U.S. DOT Office of Intermodalism; the Federal Highway Administration; the State of Illinois; the Chicago Department of Aviation; the New York-New Jersey Port Authority; and select vendors of advanced security technology systems. The ESCM operational test designed, deployed and tested a unique suite of cutting edge technologies to enhance security and operational efficiencies throughout the air cargo supply chain.

5.4.4 Universal Electronic Freight Manifest Initiative

The Universal Electronic Freight Manifest (EFM) initiative is a public-private partnership sponsored by the U.S. Department of Transportation designed to improve the operational efficiency, productivity, and security of the transportation system through the use of a common electronic freight manifest and message portal that enables access to shipment information to all supply chain partners in real time.

5.4.5 National Hazmat Tracking & Security Test

The Hazardous Materials Safety and Security Technology Field Operational Test is a project funded by the U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office and the Federal Motor Carrier Safety Administration. The project tested new combinations, or suites, of commercial off-the-shelf technology on vehicles transporting hazardous materials by highway. The goal of the project was to demonstrate the effectiveness of these technologies to enhance both safety and security with the goal of speeding up deployment within the industry. See Section 3 for additional information on this Hazmat Field Operational Test.

5.4.5 A. HazMat Transportation Security Regulations

Since Hazardous Materials Transportation receives prominent security attention from security agencies and stakeholders, the following HM-related policy and technical staff have been identified as being significant and are being further separated and documented for review.

- *Written Security Plans* – Motor carriers transporting hazardous materials have developed and implemented written security plans. These plans are required to address the security risks related to the transportation of hazardous materials. In developing these plans, motor carriers have conducted risk assessments on their operations and have developed security measures to address personnel security, facility security, and en route security. *See* 57 *Federal Register* 14510 (March 25, 2003) *codified at* 49 CFR §§ 49 CFR 172.800 *et seq*.
- *Security Awareness Training* – Motor carriers transporting hazardous materials have provided security awareness training to their hazmat employees. Pursuant to

regulation, this training must provide employees with an awareness of security risks associated with hazmat transportation and methods designed to enhance transportation security. The regulation also requires motor carriers to train their employees on how to recognize and respond to possible security threats. *See* 57 *Federal Register* 14510 (March 25, 2003) *codified at* 49 CFR § 172.704(a)(4).

- *In-Depth Security Training* – Motor carriers that are required to have a written security plan have provided their hazmat employees with in-depth security training on the security plan and its implementation. Pursuant to regulation, this training must include company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure. *See* 57 *Federal Register* 14510 (March 25, 2003) *codified at*. 49 CFR § 172.704(a)(5).
- *Background Checks* – Pursuant to the USA PATRIOT ACT, TSA has completed name-based background checks of all individuals that possess a hazardous materials endorsement to their commercial driver's licenses. Fingerprint-based background checks for hazmat-endorsed drivers are now being phased in. *See* 69 *Federal Register* 68720 (November 24, 2004) *codified at*. 49 CFR Part 1572.

5.4.5 B. HazMat Transportation Security Guidance

- RSPA[38] issued advisory guidance that outlines measures that enhance the security of hazardous materials while in transportation. This document covers personnel, facility and en route security issues. See 67 Federal Register 6963 (February 14, 2002).
- DOT FMCSA published a guidance document entitled *Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials*. *See* http://www.fmcsa.dot.gov/safetyprogs/hm/Security_Plan_Guide.htm
- Several Industry Association have developed security guidance documents applicable to motor carriers that transport hazardous materials: Some of these include: American Trucking Associations, American Chemistry Council, and National Tank Truck Carriers.

---

[38] The Research and Special Programs Administration or RSPA ceased operations on February 20, 2005 as part of a U.S. Department of Transportation (DOT) reorganization. RSPA programs have moved to one of two new agencies, the Pipeline and Hazardous Materials Safety Administration (PHMSA) which incorporates Pipeline Safety and Hazmat Safety and the Research and Innovative Technology Administration (RITA).

- Numerous consulting companies have produced guidance on hazmat transportation security, including Batelle, ICF, Total Security.US.

5.4.5 C. Other HazMat Transportation Security Initiatives:

Security Sensitivity Visits (SSVs) – FMCSA has conducted onsite visits to motor carriers that transport hazardous materials. The SSVs are intended to increase the level of awareness of hazardous materials carriers to terrorist threats, identify potential weaknesses in carrier security programs, and report potentially serious security issues to the appropriate authorities. FMCSA has completed more than 40,000 SSVs and has issued a report to Congress on the success of this program. *See* http://www.fmcsa.dot.gov/aboutus/testimonies/SSV_Report_To_Congress.pdf

Highway Watch – ATA has significantly expanded its Highway Watch program. The program teaches highway professionals how to identify suspicious activities that may be a predicate to a terrorist attack and properly report these observations to a fully functional operations center. Additional information is available at: http://www.highwaywatch.com/

5.5 Canada Border Services Agency

Partners in Protection (PIP) is a Canadian program similar to the U.S. C-TPAT program. Through an agreement called a Memorandum of Understanding, the Canada Border Services Agency's PIP program is designed to promote the cooperation of the private sector in efforts to enhance border security. The benefits of this program include the increased likelihood of expedited clearance of transborder shipments, eligibility for FAST processing, and improved supply chain security.

5.6 Industry-Oriented

5.6.1 Highway Watch

The Highway Watch program is administered by the American Trucking Associations under a cooperative agreement with the U.S. Department of Homeland Security. It is a safety and security program designed to utilize the resources of a diverse set of workers from the transportation community and enlist their efforts to help protect the nation's critical infrastructure and the transportation of goods, services, and people. Training for Highway Watch provides participants with the knowledge and the tools necessary to identify and prevent terrorists from using large vehicles or hazardous cargoes as weapons.

