



Risk Assessment and Prioritization

THE TRANSPORTATION SECTOR'S COMPONENTS ARE SUSCEPTIBLE TO THE CONSEQUENCES OF NATURAL DISASTERS AND CAN ALSO MAKE ATTRACTIVE TERRORIST TARGETS. THE SECTOR'S SIZE, ITS PHYSICALLY DISPERSED AND DECENTRALIZED NATURE, THE MANY PUBLIC AND PRIVATE ENTITIES INVOLVED IN ITS OPERATIONS, THE CRITICAL IMPORTANCE OF COST CONSIDERATIONS, AND THE INHERENT REQUIREMENT OF CONVENIENT ACCESSIBILITY TO ITS SERVICES BY ALL USERS – THESE ASPECTS COMBINE TO MAKE TRANSPORTATION VULNERABLE TO SECURITY THREATS.

The first step in preventing or minimizing the damage caused by disasters or attack is assessment of the risks to the transportation system. Risk assessment is a systematic, analytical process to identify hazards, establish their likelihood, and assess potential severity of a successful attack on some element of the system. It provides the necessary foundation for selection and implementation of actions to reduce the risk associated with existing or anticipated threats. Risk assessment has three basic components: assessment of the threat environment (likelihood of an attack); vulnerability of the system (likelihood that an attack will be successful); and the criticality and magnitude of the possible consequences (impact of a successful attack). Risk assessment, properly done, must be iterative and periodically updated to determine how risks change based on implementation of safe-

guards and countermeasures. This inherently complex process requires expert knowledge in both transportation and security.

Given the magnitude of these tasks, priorities must be established to guide decisions and balance benefits versus costs, including identification of system-level externalities and the potential for unintended consequences. A prioritized, risk-based approach is a critical element to determining practical, affordable solutions. Once the risks are identified, assessed, and prioritized, action plans can be developed to mitigate the risks.

The Department of Transportation's (DOT) history and success in addressing transportation safety in all modes provides experience and insight directly relevant to security issues. This section of the Journal covers critical infrastructure protection initiatives and presents examples of the Volpe Center's assessments in support of DOT mandates.

Critical Infrastructure Protection Initiatives

THE VOLPE CENTER'S WORK IN SUPPORT OF INFRASTRUCTURE SECURITY INITIATIVES

The government and its key agencies have a major stake in assuring the security of the nation's critical infrastructure and its underlying information resources. The Volpe Center's core capabilities and past experience support these agencies' goals and objectives toward coordinated and comprehensive preparation and response. Several key vulnerability and risk assessments that Volpe has conducted in support of national security goals are discussed in the section that follows.

Surface Transportation Vulnerability Assessment

The U.S. surface transportation system consists of interconnected infrastructures including highways, transit systems, railroads, airports, waterways, pipelines and ports, and the vehicles, aircraft, and vessels that operate along these networks. Interdependencies exist between transportation and nearly every other sector of the economy. Consequently, the effective operation of this system is essential to America's continued prosperity, economic productivity, and national security because a threat to the transportation sector may impact other industries that rely on it.

The Volpe Center's experts, representing knowledge and experience in engineering, information systems, security, and other disciplines, have been working for years on security issues for the nation's surface transportation systems. In February 1999, the Center released the "Surface Transportation Vulnerability Assessment," which examined the vulnerability of key transportation elements and the potential impact of terrorism, sabotage, or criminal activity that could seriously disrupt safety and operations. The assessment evaluated the threat of physical, biological, chemical, or cyber attack on transportation infrastructure. The assessment was conducted for the DOT through the Research and Special Programs Administration (RSPA) and the Office of Intelligence and Security, in response to the President's Commission on Critical Infrastructure Protection (PCCIP) mandates. Volpe's "Surface Transportation Vulnerability Assessment" identified and ranked threats to the operations and facilities of U.S. transportation in terms of the most critical threats; summarized countermeasures to mitigate these impacts; and also recommended improvements to

Recent administrations have encouraged increased proactive planning and activity to secure America's infrastructure against terrorist and cyber attacks.

