THE CLAUSE

Nov- Dec. 2003

A Quarterly Publication of the Boards of Contract Appeals Bar Association

Vol. XIV,
Issue 4

TABLE OF CONTENTS

Board of Governors

President:
Elaine A. Eder
US Coast Guard (G-LPL)
2100 Second Street, SW
Washington, DC 20593
202-267-1544

Vice-President:
Joseph McDade
USAF Office of General Counsel
1740 Air Force, Pentagon
Washington, DC 20330-1740
703-697-3900

BOARDS OF CONTRACT APPEALS BAR ASSOCIATION

2099 Pennsylvania Avenue, NW
Washington, DC 20006

WWW.BCABAR.ORG

Secretary:
Leigh A. Bradley
Holland & Knight
2099 Pennsylvania Ave., NW
Washington, DC 20006-6801
202-419-2444

Treasurer:
Thomas H. Gourlay, Jr.
COE Office of Counsel
441 G Street, NW
Washington, DC 20548
202-761-8542

Dec 25, 2003

After very useful and informative Annual Meeting presentations last October, we have been able to get off to a terrific start this service year! And for that, I thank many people in our organization. Our immediate past president, Dick Gallivan (Navy Litigation Office), did a tremendous amount of work on many issues, including enhanced web site features and practical guidance pertaining to e-filing. Dick took us significantly forward during his tenure over the past year, and his tact and steady leadership set us on a clear path to move successfully ahead.

As I extend thanks to Dick, I must also thank:

Jim Nagle (Oles, Morrison, Rinker & Baker) for chairing our 2003 annual meeting – with special gratitude to his panel chairs Liz Fleming (Trout & Richards), Jim McCullough (Fried Frank) and Hugh Long (USAF);

David Metzger (Holland & Knight) for his continuing work in chairing the highly regarded Executive Policy Forum;

David Fowler (Raytheon) for chairing the much appreciated Trial Practice Committee;

the Board of Governors for their dedication and all their efforts on behalf of the BCABA; and

our Gold Medal firms for their strong and continuing support.

Finally, very special thanks are extended to two sustaining forces in the growth and evolution of the organization: Hugh Long and Peter McDonald (McGladrey & Pullen). Hugh serves our indefatigable editor of *The Clause*, and Pete has always shown unparalleled energy, enthusiasm and support for the organization and all its members.

All these contributions made it possible for me to propose at our first Board of Governor's meeting for this year that the BCABA develop and implement a long-range strategic planning process and plan. With those, we can be confident that our organization will continue to provide superb service and benefit for our members and the broad government contracting community into the future. Within the context of what BCAs are, what they do, and how they do it, we will emphasize responsive and proactive actions for the BCABA's purposes of promoting just, efficient, and effective practice of government contract law and BCA litigation. Pete McDonald, Dave Metzger, and Joe McDade (USAF OGC) are working as a core team to address this initiative.

In the meantime, I look forward to talking and meeting with many of you and to ensuring BCABA programs and activities serve our practice area well now and into the future.

Sincerely, Elaine A. Eder
President

EDITOR'S COLUMN

Let me thank every one for their help at the Annual Meeting .In this issue we have several fine articles .by Dave Bodenheimer, David P. Metzger, John P. Rowley III Jennifer A. Short, Stuart Young, and Paul Pompeo. These timely and informative articles on Homeland security, Teaming Agreements, and Independent Research and Development are of great value to our readers and to this magazine.

There was no time to get a Treasurer's Report, however, Alan Gourlay tells me we have plenty of money in the bank. . MERRY CHRISTMAS, especially for our heroic and skilled soldiers in Central and South West Asia.

HOMELAND SECURITY NOW AND LATER: EMERGING ISSUES AND NEW PERILS IN CONTRACTING

David Z. Bodenheimer[1]

> "A new government department does not spring, like Athena from the brow of Zeus, full blown and ready for action." James Schlesinger, July 10, 2003.