5.6.2 Highway Information Sharing & Analysis Center

The American Trucking Associations (ATA) staffs and operates the Highway Information Sharing and Analysis Center (Highway ISAC) the HWW Call Center, and the HWW Emergency Planning and Educations Center for the benefit of all members of the highway sector, in close cooperation with the Department of Homeland Security, as well as other federal departments and agencies. Coordination and support of the activities of these three centers is provided by the Highway Operations Center. The Highway ISAC serves as the analytical and communications focal point for two-way communication and analysis of threat information and related data among highway sector operating entities, government agencies and the law enforcement and emergency response communities. The Highway ISAC is located at the Transportation Security Operations Center (TSOC) in Herndon, VA. The Highway ISAC is also supported by the Highway Watch® Call Center.

REFERENCES

Adams, Carlisle and Steve Lloyd. Understanding Public-Key Infrastructure; New Riders Press, 1999.

A.G. Edwards & Sons. St. Louis, Mo.

ATRI and GartnerG2, "Trucking Technology Survey," 2003.

L. Alexander and M. Donath, "Differential GPS Based Control of a Heavy Vehicle," Proceedings of the IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems, Tokyo, Japan, pp. 662-7, October, 1999.

L. Alexander and M. Donath, "Differential GPS Based Control of Heavy Vehicles" Final Report, Minnesota Dept. of Transportation, Report No. 2000-05, January 1999. http://www.lrrb.gen.mn.us/PDF/200005.pdf

L. Alexander, P. Cheng, M. Donath, A. Gorjestani, B. Newstrom, C. Shankwitz, and W. Trach, Jr., "Bus Rapid Transit Technologies: Assisting Drivers Operating Buses on Road Shoulders," Volume 1, Report No. CTS 04-12, 2004 http://www.its.umn.edu/research/completeyears.html

American Transportation Research Institute. "Improving Cargo Security and Efficiency Through the Development and Testing of an Electronic Supply Chain Manifest." Prepared for the Federal Aviation Administration and the Federal Highway Administration, Alexandria, VA., December 2002

American Trucking Associations. http://www.highwaywatch.com/ Accessed December 2004.

American Trucking Associations, "U.S. Freight Transportation Forecast to 2015," 2004.

American Trucking Associations, "American Trucking Trends 2003," Alexandria, VA, 2003.

American Trucking Associations, "Trucking Activity Report," Alexandria, VA, 2004.

Battelle, in association with the American Transportation Research Institute, Qualcomm, Commercial Vehicle Safety Alliance and the Spill Center. Hazardous Materials Safety and Security Operational Test Final Report for Contract DTMC75-01-D-00003, Task Order 5. Submitted to the Federal Motor Carrier Safety Administration, August 31, 2004.

Biometrics Consortium
http://www.biometrics.org

Canada Border Services Agency.
http://www.cbsaasfc.gc.ca/general/enforcement/partners/menu-e.html Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/ Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/toolbox/about/modernization/ Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fast/ Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/border_security/international_activities/partnerships/cip.xml Accessed December, 2004.

Customs and Border Protection – U.S. Department of Homeland Security. http://www.cbp.gov/xp/cgov/import/carriers/24hour_rule/ Accessed December, 2004.

Economic and Social Council. *Tamper-Indicating Seals: Practices, Problems, and Standards.* United Nations. Transmitted by U.S. Government. April 15, 2003.

Economics & Statistics Group, Alexandria, VA: American Trucking Associations, Inc., 2004.

Federal Highway Administration -- U.S. Department of Transportation. http://www.ops.fhwa.dot.gov/freight/intermodal/efm_program_plan.htm Accessed December, 2004.

Fong, R. and Guan, C. *New Container Security Regulations and Their Impact on the Supply Chain Community*. 83rd Annual Transportation Research Board Meeting. Washington, D.C., Transportation Research Board, 2004.

Government Smart Card Handbook. U.S. General Service Administration. http://www.smartcardalliance.org/industry-info/index.cfm

Johnston, Roger G. *Efficacy of Tamper-Indicating Devices*. Journal of Homeland Security, April 2002.

Johnston, Roger G. *Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste.* Science & Global Security, Volume 9, pp 93-112, 2001.

Maritime Safety Committee. *Prevention and Suppression of Acts of Terrorism Against Shipping: Container Security*. International Maritime Organization, April 12, 2002.

Nanavati, Samir, Thieme, Michael, Nanavati, Raj. "Biometrics: Identity Verification in a Networked World," Wiley Publishing, 2002 ISBN 0-471-09945-7

Nash, Andrew and William Duane, Celia Joseph, and Derek Brink. PKI- Implementing and Managing E-Security," RSA Press, 2001.

North River Consulting Group and Homeland Security Research Corp, *2004 Maritime Smart Containers Product Comparison Report*, 2004

Ojah, M. *Securing and Facilitating U.S. Land Border Trade: A Critical Analysis of the C-TPAT and FAST Programs*. 84th Annual Transportation Research Board Meeting. Washington, D.C., Transportation Research Board, 2005.

SAIC *Container Seal Technologies and Processes*, McLean, VA, 2003.

SAIC *WSDOT Intermodal Data Linkages Freight ITS Operational Test Evaluation*, Arroyo Grande, CA, 2002.

Science Applications International Corporation. Hazardous Materials Safety and Security Operational Test Evaluation Final Report for Contract DTFH61-98-C-00098; Task 9851. Submitted to the USDOT ITS Joint Programs Office and the Federal Motor Carrier Safety Administration, November 11, 2004.

TransCore *Alameda Corridor Test Report*, San Diego, CA, 2002.

TransCore *Northwest Trade Corridor*, San Diego, CA, 2001.