The President's Commission on Critical Infrastructure Protection

Efforts to protect the surface transportation system are only a small part of recent efforts throughout the federal government to protect critical national infrastructures. The first national effort addressing the nation's critical vulnerabilities resulted in the 1996 creation of the President's Commission on Critical Infrastructure Protection (PCCIP). The Commission consisted of 18 senior representatives from private industry, government, and academia. It was charged with identifying critical infrastructures, assessing their vulnerabilities, and formulating a comprehensive national strategy for protecting them from physical and cyber threats.

In October 1997, the Commission issued "Critical Foundations: Protecting America's Infrastructures," calling for a national effort to assure the security of



the United States' increasingly vulnerable and interconnected infrastructures. An infrastructure was considered critical if its incapacity or destruction would have a debilitating effect on the defense or economic security of the nation.

In support of the PCCIP and report, the Volpe Center prepared several background assessments:

Transportation Infrastructure Assurance. The Volpe Center prepared the "Interagency Transportation Infrastructure Assurance Research and Development Plan" for the National Science and Technology Council. The Plan included a summary of the nation's transportation infrastructure, its vulnerabilities and potential threats, and a discussion of current and planned R&D to improve its security.

Assessment of the NAS Vulnerabilities. The Volpe Center delivered a presentation to the PCCIP on the completed assessment of the National Airspace System's (NAS) vulnerabilities to electronic intrusions. The assessment addressed the (continued on page 6)

(continued from page 5) Federal Aviation Administration's (FAA) present and future electronic security issues, including current electronic intrusions that might cause significant delays or major accidents in the NAS. FAA systems were also analyzed to determine avenues that intruders might use, given these systems' greater potential vulnerability due to modern open systems architectures and the rapid changes in communications technologies.

Ports and Waterways Vulnerability Study. The Volpe Center conducted a Ports and Waterways Vulnerability Study in support of DOT's analyses of threats to the critical transportation infrastructure.

Pipeline Cyber Security. Volpe researched advances in supervisory control and data acquisition (SCADA)/distributed control system (DCS) technology to assess the threats and vulnerabilities associated with these advances as they relate to pipeline security. Gas pipeline technology was assessed to determine if existing equipment or new technological equipment and practices were susceptible to electronic or cyber threats.

Presidential Decision Directive 63 — Critical Infrastructure Protection

Presidential Decision Directive 63 (PDD-63), issued in May 1998, built on the recommendations of the PCCIP. It was the Administration's intent that Cabinet agencies "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures including especially our cyber systems." PDD-63 represented the culmination of an intense, interagency effort to evaluate the PCCIP recommendations and produce a workable and innovative framework for critical infrastructure protection. This includes identifying and assessing vulnerabilities, planning to reduce exposure to attack, and improving cooperation between the government and the private sector.

The Volpe Center supported the FAA in developing its response to PDD-63, which mandated that the agency develop and implement a comprehensive NAS Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

The Center also supported the DOT, in consultation with the Department of Defense, which were charged with taking on a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System (GPS).

enhance the overall safety and security of the U.S. surface transportation system.

The "Surface Transportation Vulnerability Assessment" report identified the following factors as major determinants of asset vulnerability:

- Accessibility:** Ease of getting the weapon to the target
- Effort:** Required sophistication of the attacker, and physical resistance of the target
- Control:** Degree of control the attacker has over the outcome
- Security:** In-place security measures

Vulnerabilities are key physical, technical, administrative, procedural, human-related, or systemic characteristics of an asset that make it possible for a specific attack to be successful. The Volpe Center's "Surface Transportation Vulnerability Assessment" found that highways are the most important—and robust and resilient—single-surface mode; however, the system's bridges and tunnels are significantly vulnerable, and expensive and difficult to replace. In the case of public transit, the direct impact of a single system attack would be limited geographically to that urban area, although it has the potential to affect the largest number of passengers and have the most casualties. Rail, maritime, pipeline, and intermodal freight networks were also found to be vulnerable due to rail bridges, tunnels, and maritime dock and port facilities.

