Journal of Homeland Security

Technology for Border Protection: Homeland Security Funding and Priorities

David Z. Bodenheimer

August 2003

David Z. Bodenheimer is a partner in the law firm of Crowell & Moring LLP in Washington, DC, where he specializes in government contracts and homeland security. He handles litigation, advises clients, and writes and lectures on high-technology and biodefense matters, including chemical and biological protection, electronics systems, and satellite communications. Before coming to Crowell & Moring, he worked for the Navy Department as Assistant to the General Counsel. He thanks his partner Raymond F. Monroe for his insights on border security issues.

David Z. Bodenheimer can be reached at (202) 624-2713 or dbodenheimer@crowell.com.

By any measure, protecting the United States' borders and ports pose mammoth challenges due to the sheer size of the task:[1, 2]

- 500 million people crossing the borders each year
- 5,525 miles of Canadian border
- 1,989 miles of Mexican border
- 95,000 miles of shoreline
- 350 commercial ports of entry
- 21,000 containers entering U.S. ports each day[3]

At the same time, the need for border protection must be balanced against the demand for the free flow of commerce. In 2000, trade with Canada and Mexico alone totaled $653 billion.[4] Recognizing the importance of international trade to the U.S. economy, Congress tasked the Homeland Security Department not only with protecting the borders, but also "ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce."[5]

How can the Homeland Security Department simultaneously protect the borders and preserve the flow of free trade, all while not busting the federal budget? Technology has been repeatedly presented as the critical solution for achieving these diverse objectives. In a March 2003 Congressional hearing on border security, Senator Jon Kyl emphasized the critical role of technology in meeting our homeland security needs:

[W]e'll be getting a good firsthand look at the vastness of the land, the fact that people can't possibly patrol the entire area. And therefore, we're going to continue to enhance the application of technology, not just at the ports of entry, but also in those areas in between.[6]

To track the push for technology to protect our borders, this analysis focuses on three major issues: (1) who has the responsibility—and, perhaps more important, the money—for

border and transportation security, (2) what factors are driving the priorities for, and nature of, the technology for this mission, and (3) what technologies are being sought and bought to secure the borders.

Responsibility and Funding for Border Security

The Homeland Security Act of 2002 made the Department of Homeland Security the focal point for defending the United States against terrorist attacks. While this department has a central role and substantial funding to execute this mission, the magnitude and complexity of the task ensure that a broad network of state and local governments and private entities will continue to bear considerable responsibility—and foot much of the bill—for homeland defense.

The Department of Homeland Security

Congress subdivided the organization into "directorates" headed by five Under Secretaries: (1) Information Analysis and Infrastructure Protection, (2) Science and Technology, (3) Border and Transportation Security, (4) Emergency Preparedness and Response, and (5) Management.[7] With Under Secretary Asa Hutchinson at the helm, the Border and Transportation Security Directorate has primary—though not exclusive—responsibility for protecting the borders.[8] Other Homeland Security Department elements with border security functions and funding include the Coast Guard and the Science and Technology Directorate.

Border and Transportation Security

With an $18.1 billion budget and 108,000 employees requested for fiscal year 2004, Border and Transportation Security represents the largest of the five directorates.[9] It has four major components:

1. The Bureau of Customs and Border Protection serves as the gatekeeper to prevent illegal entry into the United States. This bureau integrates approximately 42,000 employees from the Customs Service, the Immigration and Naturalization Service, and the Animal and Plant Health Inspection Service.[10]
2. The Bureau of Immigration and Customs Enforcement operates as the interior line of defense to apprehend illegal entrants and collect customs inside the borders. This bureau brings together approximately 14,000 employees from the Customs Service, the Immigration and Naturalization Service, and the Federal Protective Service.[11]
3. The Transportation Security Administration continues its mission of protecting the transportation system,[12] although its primary focus to date has been aviation security.
4. The Office of Domestic Preparedness has "the primary responsibility within the executive branch of the Government for the preparedness of the United States for acts of terrorism."[13] Included in the office's overall responsibility is the function of "working with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support."[14] Due to its role in directing and distributing grant money to state, local, and private entities, this office has high visibility in the Homeland Security Department and in Congress.