Transportation Research Board. *Cybersecurity of Freight Information Systems: A Scoping Study*. National Academy of Sciences, 2003.

Transport Topics. The 2004 Transport Topics 100 Top For Hire Carriers. As seen at http://www.ttnews.com/tt100/2004/TT100%20040719.pdf 02/28/05. Alexandria, VA, 2004.

Transport Topics. The 2004 Transport Topics 100 Largest Private Fleets. As seen at http://www.ttnews.com/tt100/2004/TT100%20040726.pdf 02/28/05. Alexandria, VA, 2004.

U.S. Department of Transportation Bureau of Transportation Statistics *U.S. International Trade and Freight Transportation Trends*, BTS03-02 Washington, DC, 2003.

Villa, J.C. and Stockton, W.R. Technology Applications to Enhance Freight Flows At The U.S.-Mexico Border In An Era of Heightened Security. *84th Annual Transportation Research Board Meeting*. Washington, D.C., Transportation Research Board, 2005.

Wolfe, M. *Electronic Cargo Seals: Context, Technologies and Marketplace*. Prepared for: Intelligent Transportation Systems Joint Program Office Federal Highway Administration U.S. Department of Transportation, July 12, 2002.

DEFINITIONS & ACRONYMS

AAPA American Association of Port Authorities
ABI Automated Broker Interface
AC Area Command
ACE Automated Commercial Environment
ACP Area Contingency Plan
ACS Automated Commercial System
AES Automated Export System
AMS Automated Manifest System
ANSI American National Standards Institute
API Application Program Interface
ASPHEP Assistant Secretary for Public Health Emergency Preparedness
ATA American Trucking Associations
ATRI American Transportation Research Institute
ATS Advance Targeting System
AVI Automatic Vehicle Identification
BASSC Business Anti-Smuggling Security Coalition
BioAPI Biometric Application Program Interface
BTS Border and Transportation Security
CAC Common Access Card, a program of the USDoD
CAP Civil Air Patrol
CBP Customs and Border Protection
CBRNE Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive
CBEFF Common Biometric Exchange Formats Framework
CDC Centers for Disease Control and Prevention
CDRG Catastrophic Disaster Response Group
CHCP Cargo Handling Cooperative Program
CIA Central Intelligence Agency
CIIMG Cyber Interagency Incident Management Group
CIP Carrier Initiative Program
CIP Critical Infrastructure Protection
CIRES Catastrophic Incident Response Execution Schedule
ConOps Concept of Operations
CONPLAN U.S. Government Interagency Domestic Terrorism Concept of Operations Plan
COP Common Operating Picture
COTS Commercial Off-The-Shelf
CSI Container Security Initiative
CT Counterterrorism
C-TPAT Customs Trade Partnership Against Terrorism
CVSA Commercial Vehicle Safety Alliance
CWG Container Working Group
DES Data Encryption Standard
DEST Domestic Emergency Support Team
DHS Department of Homeland Security
DIA Defense Intelligence Agency
DISC Disaster Information Systems Clearinghouse
DMAT Disaster Medical Assistance Team
DMORT Disaster Mortuary Operational Response Team

DoD Department of Defense
DOT Department of Transportation
DRC Disaster Recovery Center
DTRIM Domestic Threat Reduction and Incident Management
EAS Emergency Assistance Personnel or Emergency Alert System
EDI Electronic Data Interchange
EFM Electronic Freight Manifest
EOP Emergency Operations Plan
EPA Environmental Protection Agency
EPCRA Emergency Planning and Community Right-to-Know Act
ESCM Electronic Supply Chain Manifest
FDA Food and Drug Administration
FAR False Acceptance Rate
FAST Free and Secure Trade
FBI Federal Bureau of Investigation
FEMA Federal Emergency Management Agency
FHWA Federal Highway Administration
FIPS Federal Information Processing Standard
FIRST Freight Information Real-Time System
FMCSA Federal Motor Carrier Safety Administration
FOT Field Operation Test
GPO Government Printing Office
GPS Global Positioning System
GSC-IS Government Smart Card Interoperability Specification
HAZMAT Hazardous Material
HM Hazardous Materials
HME Hazmat Endorsement
HW ISAC Highway Information Sharing and Analysis Center
HWW Highway Watch
HWW EPEC Highway Watch Emergency Planning and Education Center
HSARPA Homeland Security Advanced Research Planning Agency
HSC Homeland Security Council
HSI Homeland Security Institute
HSIN Homeland Security Information Network
HSOC Homeland Security Operations Center
HSPD Homeland Security Presidential Directive
IAIP (DHS) Information Analysis and Infrastructure Protection Directorate
IBIS Interagency Border Information Service
ICD Infrastructure Coordination Division (DHS/IAIP)
ID Identification
IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers, Inc
IFTWG Intermodal Freight Technology Working Group
IMO International Maritime Organization
IND Improvised Nuclear Device
INCITS International Committee for Information Technology Standards
ISAC Information Sharing and Analysis Center
ISO Organisation for International Standards
ITDS International Trade Data System