The report defined three categories of countermeasures for transportation situations:

- Define Problems:** Perform risk assessments of key transportation facilities and operations
- Develop Effective Solutions:** Using technology and best-practice surveys, develop security standards
- Execute Solutions:** Implement immediate low-cost improvements including physical barriers, increased surveillance, monitoring equipment, and security personnel

The assessment noted that, as advanced technologies are adopted by each transportation mode, they become more vulnerable to technology-based attacks. Over the past two decades, there has been a deliberate attempt to take advantage of every bit of excess and underutilized capacity in the transportation system. Consequently, the traffic level on key infra-

“Mutual dependence and the interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways that they never have been before.”
— *Critical Foundations: Protecting America’s Infrastructures*, October 1997



OFFLOADING CONTAINERS AT VANCOUVER CONTAINER TERMINAL: The Volpe Center is supporting Customs and Border Protection (CBP) in its efforts to make global shipping more secure.
(Photo by Charles J. McCarthy)

structure segments has approached or even exceeded capacity, with increasing congestion and travel delays. Across the country, officials are beginning to apply technologies such as Intelligent Transportation Systems (ITS), which enable higher traffic volume on the existing infrastructure. However, this can make it easier for a saboteur to create system-wide “gridlock” by disrupting or degrading the technological application.

The Center’s report showed the need for a large-scale and coordinated program of education, training, and community outreach to maintain the level of awareness and vigilance necessary to reduce the possibility of successful attacks. The National Research Council (NRC) formed a committee to evaluate the vulnerabilities outlined in the Volpe Center report, and to formulate priorities for future research and development. Further research was recommended to develop countermeasures against chemical/biological and cyber attacks.

PORT ASSESSMENTS

The U.S. economy depends on efficient movement of people, goods, information, and financial resources all over the country and elsewhere in the world through an integrated transportation infrastructure of highways, railways, transit services, waterways, pipelines, and airports. Cargo terminals act as essential ‘nodes’ on this infrastructure, where people and goods are transferred from one transportation mode to another.

Unfortunately, these terminal nodes, especially at U.S. Customs locations, are points where significant cargo theft, insurance fraud, drug trafficking, and illegal immigrant trafficking have taken place. The United States has tried to combat cargo-related crimes; however, the number of crimes and economic losses continues to climb. The September 11 events have also brought to light security vulnerabilities at cargo terminals and the need to address them to reduce the terrorist threat.

Assessing the potential threat to transportation facilities and the range of measures that can be taken to guard against them requires the participation and assent of all organizations, both public and private, involved in transportation operations and oversight. This includes numerous federal agencies with transportation, law enforcement, and threat-analysis responsibilities, as well as their state and local counterparts; transit and port authorities; and private transportation providers. The Volpe Center is contributing to port security work in several areas which are described below.

Intermodal Cargo Transportation: Industry Best Security Practices

The Volpe Center developed a compilation of the intermodal cargo industry’s security best practices. This report, entitled “Intermodal Cargo Transportation: Industry Best Security Practices” and released in 1999, has been distributed

widely to industry, and the Volpe staff has presented the findings at numerous symposia, such as the National Cargo Security Council. This report represents the results of research, interviews, and onsite evaluations conducted to identify the issues related to security of cargo terminals to theft, smuggling, and other illegal activity. This report also provides industry best security practices for eliminating, mitigating, and controlling identified concerns within the security framework of cargo transportation. In keeping with the transportation infrastructure assurance philosophy, this report is not organized by mode (truck, rail, maritime, and pipeline), but rather provides an integrated discussion of all modes using cargo terminals with a special focus on intermodalism.

Conclusions and recommendations in the report include:

- A standardized, system-wide analysis of cargo security is necessary to understand all aspects of security.
- Insufficient cargo and theft data are currently collected to accurately investigate weaknesses in cargo transportation security.
- An analysis is necessary to investigate the security practices of international ports outside of the United States.
- Joint federal and industry efforts should be undertaken to standardize cargo security requirements.
- A jointly maintained cargo security system should be developed that integrates federal requirements with commercial industry best practices.
- Technology should be developed that allows non-intrusive cargo screening and tracking to detect contraband and discourage criminals and terrorists from using the transportation infrastructure.

The Center has also conducted detailed assessments of port facilities, evaluating the vulnerability of logistics processes and electronic commerce to both physical and cyber attacks.