Of the $18.1 billion sought for the Border and Transportation Security Directorate for fiscal year 2004, the Bureau of Customs and Border Protection (the gatekeeper) would get the greatest share:[15]

$6.7 billion	Bureau of Customs and Border Protection (33% increase over fiscal year 2002)
$2.8 billion	Bureau of Immigration and Customs Enforcement (16% increase over fiscal year 2002)
$4.8 billion	Transportation Security Administration (reduction from prior year)
$3.5 billion	Office of Domestic Preparedness (same as prior year)

Considerable controversy has swirled around the budgets of the Transportation Security Administration and the Office of Domestic Preparedness. The Homeland Security Department justified the slight reduction in the budget of the Transportation Security Administration for fiscal year 2004 on the basis of sizable one-time expenditures during the prior year, while Congress criticized the Transportation Security Administration for circumventing personnel ceilings and not funding "many key initiatives."[16] Congressional complaints about the Office of Domestic Preparedness cover the spectrum from a mountain of paperwork for grant applications and excessive time for funds to reach state and local governments to diversion of funds from other grant programs.[17]

The Coast Guard

Even though the Coast Guard has an obvious role in protecting our shoreline, Congress directed that the Coast Guard remain a separate and "distinct entity" reporting directly to the Secretary of Homeland Security.[18] The Coast Guard's special status reflects a congressional concern that homeland security duties not swallow its "non-homeland security missions."[19] For fiscal year 2004, the Homeland Security Department sought $6.8 billion for the Coast Guard, a 10% increase over fiscal year 2003.[20] The additional funds come in the midst of the Coast Guard's efforts to replace its aging fleet and upgrade its communications system while expanding its shoreline security duties.[21] The Coast Guard is also expanding its workforce, with 2,200 new personnel in fiscal year 2003 and 1,976 additional personnel in fiscal year 2004.[22]

Science and Technology

Although it has a broader mission than just border security, the Science and Technology Directorate has responsibility for supporting development of new technology for homeland defense; some of the new technology will have direct applications to protecting our borders.[23] For fiscal year 2004, the Science and Technology Directorate's budget includes $500 million for additional inspection technology to increase border and port security.[24] Furthermore, Homeland Security Secretary Tom Ridge announced that detection equipment for biological or chemical threats represented a near-term priority for homeland defense.[25] This directorate has multiple means for spurring new technology both internally (via the Homeland Security Advanced Research Projects Agency) and externally (in university-based centers for homeland security), as well as a Technology Clearinghouse to make such technology more readily available.[26]

State and Local Governments

With over 100,000 miles of border and shoreline to protect, state and local governments will necessarily play a critical role in homeland defense. Although the federal government will not come close to shouldering the entire bill for border security, the federal pipeline of state and local grants is bulging. In fact, not all of the funds for fiscal year 2002 have even been spent yet. If delays continue in spending fiscal year 2002 funds and distributing fiscal year 2003 funds, the fiscal year 2004 funding of Office of Domestic Preparedness grant money may create an $11 billion surge of funds to state and local governments in the near future.[27]

$2 billion	fiscal year 2002
$3.5 billion	fiscal year 2003
$2 billion	fiscal year 2003 supplemental
$3.5 billion	fiscal year 2004

Although these funds are generally designated for first responder needs of state and local government, much of the equipment bought is likely to support dual use, such as aerial surveillance or biological, chemical, or nuclear detection.[28]

The logjam of homeland security grant funding should be ready to break, as both Congress and Secretary Ridge have committed to accelerating the flow of money to state and local governments. For example, Senator Susan Collins has announced plans to introduce legislation to increase flexibility, eliminate duplicative paperwork requirements, and simplify the process.[29] Similarly, Secretary Ridge promised a one-stop shop to simplify the management and application process for state and local grants for homeland defense.[30]