IVI Intelligent Vehicle Initiative
ITS Intelligent Transportation Systems
JHU/APL The Johns Hopkins University Applied Physics Laboratory
JPO Joint Program Office
JRIES Joint Regional Intelligence Exchange System
JTTF Joint Terrorism Task Force
LDWS Lane Departure Warning Systems
LTL Less-Than-Truckload
MARAD Maritime Administration
MC Motor Carrier
MTMC Military Traffic Management Command
MTSA Maritime Transportation Security Act
NBC Nuclear, Biological, and Chemical
NCP National Oil and Hazardous Substances Pollution Contingency Plan
NGA National Geospatial-Intelligence Agency (new name of NIMA – National Imagery and Mapping Agency)
NHS National Highway System
NIC National Incident Command
NICC (DHS) National Infrastructure Coordination Center
NIEOC National Interagency Emergency Operations Center
NIMS National Incident Management System
NIPP National Infrastructure Protection Plan
NIRT Nuclear Incident Response Team
NISC National Infrastructure Security Committee
NIST National Institute of Standards & Technology
NJTTF National Joint Terrorism Task Force
NPP National Protection Plan
NRC Nuclear Regulatory Commission
NRCC National Resource Coordination Center
NRP National Response Plan
NRP-CIA Catastrophic Incident Annex to the National Response Plan
NRP-CIS Catastrophic Incident Supplement to the National Response Plan
NRS National Response System
NR T National Response Team
NSA National Security Agency
NS/EP National Security/Emergency Preparedness (Telecommunications)
NVOCC Non Vessel Operating Common Carrier
OEM Original Equipment Manufacturer
OET Office of Emergency Transportation
OSC Operation Safe Commerce
PCIS Partnership for Critical Infrastructure Protection
PIP Partners in Protection
PIV Personal Identity Verification
PKI Public-key Infrastructure
RFID Radio Frequency Identification
RSA A public-key cryptosystem that offers both encryption and digital signatures developed by Rivest, Shamir, and Adleman in 1977
RSPA Research and Special Programs Administration
RITA Research and Innovative Technology Administration

PHMSA Pipeline and Hazardous Materials Safety Administration
SEOC State Emergency Operations Center
SSI Security-Sensitive Information
SSP Sector Specific Plan
SSV Security Sensitive Visit
SSTL Smart and Secure Trade Lanes
SWERN South West Emergency Resource Network
TL Truckload
TSA Transportation Security Administration
TSIS Transportation Security Intelligence System (TSA)
TSOC Transportation Security Operations Center
TSWG Trucking Security and Anti-Terrorism Working Group
TTIC Terrorism Threat Integration Center (DHS)
TWIC Transportation Worker Identification Card/Credential
U.S. DOT U.S. Department of Transportation
US-VISIT U.S. Visitor and Immigrant Status Indicator Technology
VAN Value Added Network
VII Vehicle-Infrastructure Interface
VMT Vehicle Miles Traveled
VOCC Vessel Operating Common Carrier
WMD Weapons of Mass Destruction
WMD-CST Weapons of Mass Destruction Civil Support Team
WMDO-IM Office of Weapons of Mass Destruction Operations and Incident Management (DHS)
WME Weapons of Mass Effect
XML Extensible Mark-Up Language

APPPENDIX A - BIOMETRIC SYSTEM VENDORS

The following partial system descriptions are directly excerpted from the respective vendors' web sites and are provided as a convenience. No editorial changes have been made, and the report authors do not attest to the accuracy of the information. All statements made below represent the views of the companies as found on their web sites during the month of February, 2005. For additional information, please visit the referenced websites.

FINGERPRINT

Bioscrypt – www.bioscrypt.com

Bioscrypt Inc. is a leading provider of advanced fingerprint technology, providing the essential final link for strong authentication by verifying who you say you are, instead of "what you have" or "what you know". The company's advanced fingerprint technology offers customers a wide range of biometric options for making access to facilities, equipment and information simpler and more secure.

Bioscrypt offers four solutions: finished readers for facility access, embedded solutions for biometric integration, information security for identity management and technology licensing of our patented, award-winning algorithm Bioscrypt Core, the decision making engine for all our fingerprint products.

Precise Biometrics – www.precisebiometrics.com

Precise Biometrics develops and supplies world-leading and user-friendly biometric security solutions for authentication using fingerprints. The solutions replace keys, PINs and passwords in three areas: IT security, physical access and embedded solutions.

Our core technology, Precise BioMatch^{TM}, is the foundation for all our fingerprint authentication solutions, and our cutting-edge Precise Match-on-Card^{TM} technology is expected to become a global standard for fingerprint solutions on smart cards.

Identix – www.identix.com

Identix provides fingerprint, facial and skin biometric technologies, as well as systems, and critical system components that empower the identification of individuals in large-scale ID and ID management programs.

The Company's offerings include live scan systems and services for biometric data capture, mobile systems for on-the-spot ID, and backend standards-based modules and software components for biometric matching and data mining. With a global network of partners, such as leading system integrators, defense prime contractors and OEMs, Identix serves a broad range of markets including government, law enforcement, gaming, finance, travel, transportation, corporate enterprise and healthcare. Identix Incorporated is now headquartered in Minnetonka, Minnesota with principal offices in New Jersey, Virginia, California and the United Kingdom. Identix has approximately 500 employees worldwide.

SecuGen – www.secugen.com

SecuGen Corporation is the world's leading provider of optical fingerprint recognition technology, products, tools and platforms. SecuGen strives to provide its customers with the highest quality products and service through continuous research & development and dedicated technical support.

SecuGen's core technologies include patented SEIR-based fingerprint sensors with 500 dpi resolution and proprietary extraction and matching algorithms. Known for their extreme durability, accuracy, and support for a wide range of platforms, SecuGen's fingerprint biometric products include OEM components, software developer kits, complete solutions, and ready-to-use PC peripherals, including the SecuGen Hamster™ (fingerprint reader) and SecuGen OptiMouse™ (fingerprint mouse).

STMicroelectronics – www.st.com

STMicroelectronics is a global independent semiconductor company and is a leader in developing and delivering semiconductor solutions across the spectrum of microelectronics applications. An unrivaled combination of silicon and system expertise, manufacturing strength, Intellectual Property (IP) portfolio and strategic partners positions the Company at the forefront of System-on-Chip (SoC) technology and its products play a key role in enabling today's convergence trends.