Ongoing Port Assessments Worldwide

To gather more information and address the problems noted in the 1999 report, the Volpe Center is visiting airports and seaports worldwide to learn about procedures and techniques that can be applied to reduce the threat of cargo theft and terrorism. In March and April 2002, Center staff visited the Civil Aviation Authority and Customs Departments at United Arab Emirates (U.A.E.) airports to gather information on best security practices used there to reduce the threat of cargo theft

and terrorism. U.A.E. airports were chosen because they have the largest cargo traffic in the Middle East and utilize sophisticated information technology networks. The findings will be published in a report on Intermodal Best Security Practices in International Aviation and Maritime Cargo Operations. This report is part of the Volpe Center's support to the DOT Office of Intelligence and Security and the Global Maritime and Transportation School at the U.S. Merchant Marine Academy. Topics addressed include cargo theft, insurance fraud, drug trafficking, transport of illegal immigrants into the United States, and terrorism issues.

The Volpe Center is preparing another report on Intermodal Best Security Practices in Cargo Container Operations. This report is also part of the Volpe Center's support to the Global Maritime and Transportation School at the U.S. Merchant Marine Academy. In the fall of 2002, Volpe personnel visited the Naples Port Authority, Italian Customs Service, Italian Coast Guard, and container terminal operations at the Port of Naples, Italy, to gather information on best cargo security practices. The Volpe team also visited Malta to meet with the Malta Maritime Authority and the Malta Customs Service, and to observe container terminal operations at the Freeport. Other ports visited include the Port of Rotterdam, Netherlands, and the ports of Jebel Ali, Rashid, and Hamriyah in Dubai, U.A.E. Additional surveys took place in Hamburg, Shanghai, and Singapore.

The Volpe Center is preparing a final best practices report using data from the ports noted above, as well as data from the Port of Vancouver, Canada, under a recent Customs and Border Protection project, and the Port of Hamburg, Germany, under Operation Safe Commerce. In December 2003, the Volpe Center staff was also asked to brief officials from the U.S. Coast Guard Office of Homeland Security on the Center's capabilities and experience in performing foreign port vulnerability assessments.

Operation Safe Commerce

One of the most common and frightening terrorist scenarios being discussed today is the use of oceangoing containers to smuggle terrorists and weapons of mass destruction into the United States. For example, international terrorists could, with relative ease, smuggle a crude nuclear device via one of the more than 17,000 containers that arrive in the United States each day, and detonate that device. The physical devastation

Assessments across modal systems

The national transportation system is a network of many modal systems that provides unparalleled accessibility and mobility. The Volpe Center has developed a core capability to assess the vulnerabilities of components of the transportation enterprise by combining systems engineering with operations and planning expertise.

Air Traffic Control Systems and Facilities

In support of the Federal Aviation Administration (FAA), the Volpe Center conducted a vulnerability assessment of representative U.S. air traffic control facilities. The assessment included an audit of existing physical security and access to mechanical systems. Potential pathways for the introduction of harmful biological and chemical agents into the facilities were identified. The report detailed threat scenarios and recommended steps for threat reduction and protection of employees.

The Nation's Pipelines

As a follow on to the Volpe-prepared "Surface Transportation Vulnerability Assessment" (described in this section), the Volpe Center prepared a report to review the vulnerabilities of the Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) technology in the nation's oil and natural gas infrastructures. The SCADA system uses computer technology to gather data on pipeline pressure, temperature, and delivery flow rates from remote locations along the pipelines. The report examines the inherent vulnerabilities of new computer environment technology and interoperability. One significant finding highlights the fact that the oil pipeline infrastructure is highly dependent on the electrical power and telecommunications infrastructure. Based on the study's findings, Volpe staff made recommendations regarding information assurance and protection concepts for the computing environment infrastructure that supports the transmission and shipment of natural gas and oil.

Food and Milk Supply Chains

The goal of effective supply chain management is to ensure that each link provides adequate security without adversely affecting the movement of shipments to their final destinations. This can be particularly important for subsistence commodities (food and food products). In support of two projects, Volpe Center teams will closely analyze supply chains, identify vulnerabilities, propose and demonstrate

improvements, and evaluate the effectiveness of the demonstration technologies and business practices. For a project sponsored by TSWG and the Food and Drug Administration (FDA), the Center will assess the security of the U.S. milk supply chain. For the DoD, the Center will examine the interactions between enhanced security and shipment efficiency in moving DoD subsistence commodities to overseas locations.