Perhaps it would have been easier if the Homeland Security Department had been birthed from Zeus' brow amidst warring factions, arbitrary Greek gods, and tasks of Herculean proportions. The Department confronts essentially the same challenges, but must do so in its infancy: cleaning up inherited messes from predecessor agencies (the Augean stables), threading the needle between warring Congressional committees (Hera versus Zeus), and battling terrorism (the Hydra), but only if done in the "right" way.[2] Just as Hercules sought help in performing his twelve Labours, the Homeland Security Department depends heavily upon private industry for the technology, support, and

---

1 David Z. Bodenheimer is a partner in the Washington, D.C., office of Crowell & Moring LLP where he specializes in Government Contracts and Homeland Security matters, including chemical/biological protection, border security and technology, and the SAFETY Act. He may be reached at (202) 624-2713 or dbodenheimer@crowell.com.

2 In assigning two additional "Labours" to Hercules, Eurystheus contended that improper shortcuts had been taken in killing the Hydra (calling for Iolaus' help) and cleaning the Augean stables (diverting the two rivers).

expertise to fulfill its many-headed missions. For this reason, the Department's problems will often become industry's problems.

During its inaugural year, the Homeland Security Department has hewed its way through a host of knotty issues, some of which arose out of the largest federal government reorganization in 50 years, while others sprang from the multiple – sometimes conflicting – missions of balancing anti-terrorism safeguards against budget constraints, individual rights, and efficient flow of trade. Despite progress, major issues remain. Both the Department and industry can expect to face emerging issues, opportunities, and pitfalls in the following areas:

1) Sharing Information
2) Moving Goods
3) Protecting Secrets
4) Spreading Technology
5) Forging Interoperability
6) Going Global
7) Funneling Funds to State & Local Governments
8) Tapping Private Funds
9) Avoiding Political Fallout
10) Finding the Right Person and Rule

Sharing Information

For the Homeland Security Department, few tasks have higher visibility or priority than receiving, coordinating, and sharing information.

The Mandate for Sharing Information

Since Pearl Harbor, the risks of not sharing information in a timely and effective manner have been well known. To this end, the Homeland Security Act of 2002 (Pub. L. No. 107-296, § 201(d)(1)) requires the Department to access, receive, analyze, and integrate "law enforcement information, intelligence information, and other information" from federal, state, and local governments and private sector entities. The General Accounting Office (GAO) recently summed up this core mission:

> To accomplish this [anti-terrorism] mission, the act established specific homeland security responsibilities for the department and directed it to coordinate its efforts and share information within DHS and with other federal agencies, state and local governments, the private sector, and other entities. This information sharing is critical to successfully addressing increasing threats and fulfilling the mission of DHS.[3]

---

3 *GAO, "Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues," p. 12 (Sept. 17, 2003) (GAO-03-1165T) (www.gao.gov).*

However, Congress recognized that unfettered information sharing posed other risks that the Department must weight in fulfilling its charter.

Privacy Issues in Information Sharing and Gathering

Balanced against this mandate for gathering and sharing information, the Homeland Security Act required the Department to "establish procedures" to "protect the constitutional and statutory rights of any individuals who are the subjects of such information" and to appoint a Privacy Officer responsible for "privacy policy" and protecting privacy rights. Pub. L. No. 107-296, §§ 221(3), 222. In the Homeland Security arena, both the Department and contractors may encounter privacy issues in a number of contexts.

Electronic Privacy

As illustrated by the Congressionally-mandated demise of the Total Information Awareness (TIA) program for collecting and analyzing public and private data,[4] privacy has been a hot-button issue in the Homeland Security arena. Electronic data systems represent a linchpin for collecting, storing, and sharing data, but such systems may trigger Privacy Act coverage. 5 U.S.C. § 552a. Such privacy requirements may apply not only to government agencies, but also to the contractors operating such systems. *See* 5 U.S.C. § 552a(m)(1) (applicability to government contractors). Indeed, the Federal Acquisition Regulation (FAR) warns of the possibility of criminal penalties for Privacy Act violations:

> An agency officer or employee may be criminally liable for violations of the Act. When the contract provides for operation of a system of records on individuals, contractors and their employees are considered employees of the agency for purposes of the criminal penalties of the Act.

As a result, both the Department and contractors must be attuned to privacy issues that may arise out of electronic systems that collect, store, or share personal information potentially subject to federal or state privacy restrictions.

Physical Privacy

With so much territory to cover, agencies are looking at remotely piloted vehicles and blimps for aerial surveillance. For example, Under Secretary Hutchinson testified before Congress about the Department's specific interest in unmanned surveillance vehicles, or drones, as a potential technology for border security.[5] Similarly, a sensor-

---

4 Fiscal Year 2004 Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131 (prohibiting funds for TIA except for foreign counterterrorism intelligence).