Private Entities

A sizable portion of the financial burden of security will fall upon private entities. During a March 2003 congressional hearing, Secretary Ridge confirmed his view that, with the exception of aviation, the private sector should expect to absorb much of the cost of enhancing security against terrorism.[31] For example, the Virginia Port Authority expects that security enhancements—such as video surveillance equipment and electronic fencing—will cost approximately $20 million, of which only $5 million has been covered so far by a federal grant.[32]

For private concerns, security enhancements that expedite the flow of commerce represent a high priority. The Container Security Initiative seeks to push out the borders and speed the entry of goods into the United States by targeting high-risk cargo in major international ports.[33] As part of the Container Security Initiative effort, the Department of Homeland Security will be working with private companies to increase the use of “tamper-evident” containers that can zip through the security screening process. Another initiative—the Customs-Trade Partnership Against Terrorism—offers the trade community (such as importers, customs brokers, and shippers) the opportunity for expedited border processing if the company meets Customs-Trade Partnership Against Terrorism standards for procedural, physical, personnel, and conveyance security in the supply train.[34] For fiscal year 2004, the Homeland Security Department’s budget includes $62 million for the

Container Security Initiative (primarily for federal personnel in key international ports) and $18 million for the Customs-Trade Partnership Against Terrorism.[35]

Factors Driving the Technology Choices for Border Technology

For border security, technology is the future, and the future is now. During March 2003 congressional hearings, Representative Zach Wamp aptly described the technology transition now taking place:

The old security paradigm in this country of guns, gates and guards is changing fast. And technology is going to replace it all.[36]

Behind this impetus exists a broad political consensus that technological advances are essential to securing our borders, as Senator Edward Kennedy emphasized the need for the "best technology," while Senator Jon Kyl focused on the necessity of technology to cover "the vastness of the area."[37]

With limited funds and virtually unlimited demands, what are the factors driving the priorities for choosing among the many border security technologies? Although no formal roadmap generally exists for defining such priorities, congressional testimony and legislation suggest what type of technologies are most in demand for border security. The defining factors include interoperability, off-the-shelf availability, adaptability, force-multiplier capability, and legislative requirements.

Interoperability

The theme of interoperability has peppered the 2003 congressional hearings. For example, Senator Kennedy underscored not only the need for "getting the best technology," but also "having it interoperable."[38] Two areas of technology—communications and databases—have generated the most discussion regarding the requirement for interoperability. For communications, Homeland Security Secretary Tom Ridge identified interoperability as one of the "highest priorities" of his department and testified about more than $40 million being spent on demonstration projects to improve interoperable communications.[39] The Enhanced Border Security and Visa Entry Reform Act of 2002 includes specific requirements for interoperability of security databases used in making determinations for admissions to the United States.[40] Accordingly, companies looking to sell border security technology to the federal government should anticipate that interoperability will assume an increasingly important role in such procurements.

Off-the-Shelf Availability

On several occasions, Secretary Ridge emphasized his department's specific interest in "off-the-shelf" technologies "that have immediate application."[41] Such off-the-shelf products not only have the advantage of immediate availability for use against terrorism, but also may qualify as commercial items, for which the procurement process is generally far more streamlined, with fewer contract clauses, greater protection of contractor data rights, and lessened burdens for submission of cost data.[42] At least for information technology, the Homeland Security Act establishes a specific preference for use of "off-the-shelf commercially developed technologies."[43] For these reasons, off-the-shelf technology may hold an edge over developmental technology, at least in the near term as the Homeland

Security Department scrambles to protect the greatest part of the border in the least amount of time.

Adaptability

Given the span and variability of the thousands of miles of border and shoreline, "one size fits all" solutions simply will not work. In other words, the snowmobiles favored in North Dakota would be the epitome of misspent federal funds in Texas. In border security, the term "microclimate" has been used to describe the fact that state and local security needs vary widely from Hawaii to Maine to New Mexico. The technology with the flexibility to adapt to a broad array of climates and geographies offers the greatest promise for the most extensive markets.