Port Security

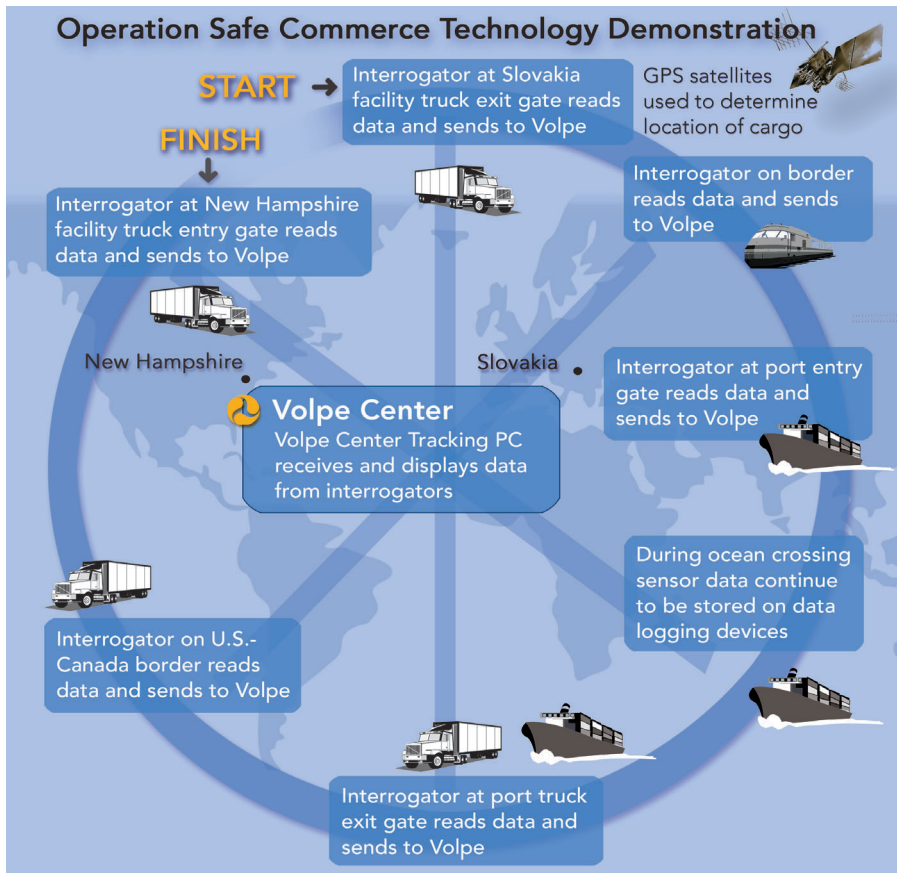
The Volpe Center began working in March 2002 with the First Coast Guard District on the "Boston - A Model Port" project. The project involves evaluating the liquefied natural gas (LNG) delivery system and the cruise ship industry in Boston Harbor. Boston was the test site for this project, with the ultimate goal being to develop and evaluate certain practices that will reduce port-security vulnerabilities in any port.

Intercity Buses

The size and pervasive nature of the nation's trucking and busing infrastructure pose significant protection challenges. In response to a request from the Federal Motor Carrier Safety Administration (FMCSA), the Volpe Center conducted an assessment of motorcoach security. The Volpe team identified various countermeasures based on the level of risk present, how critical the vulnerability may be, system design, and availability and cost of countermeasures. The Volpe Center is working with FMCSA and the Transportation Security Administration (TSA) to produce a version of the report for the motorcoach industry.



In October 2001, a passenger attacked the bus driver and then forced this Greyhound bus off the road in Manchester, Tennessee, killing six people. (Photo ©Rusty Russell/Getty Images)



OPERATION SAFE COMMERCE TECHNOLOGY DEMONSTRATION: An innovative public-private partnership supports Operation Safe Commerce, which aims to develop a model for improved security and mobility of containerized freight. Volpe performed an assessment of an entire multimodal, global supply chain and demonstrated tracking and sensing technologies. Data were captured by interrogation stations and transmitted to the Volpe Center.

caused by that small nuclear explosion would be tragic, and it would be followed by far more widespread damage of a different kind. In all likelihood, fear would bring the global movement and processing of oceangoing cargo to a halt for a prolonged period.