5 *Border Technology: Keeping Terrorists Out of the United States – 2003: Joint Hearings Before the Senate Subcomm. on Terrorism, Technology, and Homeland Security and Border Security, Immigration, and Citizenship,* 108th Cong., 1st Sess. (Mar. 12, 2003) (statement of Under Sec. Hutchinson) (hereafter *Senate Border Technology Hearings*).

packed blimp has recently floated over Manassas, Virginia to test aerial surveillance capabilities for Homeland Security missions.[6] Such potential surveillance has not been without controversy: "Civil libertarians expressed concern that the blimps will be another government tool that infringes on privacy." [7] As a result, privacy issues will inevitably become tangled with Homeland Security programs involving such surveillance.

International Privacy

Some of the U.S. anti-terrorism requirements may collide head-long with international privacy laws: "The Europeans say the use of extensive information on passengers violates privacy laws."[8] The European Data Protection Directive has been a major factor in driving international privacy protection: "Existing privacy and data protection laws in many countries impose criminal sanctions, including unlimited fines and imprisonment, for non-compliance with elements of their legislation."[9] Given that Homeland Security cannot succeed without international cooperation, the Department and industry must navigate foreign privacy rules that may be compromised by certain data collection and sharing practices employed in the fight against terrorism.

Moving Goods

Controlling cargo has drawn increasing scrutiny among the many gargantuan tasks required for securing the border.

The Mandate For Securing The Border

As one of its primary missions, the Department has the responsibility for "Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States," as well as "Preventing the entry of . . . instruments of terrorism into the United States." Pub. L. No. 107-296, § 402. However, the task of stopping terrorism must not choke off trade, as the Department must balance the countervailing responsibility of "ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce." *Id.*

The Magnitude of the Task and the Risks

With 95,000 miles of shoreline and 7,500 miles of border circumscribing the U.S., the job of securing the border is daunting. Every day, 21,000 foreign containers enter the

---

6 Vogel, "Military Has High Hopes for New Eye in the Sky: Sensor-Equipped Blimps Could Aid Homeland Security," *Washington Post*, p. B1 (Aug. 8, 2003).

7 Associated Press, "U.S. Navy May Use Blimps as Anti-Terror Tool" (Aug. 7, 2002) (www.foxnews.com).

8 Knight, "Some Air Carriers in Europe Skirt Antiterror Steps," *The Wall Street Journal,* p. D10 (Sept. 24, 2003).

9 "The Need for Compliance," *Expertise. Privacy & Data Protection* (www.crowell.com).

United States, but only 2 percent are inspected.[10] The consequences of an undetected, bomb-laden container could be catastrophic:

> For example, in May 2002, the Brookings Institution estimated that costs associated with U.S. port closures resulting from a detonated WMD [weapons of mass destruction] could amount to $1 trillion. Estimating the cost of discovering an undetonated WMD at a U.S. seaport, Booz, Allen and Hamilton reported in October 2002 that a 12-day closure would cost approximately $58 billion.[11]

Single-handedly, Charles McKinley illustrated how porous and vulnerable the cargo chain is by packing himself inside a wooden crate and shipping himself as human cargo from Brooklyn, New York to Dallas, Texas to save airfare.[12]

At the same time, international trade continues as the economic lifeblood for the U.S. economy, with United States trade in 2000 with its Canadian and Mexican neighbors alone accounting for $653 billion.[13] By 2006, international trade volume with all countries will top $2 trillion.[14] As Secretary Ridge explained, the specter of terror must not stop the wheels of trade from rolling:

> [W]e could pass regulations that would so tightly constrict legitimate trade and commerce that our economy would slow to a crawl. Yes, such rules might prevent a terrorist attack someday, but such rules would also cause economic dislocation and disruption every day, literally in every corner of the globe. To cripple our economy without firing a shot, that's not just counterproductive, that's a terrorist's dream, and that should be our nightmare.[15]

---

10 Hasson, "Despite Technology, Cargo Vulnerable," *Federal Computer Wee* (Mar. 20, 2003); Lisagor, "Operation Safe Commerce Advancing," *Federal Computer Week*, at 2 (Apr. 16, 2003) (www.fcw.com/fcw/articles/2003).