Force-Multiplier Capability

Border and transportation security already account for more than half of the personnel in the Homeland Security Department, yet the U.S. borders could not be sealed with ten times the 108,000 employees now on the job at the Border and Transportation Security Directorate. For this reason, congressional hearings have focused upon the force-multiplying nature of technology.[44] As with productivity improvements in the private sector during the past decade, the Homeland Security Department will likely face increasing pressure to boost its own productivity levels to cover more territory with fewer people. Consequently, the technology of choice will be that with the greatest force multiplier or bang for the buck.[45]

Legislative Requirements

Congress has not shied away from giving very specific direction about what technology must be implemented for border security. For example, the Enhanced Border Security and Visa Entry Reform Act of 2002 specifically mandates the development and implementation of an interoperable law enforcement and intelligence data system (the "Chimera" system) to be used for visas, admissions, and deportations.[46] The act also requires biometric information for establishing the identity of entrants into the United States.[47] The USA Patriot Act includes requirements for technical standards for identifying visa and admissions applicants and for implementing an integrated entry and exit data system.[48] Given this level of oversight of border technology, Congress will likely continue to be a force in shaping technology decisions for homeland security.

Acquisition of Border Security Technology

For border security, the technology ranges from the mundane to the exotic. Some of the technologies now attracting the most congressional attention and homeland security dollars are biometric identification, land-based surveillance and detection, aerial surveillance and interdiction, port and shoreline security, radiation detection, and cargo security.

Biometric Information

Biometric technology offers the potential for automated identification of travelers by using distinct physiological characteristics, such as fingerprints, iris characteristics, hand geometry, or facial features. For biometric identifiers, technological hurdles remain: (1) approximately 2% of the population cannot provide usable fingerprint images; (2) even to begin large-scale testing, sufficiently large biometric databases exist only for fingerprints

and facial recognition; (3) performance of a biometric system of the size needed (100 to 200 million records) has yet to be tested, much less proven.[49]

Despite these technological challenges, Congress has mandated the use of biometric information for controlling foreign entry into the United States by October 2004.[50] The Homeland Security Department expects to implement the first phase of such a system at international airports and seaports by the end of 2003,[51] but the Attorney General has reported to Congress that other deployments will be delayed by at least a year beyond October 2004.[52] The cost for developing and implementing the biometric border control system has been estimated at $3.8 billion over the next six years.[53]

The existing system—the National Security Entry-Exit Registration System—matches biometric information (fingerprints and photographs) against a database of known terrorists and criminals.[54, 55] However, the system encountered developmental problems and will be displaced by a new system.[56] On 29 April 2003, Homeland Security Secretary Tom Ridge announced the launch of the U.S. Visitor and Immigrant Status Indication Technology (U.S. VISIT) system, which will use at least two biometric identifiers (photographs, fingerprints, iris scans) for an electronic check-in, check-out system for people coming to the United States to work, study, or visit.[57]

Land-Based Surveillance and Detection

As part of the "smart border," electronic surveillance and detection have taken a front seat in the daunting task of securing over 7,500 miles of border. For protecting the borders with Canada and Mexico, Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson explained that "in combination with [motion sensors], we have the integrated surveillance and intelligence system that has cameras on poles that are triggered by sensors that are monitored."[58] These surveillance systems include infrared surveillance scopes for enhanced detection capability.[59] On the border with Canada, the Bureau of Customs and Border Protection plans to add another 90 remote video surveillance camera systems to the existing network of 235 surveillance systems that make up the Integrated Surveillance Intelligence System.[60]

The Homeland Security Department has also identified development of "non-intrusive inspection technology" as a priority.[61] Some examples in Broad Agency Announcements released by the Technical Support Working Group are[62]

- Standoff explosive detection capability with a threshold range of 10 meters
- Remote detection of large vehicle bombs at a desired range of 400 meters
- Portable biological toxin warning sensors

Such technology will presumably be funded, at least in part, by the Homeland Security Department's Science and Technology Directorate, which has cognizance over development of new antiterrorism technology.