Key federal, state, and private entities are working together to construct a prototype of a secure international trade corridor. Operation Safe Commerce aims to develop a model for improved security and mobility of shipments of containerized freight, while maintaining open borders and facilitating international commerce. Under the sponsorship of the Combating Terrorism Technology Support Office/Technical Support Working Group (CTTSO/TSWG), the Volpe Center supported the U.S. Coast Guard, U.S. Marshals Service, and Customs and Border Protection in this innovative public-private partnership. Other public partners include the U.S. Attorneys Offices for Vermont and New Hampshire, and the State of New Hampshire Governor's Office. CTTSO/TSWG is an interagency group whose mission is to provide for rapid research,

development, and prototyping of new technology for the National Research and Development Program for Combating Terrorism.

In spring 2002, the Center executed Phase I of Operation Safe Commerce, in which a single cargo container was tracked and its security monitored, during shipment from Central Europe to the United States. The Volpe team achieved its objectives for Phase I: identification of security concerns and practices within a supply chain for a single container; and demonstration of available technologies for tracking and monitoring the container's integrity and contents. The report was released in October 2002. It is available from the Volpe Center but is restricted to those organizations involved in cargo security efforts.

Volpe reviewed commercially available tracking and security systems, and analyzed the shipment process of an industry volunteer shipper's container. The team's analysis of the shipment process is a particularly significant achievement, as it was one of the

first assessments of a transatlantic supply chain. In parallel to defining the supply chain, the team documented security practices and technologies used by the organizations that handled the container, and identified potential vulnerabilities in the supply chain. These vulnerabilities, which cannot be discussed here, are typical of many international supply chain operations. The supply chain of the sample shipment was relatively simple, involving a single commodity, single points of origin and destination, and a single carrier and freight forwarder. Nevertheless, the shipment illustrated many of the complexities of container shipping—it traversed several international borders, and involved motor carrier, rail, and maritime transportation.

The demonstration of tracking and sensing technologies began in Slovakia, the supply chain point-of-origin, where the Volpe team installed a GPS transceiver and data logger, electronic seals, and intrusion sensors on the container. At five locations along the route, the team had installed interrogation stations for collecting data from the container and transmitting it to the Volpe Center. Over the next ten days, the team moni-

tored the container's location and integrity as it traveled across Europe and the Atlantic, through the Port of Montreal, and across the U.S. border to its final destination in New Hampshire, where the container arrived with the seal intact.

Volpe's technology demonstration provided valuable insight into the effectiveness and feasibility of using container tracking and sensing technologies, and identified specific technical capabilities needed by an integrated container security system. Future Operation Safe Commerce initiatives are expected to be conducted in collaboration with related initiatives in government and industry to improve the security and efficiency of international commerce, with Operation Safe Commerce used as a "test bed" to evaluate key issues and proposed improvements.

VULNERABILITY ASSESSMENT OF THE TRANSPORTATION INFRASTRUCTURE RELYING ON THE GLOBAL POSITIONING SYSTEM

The Global Positioning System (GPS) was scheduled to be the sole source of radionavigation for aircraft guidance systems by the year 2010. However, the Presidential Commission on Critical Infrastructure Protection recognized that using GPS alone would create the potential for a single source of failure. Thus the U.S. DOT was mandated by PDD-63 to undertake a thorough evaluation of the national transportation infrastructure that relies on the GPS to address the vulnerability of the system and ensure that civil transportation systems are not totally dependent on any one technology.

The Volpe Center supported that effort by conducting an independent, integrated assessment of risks to civil users in the United States of GPS-based systems. A report on the project findings, entitled, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," was submitted in 2001 to the Assistant Secretary for Transportation Policy at DOT. The Center's research assessed the risks and made recommendations for the navigation systems mix needed to both improve radionavigation and provide backup to GPS.