Zvetco – www.zvetcobiometrics.com

Founded in 1999, Zvetco Biometrics (Zvetco L.L.C.) is a manufacturer of best-in-class identity authentication hardware that uses innovative fingerprint sensing technology to safeguard data access. Zvetco also offers custom engineered parts, consulting services and OEM products.

Zvetco Biometrics' Verifi™ line of biometric products incorporates precision fingerprint-sensing technology into ergonomic computer peripherals that deliver unparalleled performance, reliability and convenience.

All of the Verifi™ products offer unequaled acquisition, recognition and error rejection rates, the highest "Spoof Protection" on the market, and extremely high resistance to Electrostatic Discharge (ESD).

Zvetco Biometrics provides its customers in the corporate enterprise, financial services, healthcare, gaming and retail industries with cost-effective biometric tools that enhance security, increase accountability, and eliminate the cost and inconvenience of password-based access.

Targus – www.targus.com

Targus Group International, Inc. pioneered the notebook carrying case category, partnering with corporations, retailers, and OEMs to provide the best possible protection for notebook PCs. Targus continues to define and shape the market for mobile computing cases and accessories. As the leading global supplier of portable solutions, Targus has offices on every continent and distributes in over 145 countries.

IRIS

LG Electronics – www.lgiris.com

LG Electronics Iris Technology Division was established in the United States in 2002, providing global management responsibility and overall direction for strategy, product development, marketing, sales and distribution of the Company's iris recognition technology products.

The US unit, with offices in Englewood Cliffs and Jamesburg, New Jersey, works closely with LG ELITE, the Company's Korean-based center for innovation, research and development. Today, the efforts of these business groups are focused on new product development while continuing to enhance the LG IrisAccess® 3000 range - the second generation of a proven Iris Access platform, which through lab testing and real-world use, has set standards for accuracy, speed, user convenience, as well as integration versatility.

OKI – www.oki.com

The people of Oki Electric, in the company's traditional progressive spirit, are committed to creating superior network solutions and providing excellent information and communications services nationally and internationally to meet the diversified needs of customers in the digital age.

Airport check-in systems, reservation and ticketing systems for travel agencies, electronic government solutions, intelligent transport systems (ITSs), telemetry and telecontrol systems, underwater acoustic systems, multipoint conference systems, banking branch systems, integrated image processing systems, call center systems, automated teller machines (ATMs), remote branch terminals, cash handling systems, iris recognition systems, e-banking solutions Internet payment, web site construction and solutions, Internet transaction consulting, web site transaction middleware, electronic statement presentment systems Enterprise resource planning (ERP), supply chain management (SCM), infrastructure management (IM), product life-cycle management (PLM), customer relationship management (CRM) Light-emitting diode (LED) color / monochrome printers, serial impact dot matrix printers, LED facsimiles.

Panasonic – www.panasonic.com

Panasonic's proven biometrics solutions extend your security capabilities beyond surveillance and monitoring, to provide a highly effective 'front-end' to your complete security solution.
Verifying identity with Iris Reader
Biometric technology overcomes many of the disadvantages of conventional ID and verification techniques such as keys, ID cards and passwords. Instead, Panasonic's solution uses on Iris Reader to verify the identity of authorized persons - positively and definitively - with virtually no chance of mis-identification.

Panasonic's expertise, combined with Iridian Technologies' proven developments in Iris Reader Technology, produce highly accurate, easy to use means of applying a wide range of current and future security requirements. The Gold Standard for Biometrics Recognition Iris Reader is the most accurate, stable, scalable and non-invasive human authentication technology in existence. It offers significant advantages over other less accurate biometric identification methods, such as fingerprints, voice and facial recognition, hand geometry, and keystroke analysis. The process is scientifically proven, user safe and operationally reliable. It offers state-of-the-art authentication, destined to replace tokens, PINs, and passwords. Do your requirements focus around network security or electronic commerce transactions, or financial or healthcare data access, or government, public safety or justice environments? Panasonic's Authenticam™ with Iridian's Private IDT software provides the most cost effective way to ensure data access security and minimizes fraudulent activities in cyber communities.

IriTech – www.iritech.com

IriTech offers a portfolio of biometric-based hardware and software products that give government and private industry users advanced solutions for identity assurance, information security, and drug abuse detection. The company creates solutions using two core technologies: iris recognition and pupil reaction analysis.

IriTech's premier iris recognition solution based on its own patented algorithm corrects many of the problems that have challenged early iris recognition applications. Identification failures caused by watery eyes, long eyelashes, and incorrect positioning of the eye in front of the camera which captures the iris image are reduced by the IriTech system.

IriTech bundles its unique iris recognition algorithm with its own bi-camera, stereo facial recognition system. This multi-modal biometric approach adds an additional layer of identification insurance while the dual camera for iris identification maps both eyes in contrast to the previous generation of imaging technologies that relied on information from one eye only. IriTech is the only company to date that offers both iris and facial recognition with its own internally developed and patented technologies. The benefit for the government or industry user is a fully functional and integrated biometric identity solution without compatibility problems, system integration delays, or added costs.

On the drug testing front, IriTech's technology requires no bodily fluids, lacks reagents, provides faster results and is more sensitive, cost effective and tamper resistant than traditional techniques such as urine testing. Additionally, in contrast to other pupil analysis players, the IriTech solution does not require a baseline test, test both eyes and evaluates over 40 parameters.

IriTech was established in San Jose, California in 2000 but is now headquartered in Vienna, Virginia - at the heart of US public/private efforts to harness the benefits of biometric technology for greater domestic and international security. In 2001 the company was issued US patents for its iris identification algorithm and pupil reaction drug pre-screening system. A patent is pending for its camera system for iris identification with stereo face recognition.