Aerial Surveillance and Interdiction

With the burgeoning demand for aerial surveillance, the homeland security market for helicopters has been booming. For enforcement efforts along the southern border, the Bureau of Customs and Border Protection has purchased additional A-Star and Huey helicopters.[63] Furthermore, the northern border, which had been a much lower priority

before 11 September 2001, has seen the deployment of additional helicopters.[64] Homeland Security Secretary Tom Ridge has authorized use of the Coast Guard's Helicopter Interdiction Tactical Squadron for coastal homeland security missions. The squadron's MH-68 helicopters mounted with precision-guided machine guns will enforce security zones around tankers, provide aerial protection for naval vessel zones, and control restricted waterfront areas.[65, 66]

In addition to helicopters, Under Secretary Hutchinson has identified remotely piloted aerial surveillance vehicles, or drones, as a technology for border security.[67] 67 Drone technology appears well suited to the vast wilderness and myriad logging roads along the northern border, particularly during inclement weather that might ground piloted aircraft. Given the well-publicized successes of remotely piloted aircraft in Afghanistan and Iraq, such technology will likely be a high priority in the near future for border surveillance.

Port and Shoreline Security

With airport and border security taking precedence, port security has lagged, as Congress found that "ports are often very open and exposed and are susceptible to large scale acts of terrorism that could cause a large loss of life or economic disruption."[68] Indeed, a 2002 war game concluded that a dirty bomb attack shutting down ports for a week would drain $58 billion from the nation's economy.[69] During fiscal year 2003, approximately $217 million in grants began flowing toward port security assessments, preliminary improvements, and training.[70]

For port security, the technology runs the gamut from low-tech to high-tech: electronic fencing, improved lighting, video-surveillance equipment, radiation detection devices, and biometric identification cards.[71] The Coast Guard has boosted its capability for harbor security with a $140 million contract in April 2003 for up to 700 *Defender*-class harbor patrol boats armed with machine guns.[72] With $500 million in the fiscal year 2004 budget for the Deepwater program, the Coast Guard will continue upgrading its fleet with new vessels for port and shoreline security.[73] Similarly, the Coast Guard will be acquiring new computer hardware and software for its Maritime Domain Awareness program to develop and improve the information architecture for obtaining, processing, and sharing intelligence data.[74]

Radiation Detection

Given the potentially catastrophic impact of a nuclear attack, radiation detection has maintained a high priority for border and port security. As of May 2003, the Border and Transportation Directorate had distributed 15,000 handheld radiation detectors to supply every border inspector in the nation.[75] In addition, the directorate is fielding $45 million in non-intrusive inspection systems for detecting radioactive isotopes and other potential threats.[76] One such system, the $100,000 Radiation Isotope Identification Device—now fielded to screen truck-board cargo at ports—is so sensitive that it can detect a driver who recently received medical radiation treatment.[77] Furthermore, the Science and Technology Directorate has developed technical standards for the performance and testing of radiation detection equipment.[78] This directorate's Broad Agency Announcement in May 2003 sought a host of proposals for such technology as a "Standoff Maritime Radiological Gamma/Neutron Detector" and "Real-Time Radioisotope Identification and Reporting."[79]

Cargo Security

Every day, 21,000 cargo containers enter U.S. ports, yet only 4% of them get inspected.[80, 81] The Homeland Security Department is implementing programs such as Operation Safe Commerce, the Container Security Initiative, the Automated Commercial Environment, and the Customs-Trade Partnership Against Terrorism to target high-risk cargo while expediting the rest of the freight. As part of these initiatives, "smart" containers will include Global Positioning System technology to track the cargo as well as light and magnetic sensors to detect tampering with, or intrusions into, the container during shipment.[82] In addition to this initiative, mobile portals using gamma rays and Geiger counters are "powerful enough to spot anomalies within containers, including humans hiding inside."[83] However, the $1 million pricetag on these mobile portals has limited their deployment.