Once hailed as the only navigation system necessary for aviation and other modes of civil transportation, the role of GPS has been reevaluated in the last few years. GPS is accepted as an

increasingly important component in the nation's transportation infrastructure, but it is no longer seen as a single-source solution that can replace all other forms of radionavigation.

A major element of GPS vulnerability lies in the very low power that makes it vulnerable to jamming. GPS also is vulnerable to spoofing, to picking up broadcast signals with deliberately misleading information, and to unintentional interference. The latter can be due to natural causes (for example, solar flares and ionospheric scintillation), and also to human sources (for example, TV broadcasts, mobile satellite services, ultra wide-band systems, military jamming/spoofing tests, and military communications systems). A peculiar but valid class of vulnerability is the degree of unrealistic expectations that can be produced in enthusiastic but unwary GPS users. If there is inadequate integrity monitoring, the ready willingness to accept a GPS-driven electronic display, for example, can magnify the effectiveness of jamming on the user. Loss of GPS is a threat not only to civil transportation users, but also to banking, communications, data processing, and Internet enterprises that rely increasingly on the GPS timing signal.

Taking these potential vulnerabilities into account, GPS-related disruption can cause serious injury or fatality, negative economic impact, environmental and property damage, loss of confidence in a transportation mode, and liability to a service provider. The Volpe Center assessed the vulnerability of critical GPS applications and recommended appropriate mitigation techniques in critical applications wherever possible.

The worst effects of GPS disruption can be mitigated by strengthening the GPS signal, protecting the spectrum, integrating GPS with independent systems, and/or developing appropriate operational procedures. Mitigation techniques will require some combination of terrestrial or space-based navigation and timing systems, on-board inertial navigation systems, and improved integrity monitoring and operational procedures.

The Volpe report also recommends that DOT work with DoD to identify and evaluate anti-jam and anti-spoofing technologies used by the military, including receivers and antennas that are available and applicable to the civil sector. In addition, the study recommends a comprehensive analysis of GPS backup technologies for navigation and precise timing, including VOR/DME, ILS, Loran-C, and inertial navigation systems. It also recommends that all transportation modes follow the lead of the aviation sector by considering the use of Receiver Autonomous Integrity Monitoring (RAIM) of GPS signals.

The Volpe Center assessment concluded, “If the government expeditiously develops and executes a plan based on these recommendations, there is every reason to be optimistic that GPS will fulfill its potential as a key element of the national transportation infrastructure.”

Volpe GPS Recommendations and Action Plan

The DOT operating administrations, having conducted a thorough review of the Volpe Center study, announced that they concur with all of the report recommendations. As announced in March 2002, the DOT is implementing a GPS action plan that includes the following initiatives for maintaining the viability of the nation’s transportation infrastructure:

- Ensure that adequate GPS backup systems are maintained.
- Maintain the partnership with the DoD to continue modernizing GPS with the implementation of new civil signals.
- Facilitate transfer of appropriate GPS anti-jam technology from the military for civil use.
- Conduct industry outreach to develop GPS receiver performance standards.
- Emphasize and promote education programs with state and local departments of transportation that advise users about GPS vulnerabilities.
- Assess radionavigation capabilities across all the modes of transportation to identify the most appropriate mix of systems, from both a capabilities and cost perspective, for the next 10 years and beyond. This will include completing the evaluation of the long-term need for the continuation of Loran-C systems.

Transportation Secretary Norman Mineta noted, “The action plan... will ensure that the vulnerabilities identified in the (Volpe) report do not affect the safety and security of our transportation system as we work to ensure that GPS fulfills its potential.”

FAA INFORMATION SYSTEM SECURITY ASSESSMENT

Our National Airspace Systems (NAS) represent an increasingly complex network of interconnected systems, including more than 38,000 facilities and related systems that support air traffic control. The heavy reliance of passenger and com-



mercial air transportation on information systems to support every facet of air service operations makes these systems a tempting target for sabotage. Having critical air traffic control systems rendered dysfunctional or programmed with inaccurate data poses serious consequences not only for the flying public, but also for the entire air transportation sector, if the disruption is sufficiently widespread.