As an industry pioneer in iris recognition, the company is an active member of the INCITS (International Committee for International Technology Standards) Task Group on Biometric Data Interchange Formats. IriTech's iris recognition technologies are fully compatible with INCITS 379.

FACIAL RECOGNITION

Viisage – www.viisage.com

Viisage delivers advanced technology identity solutions for governments, law enforcement agencies and businesses concerned with enhancing security, reducing identity theft, and protecting personal privacy. Viisage creates solutions using secure credential and face recognition biometric technologies that quickly, reliably, and accurately identify individuals in both one-to-one and one-to-many situations. The Company’s goal is to help its customers solve three critical aspects of verifying and managing identities: Assurance that the identification presented is authentic, confidence that the person holding this identification document is uniquely tied to and authorized to use the credential, and verification of the privileges the credential grants. With over 3,000 installations worldwide, including all U.S. passports, Viisage’s solutions stand out as a result of the company’s industry-leading technologies that address customer needs.

For over a decade, Viisage has been providing secure identification solutions for a wide variety of organizations and applications. Whether in an over-the-counter or a central printing solution, Viisage’s end-to-end solution includes proofing, enrollment, and issuance of credentials, secure tracking of inventory, and advanced investigative tools. To date, Viisage has delivered more than 165 million secure identification credentials. With the acquisition of Arlington, Virginia-based Trans Digital Technologies (TDT), Viisage has expanded its reach to include all technologies and services for the U.S. passports and the U.S. Department of Defense's Common Access Card (CAC) program. Additional customers who have benefited from Viisage’s identity solutions include state motor vehicle offices, departments of corrections, departments of social services, and foreign government agencies. The 16 state motor vehicle offices, including Connecticut, Illinois and Mississippi, that have deployed Viisage’s credential technologies to create secure drivers’ licenses attest to the Company’s proven advanced technology solutions that provide a demonstrated return on investment. Further, the six states that employ

Viisage’s advanced face recognition investigative tools are realizing even greater results in their fight against identity theft.

Identix – www.identix.com

Identix provides fingerprint, facial and skin biometric technologies, as well as systems, and critical system components that empower the identification of individuals in large-scale ID and ID management programs.

The Company's offerings include live scan systems and services for biometric data capture, mobile systems for on-the-spot ID, and backend standards-based modules and software components for biometric matching and data mining. With a global network of partners, such as leading system integrators, defense prime contractors and OEMs, Identix serves a broad range of markets including government, law enforcement, gaming, finance, travel, transportation, corporate enterprise and healthcare. Identix Incorporated is headquartered in Minnetonka, Minnesota with principal offices in New Jersey, Virginia, California and the United Kingdom. Identix has approximately 500 employees worldwide.

The company was formed in 1982 and went public in 1985. Identix acquired several companies in the mid-1990s and most recently, in 2002, completed a merger with Visionics Corporation, to become the Identix of today.

Cognitec Systems - www.cognitec-systems.de/index.html

Cognitec Systems develops and markets the well-established and world-leading FaceVACS® face recognition software. Cognitec's software experts have been developing face recognition technology since 1995. In various independent evaluation tests including the Face Recognition Vendor Test 2002, FaceVACS® has proven to be the leading technology available on the market.

Industry and government customers use FaceVACS® for physical access control since 1996. The installation of the SmartGate system at Sydney International Airport in 2002 was a major step towards a solution for automated border control using Cognitec's software. Software companies all over the world have started developing applications using our software development kit.

Cognitec's technology and products build upon the extensive knowledge of our scientists and software engineers who have been working with face recognition systems for years. We make this knowledge available to our customers in order to apply face recognition to your problems. Our commitment is to deliver the industry-leading performance in face recognition.

A4Vision – www.a4vision.com

A4Vision (Applications for Vision) develops and licenses advanced identification systems and solutions for tracking and targeting camera systems using breakthrough 3D face recognition technology.

A4Vision products are designed for broad security applications such as surveillance and access control, law enforcement and commercial markets for PC and Internet applications. A4Vision's 3D facial biometric and camera tracking systems are based on a combination of patented optical technology, targeting and tracking software, and recognition algorithms. Through innovations in 3D data capturing and processing capabilities, these systems permit industry-leading accuracy in real-time facial recognition and tracking.

A4Vision is headquartered in Sunnyvale, California (USA) with offices in Geneva, Switzerland and Moscow, Russia.

Acsys Biometrics – www.acsysbiometricscorp.com

The Acsys product line offers powerful identity verification technology for enterprises of all sizes, for physical and logical access control, and for third-party development.

Acsys has enterprise-ready biometric solutions for diverse government agencies, as well as the financial services, airport, gaming, retail, manufacturing, e-commerce, security and health sectors. Applications are unlimited due to the ongoing customization of software to suit the specialized needs of individual clients.

Animetrics, Inc. - www.animetrics.com

Animetrics Inc. is a leading developer of next-generation 3D face recognition and face creation solutions. Animetrics' FACEngine™ family of products solve critical problems with today's facial biometric systems including the pose or angle of the face, poor or uneven lighting conditions and eventually expressions. Based on three patent-pending technologies, Animetrics' core algorithms provide unmatched speed and precision in performing 3D analysis of photographic and video imagery. Animetrics' solution is not only unique in that it has tackled and solved critical face recognition problems; it is also cost effective. Our expectation is that 2D cameras will be in use for years to come. Animetrics technology can take a 2D image of a face and convert it to 3D for accurate verification and identification

FACEngine is well suited for government, homeland security, law enforcement and commercial markets. Market segments include physical and logical access as well as ID verification. A new emerging market will be smart systems which include video surveillance and image database indexing and searches. Animetrics' break-through technology is enabling face recognition to become the biometric of choice!