Conclusion

Ironically, the immensity and diversity of the United States—the engine that powers much of our economic success—has proven to be a liability in the effort to maintain border security. The challenge of securing 7,500 miles of border and 95,000 miles of shoreline is simply too great to be overcome with more "guns, gates and guards." Instead, the United States must press its edge in technology to find and field solutions that secure the borders without busting the budget.

References

Click on an end note number to return to the article.

1. Department of Homeland Security website, Border & Transportation Security page.

2. Statement of Rep. Harold Rogers, hearing on border security, House Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 27 March 2003.

3. Judi Hasson, "Despite Technology, Cargo Vulnerable," *Federal Computer Week*, 20 March 2003.

4. Nancy Kingsbury, General Accounting Office Managing Director of Applied Research and Methods, "Border Security: Challenges in Implementing Border Technology" (GAO-03-546T), testimony before the Senate Judiciary Committee, Subcommittees on Terrorism, Technology, and Homeland Security and on Border Security, Immigration, and Citizenship, 2 March 2003.

5. Homeland Security Act of 2002, Public Law 107-296, sec. 402(8), 116 Stat. 2178, 25 November 2002.

6. Statement of Sen. Jon Kyl, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003," Senate Judiciary Committee, Subcommittees on Terrorism, Technology, and Homeland Security and on Border Security, Immigration, and Citizenship, 108th Congress, 1st Session, 12 March 2003.

7. Public Law 107-296, secs. 103(a), 201, 301, 401, 501, and 701.

8. Ibid., sec. 402.

9. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, hearing on the fiscal year 2004 budget overview—Border and Transportation Security, Senate Judiciary Committee, Subcommittee on Homeland Security, 108th Congress, 1st Session, 6 May 2003.

10. Ibid.; see also the Department of Homeland Security website, "DHS Organization" page.

11. Ibid.; see also the Bureau of Immigration and Customs Enforcement website.

12. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, hearing on the fiscal year 2004 budget overview.

13. Public Law 107-296, sec. 430(c).

14. Ibid.

15. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, hearing on border security, House Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 27 March 2003.

16. Statement of Rep. Harold Rogers, hearing on transportation security, House Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 27 March 2003.

17. Statements of Sens. Susan Collins, Joseph Lieberman, Carl Levin, and Daniel Akaka, hearing on "Investing in Homeland Security: Streamlining and Enhancing Homeland Security Grant Programs," Senate Governmental Affairs Committee, 108th Congress 1st Session 1 May 2003.

18. Public Law 107-296, sec. 888.

19. Ibid.

20. Statement of Homeland Security Secretary Tom Ridge, hearing on fiscal year 2004 homeland security appropriations, House Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 20 March 2003.

21. Statement of Coast Guard Commandant Admiral Collins, hearing on homeland security, Senate Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 1 May 2003.

22. General Accounting Office, "Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department" (GAO-03-467T), testimony before the Senate Commerce, Science, and Transportation Committee, Oceans, Atmosphere, and Fisheries Subcommittee, 12 February 2003, p. 9.

23. Public Law 107-296, sec. 302.

24. Statement of Sen. Jon Kyl, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

25. Statement of Homeland Security Secretary Tom Ridge, hearing on fiscal year 2004 homeland security appropriations.

26. Public Law 107-296, secs. 307, 308, and 313.

27. Statements of Rep. Harold Rogers and Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, hearing on border security.

28. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, hearing on border security.

29. Statement of Sen. Susan Collins, hearing on "Investing in Homeland Security: Streamlining and Enhancing Homeland Security Grant Programs."

30. Statement of Homeland Security Secretary Tom Ridge, hearing on fiscal year 2004 homeland security appropriations.

31. Ibid.

32. Garry Kranz, "Port Security Tightens," *Virginia Business*, May 2003, p. 26.

33. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, "Cargo Containers: The Next Terrorist Target?" Senate Governmental Affairs Committee hearing, 108th Congress, 1st Session, 20 March 2003.

34. Ibid.

35. Department of Homeland Security Budget in Brief, p. 7.

36. Statement of Rep. Zach Wamp, hearing on fiscal year 2004 homeland security appropriations, House Appropriations Committee, Homeland Security Subcommittee, 108th Congress, 1st Session, 20 March 2003.