The Federal Aviation Administration (FAA) recognizes the crucial importance of protecting air traffic control information and the NAS systems that control and disseminate it. As a part of the FAA’s security efforts, the Volpe Center has been conducting risk assessments of critical NAS systems, including terminal automation systems, communication switches and recorders, navigation and landing systems, radar and other surveillance equipment, and flight beacons. The risk assessments are being performed for the FAA’s Air Traffic Services Security Program Office and the NAS Integrated Product Teams (IPT) as part of a program to ensure the integrity of NAS, instituted in response to PDD-63 which required the FAA to develop and implement a comprehensive security program to protect its critical cyber and physical infrastructure.

The program includes preparation of a Security Certification and Authorization Package (SCAP) to address the risks that are identified in individual systems. A SCAP consists of five response documents: a risk assessment, a risk mitigation plan, a security plan, a security test and evaluation (ST&E), and a contingency plan. The Volpe Center is responsible for the preparation of SCAPs and also performs technical reviews of SCAPs prepared by others for the FAA.

AIR FORCE NAVSTAR GLOBAL POSITIONING SYSTEM: This is an artist's rendering of a GPS BlockIIIF satellite designed, developed, and produced by Rockwell International Corporation. The GPS satellite provides three-dimensional navigation data for military and civilian applications. (Illustration ©AP/Wide World Photos)

The NAS studies conducted by the Center involve analyzing data sensitivity, identifying threats and vulnerabilities, assessing the likelihood and severity of various threat-vulnerability combinations, and recommending countermeasures to mitigate such occurrences. Risks are ranked in terms of the confidentiality, integrity, and availability of the system's information. The most common problems identified were password management deficiencies, networking problems, lack of security audits, and untimely installation of security patches for software operating systems/applications.


A number of these problems can be addressed with relatively simple fixes, either in software or through systems upgrades. Countermeasures include upgrading to commercial-off-the-shelf (COTS) software that addresses password problems; reconfigured firewalls and routers to maximize security controls; virtual private networks; vulnerability assessment scanning; and enhanced control mechanisms to monitor network use and access. Volpe staff also developed a CD-ROM that provides automated information on security technologies and products for use by field personnel specifying new security systems.

RISK ASSESSMENT & PRIORITIZATION LESSONS LEARNED

By evaluating the vulnerability of transportation's physical and cyber infrastructure, the Volpe Center provides clients with an understanding of potential security threats so that countermeasure strategies can be developed. Thorough assess-

ment supports the creation of effective, comprehensive, and integrated solutions. The Center's systems approach to analyzing vulnerabilities also makes it possible to prioritize threats and evaluate the costs and benefits of countermeasures. Understanding vulnerabilities also increases awareness of long-term security issues and makes it more likely that security measures will be designed into new facilities.

The special and diffuse nature of terrorism means that risks to the transportation sector, and how they are identified and addressed, differ substantially from public safety risks and environmental problems. Terrorist threats are characterized by lack of information and unpredictability about timing, location, and scale. The complexity of the transportation sector and the nature of security threats require a rigorous vulnerability assessment methodology that can help to identify potential security problems and allow threat levels to be estimated with reasonable confidence. This requires undertaking a broad system perspective and understanding the interrelationships between many factors. In addition, successful vulnerability analysis cannot be static, given that security threats are constantly evolving and changing.

Understanding, analyzing, and sustaining the robustness and resilience of our critical transportation infrastructures require multiple viewpoints and a broad set of interdisciplinary skills. The Volpe National Transportation Center's experts will continue to work closely with other agencies, particularly the Departments of Transportation and Homeland Security (DHS), and with the entire transportation community, to assess risk and develop ways to minimize risks to personal safety and economic loss for operators and users of the system. These efforts are vital to prevent the serious national economic damage inevitably associated with any sustained significant reduction of the availability and performance of transportation services. 

RISK IS A FUNCTION OF VULNERABILITY AND CONSEQUENCE

$$\text{Risk} = [\text{Threat} \times \text{Vulnerability}] \times \text{Consequence}$$

- Threat** is a measure of the likelihood that a specific type of attack will be initiated against a specific target
- Vulnerability** is a measure of the likelihood that various types of safeguards against threat scenarios will fail
- Consequence** is the magnitude of the negative effects if the attack is successful