VOICE RECOGNITION

Nuance – www.nuance.com

Nuance is leading the industry in the deployment of voice interfaces which provide automated telephone access to enterprise, telecommunications and Web-based applications. Nuance has hundreds of customers who have purchased the software for applications as diverse as stock trading, travel reservations, product ordering, personal assistants, banking, voice-activated dialing, call routing, and voice portal services.

Nuance customers are industry leaders who demand quality solutions. Below is a partial list of our customers with descriptions of how they are using the software to provide better customer service, reduce costs and realize new revenue streams.

Additionally, Nuance partners are providing many solutions and services, from the resale of Nuance software to systems integration, interactive voice response and component hardware, and custom development and consulting services.

ScanSoft – www.scansoft.com

ScanSoft is the world's premier supplier of speech and imaging solutions that help facilitate information exchange within and between the world’s leading companies and their customers. Our solutions capture vital information and transform it into meaningful and actionable form—helping eliminate barriers to productivity, enhance the work experience, provide universal access, and simplify the interaction with hardware and software systems. ScanSoft customers span a range of industries and disciplines with particular concentration in industries that breed information, including financial services, healthcare, government, education, utilities, travel and telecommunications. Today, more than 15 million people use a ScanSoft productivity application; half the Fortune 100 use our speech solutions and nearly one thousand devices—handsets, printers, automobiles—incorporate our technology.

Voicevault – www.voicevault.com

Voice*vault*, is the world leader in the application of voice verification. Voice*vault* provides an entrusted third party service allowing you to verify customers by their voice over the phone (Voice*vault*phone), web (Voice*vault*web), Internet (Voice*vault*net) in less than a second, regardless of where in the world the person is located.

Voice verification which is the confirmation of an individual’s identity through their speech, is a form of biometric authentication; biometrics are methods of verifying people based on physiological and behavioral characteristics. Other biometrics include iris scanning, finger printing and facial recognition.

Voice*vault*’s voice verification engine offers a replacement and or enhancement for PINs, passwords and other ‘Mother’s Maiden name?’ routines representing the best in terms of speed of verification, accuracy and value. Voice*vault* enables organizations to reduce cost and fraud, enhance security and improve overall efficiency.

Voicevault has developed a range of cutting edge applications to provide cost effective solutions for the needs and demands of today's global financial services, communications & high tech, healthcare and public service sectors.

These solutions which operate over the telephone or Internet, include Password Reset for the secure, automated resetting of PINs and passwords; Call Centre Gateway, for a more efficient and user-friendly method of accessing call centres, Voice Purchasing Portal, which provides a secure virtual group purchasing solution for an organisation's membership base and TeleTrack Corrections for monitoring low risk offenders.

HAND GEOMETRY

IR Recognition Systems, Inc - www.recogsys.com

Recognition Systems, Inc., a division of Ingersoll-Rand, is the worldwide leader in Biometric access control, time and attendance, and personal identification products. Biometric devices are electronic means of measuring unique characteristics or actions of a person, and are used to identify, or verify the identity of, an individual.

The company, founded in 1986, pioneered the commercialization of biometrics using its patented hand geometry. This technology verifies identity by the size and shape of the hand. The widespread use of Recognition Systems HandReaders in access control and time and attendance applications has established Recognition Systems as the market leader in biometric verification.

Recognition Systems HandReaders provide improved security, accuracy, and convenience for these three important applications: For Access Control, the HandReaders ensure that the person who enters isn't merely carrying someone else's access card or PIN. For Time and Attendance, the HandReaders improve payroll accuracy and simplicity by eliminating "buddy-punching." For Personal Identification, the HandReaders guarantee that the people on a site actually belong there.

The HandReaders are fast, easy to use, and reliable. As of the mid-year 2002, over 70,000 units have been installed throughout the world, in a wide variety of applications. There are over 18,000 employees at San Francisco International Airport who have depended on HandReaders for tarmac access since 1993 with over 100 million transactions. The 1996 Olympic Games utilized the HandReaders to protect access to the Olympic Village. More than 65,000 people were enrolled and over 1 million transactions were handled in 28 days. There are more than 900 HandReaders that control client and employee access to special areas of Italian banks and over 100 units perform similar functions in Russia. The HandReaders now play a vital role in a border crossing system for frequent travelers. The program, called INSPASS, is currently being expanded in United States airports. In the United Kingdom, Her Majesty's Prisons rely on the HandReaders for prisoner tracking. Universities use the HandReaders for their on-campus meal programs; to safeguard access to dormitories, and to protect their computer

centers. Veteran's hospitals throughout the United States use HandReaders to protect drug dispensaries. HandReaders allow members to access clubs around the globe without having to remember to carry a card. Schools and day care centers use hand readers to verify the identity of parents and safeguard the children left in their care. The list goes on.
Recognition Systems can attribute the majority of its success, profitability and growth to three specific markets:

BioMet Partners – www.biomet.ch

Biomet Partners, Inc. is the developer of patented 3-dimensional two-finger geometry biometric technology for fast, accurate, low cost, and user-friendly verification of a person's identity. The technology has been highly successful in a wide range of "real-world" applications, including access control, time and attendance systems, enhanced security systems, season ticket control (for sports, theaters, theme parks), passenger identity at airports, and many more.

The company was founded in 1992 as a development partnership and was registered in Nevada, USA in 1995. We are a privately held company with headquarters in Switzerland.

Two-finger geometry readers from Biomet Partners have been in commercial use since 1995, starting with the Digi-2 cameras. More than 50 million users have been enrolled on Biomet's finger geometry products. Many thousands of units are installed throughout the world, in a wide variety of applications.

Biomet's products are marketed internationally through Systems Integrators, Strategic Partners and Manufacturers (OEMs) who integrate them into their own products.