37. Statements of Senators Edward Kennedy and Jon Kyl, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003," Senate Judiciary Committee, Subcommittees on Terrorism, Technology, and Homeland Security and on Border Security, Immigration, and Citizenship, 108th Congress, 1st Session, 12 March 2003.

38. Statement of Sen. Kennedy, ibid.

39. Statement of Homeland Security Secretary Tom Ridge, hearing on "Investing in Homeland Security: Streamlining and Enhancing Homeland Security Grant Programs."

40. Public Law 107-173, sec. 302.

41. Statement of Homeland Security Secretary Tom Ridge, hearing on fiscal year 2004 homeland security appropriations.

42. Federal Acquisition Regulations, secs. 12.301, 12.211, and 15.403-1(b).

43. Public Law 107-296, sec. 509.

44. Statement of Sen. Jon Kyl, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

45. As Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson stated, "We cannot be everywhere at once. But technology such as this [US VISIT system], used properly, can multiply our force strength and effectiveness many times over"—Office of the Press Secretary for Homeland Security, "Remarks by Under Secretary Asa Hutchinson at the Economic Development Administration's Annual Conference," 7 May 2003.

46. Public Law 107-173, sec. 202.

47. Ibid., sec. 302.

48. Public Law 107-56, sec. 414.

49. Nancy Kingsbury, "Border Security: Challenges in Implementing Border Technology."

50. Public Law 107-173, sec. 302; Public Law 107-56, sec. 403.

51. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security," 29 April 2003.

52. Nancy Kingsbury, "Border Security: Challenges in Implementing Border Technology," p. 10.

53. Ibid., p. 11.

54. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

55. Sara Michael, "Border Tech Advances Highlighted," *Federal Computer Week*, 12 March 2003, p. 2.

56. Judi Hasson, "Ridge Announces VISIT System," *Federal Computer Week*, 29 April 2003, p. 1.

57. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security."

58. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

59. Ibid.

60. Judi Hasson, "DHS Adding Cameras to Borders," *Federal Computer Week*, 21 April 2003, p. 1.

61. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

62. Homeland Security Department, Technical Support Working Group website.

63. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security."

64. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

65. Office of the Press Secretary for Homeland Security, "Armed Coast Guard Helicopters to Be Used for Homeland Security," 1 May 2002.

66. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security."

67. Statement of Under Secretary of Homeland Security for Border and Transportation Security Asa Hutchinson, joint hearing on "Border Technology: Keeping Terrorists Out of the United States—2003."

68. Maritime Transportation Security Act of 2002, Public Law 107-295, sec. 101 (7).

69. Garry Kranz, "Port Security Tightens," p. 25.

70. General Accounting Office, "Combatting Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports" (GAO-03-15), report to the Chairman of the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, October 2002, p. 11.

71. Garry Kranz, "Port Security Tightens," p. 26.

72. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security."

73. Homeland Security Department Press Office, DHS Organization, "Fiscal Year 2004 Budget Fact Sheet," 3 February 2003.

74. Statement of Coast Guard Commandant Admiral Collins, hearing on homeland security.

75. Office of the Homeland Security Press Secretary, "Remarks by Under Secretary Asa Hutchinson at the Economic Development Administration's Annual Conference," 7 May 2003, p. 7.

76. Ibid.

77. Garry Kranz, "Port Security Tightens," p. 26.

78. Office of the Press Secretary for Homeland Security, "First 100 Days of Homeland Security."

79. Homeland Security Department, Technical Support Working Group website.

80. Judi Hasson, "Despite Technology, Cargo Vulnerable."

81. Megan Lisagor, "Operation Safe Commerce Advancing," *Federal Computer Week*, 16 April 2003, p. 2.

82. Statement of Mr. Hall, Senate Governmental Affairs Committee hearing, 108th Congress, 1st Session, 20 March 2003.

83. Garry Kranz, "Port Security Tightens," p. 28.