KEYSTROKE DYNAMICS

Mantra Technologies – www.mantratec.com

Mantra Technologies is a leader in Biometric security and Business solutions. Automated Fingerprint Identification System (AFIS) and software for fingerprint identification search matching / fingerprint recognition are the primary products of Mantra Technologies. We provide the accuracy criminal and civil fingerprint identification search and authentication systems in the industry. Our solutions replace keys, Pins and passwords in IT security, physical access and embedded solutions.

We are dedicated to develop state-of-the-art technologies and solutions that are innovative, cost effective and add value to the existing systems. All the solutions from Mantra Technologies are basically to take technology to the common man and make life simpler, easier and safer.

We are committed to providing total and quality solutions to give technology leverage in enhancing business and security. Mantra Technologies has very strong focus on Research and Development, Marketing and Customer Support to encompass expertise in the below mentioned areas:

- Biometric Technology and Security Systems
- Smart Card based Systems
- Business Solutions
- GIS Systems
- IVR Systems
- Cinema Software

Mantra Technologies primary customer are large-scale system integrators, Fingerprint identification system suppliers and both criminal and civil identification system end users.

Among the applications where our Fingerprint identification System software can be incorporated or for which Mantra will supply Fingerprint Identification Systems and Software are system related to: Time and Attendance, Access Control Systems, Criminal Identification, Business Transactions. Pos and Authentication for Citizen, Employee and Customers.

BioPassword – www.biopassword.com

BioPassword, Inc. is a provider of software solutions that secure access to critical data and network resources, while improving process efficiencies and decreasing IT costs. The company's flagship product, BioPassword®, is a patented software-only solution that uses keystroke dynamics, a security technology based on biometrics, to accurately identify users by the way they type. BioPassword products provide scalable, easy-to-deploy, and easy-to-support user authentication at an affordable price. Supported by a large network of technology partners and resellers, BioPassword solutions are licensed to thousands of users at over thirty global organizations. Major customers include market leaders in the financial, healthcare, government, and media and entertainment industries.

SIGNATURE RECOGNITION

CIC – www.cic.com

Communication Intelligence Corporation (CIC) is the leading supplier of biometric signature verification and natural input software and a leading supplier of electronic signature solutions focused on emerging, high potential applications including paperless workflow, handheld computers, smartphones and eCommerce enabling the world with "The Power to Sign Online®". CIC's products are designed to increase the ease of use, functionality, and security of electronic devices and eBusiness processes. CIC sells directly to OEMs and Enterprises and has products available through major retail outlets such as, CompUSA, Staples, OfficeMax, and key integration/channel partners or direct via our website. Industry leaders such as Charles Schwab, Fujitsu, Handspring, IBM, Oracle, Palm Inc., Prudential, Siebel Systems and Sony Ericsson have licensed the company's technology. CIC is headquartered in Redwood Shores, California and has a joint venture, CICC, in Nanjing, China.

CIC offers a wide range of multi-platform software products that enable or enhance pen-based computing. Core technologies are classified into two broad categories: natural input technologies and transaction and communication enabling technologies.

Natural input technologies are designed to allow users to interact with a computer or handheld device by using an electronic pen or "stylus" as the primary input device or in conjunction with a keyboard. CIC's natural input offerings include multilingual handwriting recognition systems, software keyboards, predictive text entry, and electronic ink capture technologies. Many small handheld devices such as electronic organizers, pagers and smart cellular phones do not have a keyboard. For such devices, handwriting recognition and software keyboards offer the most viable solutions for performing text entry and editing. CIC's predictive text entry technology simplifies data entry even further by reducing the number of actual letters required to be entered. The Company's ink capture technologies facilitate the capture of electronic ink for note-taking, drawings or short handwritten messages.

Transaction and Communication Enabling Technologies. The Company's transaction and communication enabling technologies are designed to provide a cost-effective means for securing electronic transactions, providing network and device access control, and enabling workflow automation of traditional paper form processing. CIC believes that these technologies offer more efficient methods for conducting electronic transactions while providing more functional user authentication and heightened data security. The Company's transaction and communication enabling technologies have been fundamental in its development of software for electronic signatures, handwritten biometric signature verification, data security, and data compression.

Softpro – www.signplus.com

SOFTPRO is based in Boeblingen, Germany and has local subsidiaries for the North American and Asian-Pacific market in Newark (Delaware) and Singapore. The group currently employs an international staff of over 60.

SOFTPRO is the leading vendor of systems for the verification of handwritten signatures, worldwide. The company's portfolio contains solutions for authentication processes and documents. Therefore static and dynamic (biometric) characteristics of signatures are extracted and evaluated.

More than 200 companies are using modules of the SOFTPRO SignPlus® system successfully such as American Express, ABN Amro, Bank of America, Barclays, Citigroup, JP Morgan Chase, DaimlerChrysler, Discover Financial, HypoVereinsbank, Lloyds TSB, Mercedes-AMG and SEB.

Since 2002, the offer to secure electronic documents with handwritten signatures extended the customer portfolio of SOFTPRO to other industries such as automotive, insurance, chemical, pharmaceutical, construction, health, life sciences and logistics.

The two major investors in SOFTPRO are GE Capital (since 1998) and AdCapital (since 2001).

SOFTPRO partners include A2iA, BancTec, Carreker, Fujitsu Siemens Computers, HP, IBM, Interlink, Kleindienst, Microsoft, NCR, UNISYS and Wacom as well as APP Informatik Davos.

WonderNet Ltd – www.wondernet.co.il

WonderNet Ltd. Introduces a new generation of convenient, cost effective and secure biometric authentication with Penflow – a high-precision Biometric Signature Authentication system that enables remote authentication without changing the way we work.