11 GAO, "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors," p. 8 (July 2003) (GAO-03-777) (www.gao.gov/homelandsecurity).

12 Power, "Bush Seeks Tougher Curbs on Airline Cargo," *Wall Street Journal*, p. A4 (Sept. 22, 2003).

13 GAO, "Border Security: Challenges in Implementing Border Technology," p. 9 (Mar. 12, 2003) (GAO-03-546T) (www.gao.gov/homelandsecurity).

14 GAO, "Homeland Security: Challenges Facing the Department of Homeland Security in Balancing its Border Security and Trade Facilitation Missions," p. 6 (June 16, 2003) (GAO-03-902T) (www.gao.gov/homelandsecurity).

15 Press Release, "Remarks by Secretary of Homeland Security Tom Ridge at the Custom and Border Protection Trade Symposium," p. 2 (Nov. 20, 2003) (www.dha.gov/dhspublic/display?content=2324).

Moving the Cargo

The Homeland Security has initiated a number of programs to keep the terrorists out, but the cargo moving. Technology also promises to play a major role in maintaining cargo security through electronic seals, tamper-proof containers, GPS tracking systems, non-intrusive inspection devices, and biometric security controls.

Container Security Initiative

The Container Security Initiative (CSI) seeks to push out the borders by placing Customs staff at high-volume foreign ports to screen containers for WMD. Through use of the Automated Targeting System, the CSI team of United States and foreign inspectors screen container data and identify high-risk cargo to be subjected to inspection. At a minimum, such foreign ports must have the non-intrusive inspection equipment to perform such inspections. The CSI budget increases from $4.3 million in 2002 to $61.2 million in 2004.[16]

Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism (C-TPAT) focuses upon improving the global supply chain through security in the private sector. By agreeing to certain security measures, companies may be able to expedite their cargo through the transportation system. The C-TPAT budget rises from $8.3 million in 2002 to $12.1 million in 2004.[17]

Automated Commercial Environment

The Automated Commercial Environment (ACE) will replace the existing Customs system for tracking, controlling, and processing all commercial goods imported into, or exported out of, the U.S. The system is expected to cost $1.7 billion.[18]

Protecting Secrets

From intelligence data to SAFETY Act applications to critical infrastructure information, the Department will stand atop a treasure trove of trade secrets and national security intelligence.

---

16 GAO, "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors," pp. 2, 9-10 (July 2003) (GAO-03-770) (www.gao.gov/homelandsecurity).

17 *Id.*, pp. 3, 14, 17.

18 GAO, "Homeland Security: Challenges Facing the Department of Homeland Security in Balancing its Border Security and Trade Facilitation Missions," p. 7 (June 16, 2003) (GAO-03-902T) (www.gao.gov/homelandsecurity).

The Mandate to Collect and Protect Data

In an effort to centralize data, the Homeland Security Act requires that the Department have access to "all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States" and "all information concerning infrastructure and other vulnerabilities." Pub. L. No. 107-296, § 202(a). For SAFETY Act applications, the Act includes provisions for contractors' submissions of "safety and hazard analyses" and other information relating to anti-terrorism technology. *Id.*, § 863(d).

In some instances, the Act includes express protections for such information. *Id.*, § 214(a) (protection for critical infrastructure information); § 892(e) (federal control of information shared with state and local governments). However, the Act does not carve out specific protection for many other types of information to be submitted, such as SAFETY Act applications.

Cyber Risks to Information

Breaches of cyber security, such as hacking, have skyrocketed in recent years, with an 800-percent increase in reported "computer security incidents" from 1999 to 2002, with further dramatic rises in the first two quarters of 2003.[19] In one instance, a British computer administrator "used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks."[20] Notwithstanding such risks, GAO found significant and "widespread" deficiencies in information security within federal agencies.[21]

Managing Cyber Risks

For contractors, cyber risks have at least two implications. First, the Department will necessarily need technology and support to protect and harden electronic data systems from cyber attacks. Second, contractors must weigh legal options in the event that trade secrets spill into the public domain.

Technology Solutions

As the pace and sophistication of cyber attacks increase, the technology for cyber security must rapidly and substantially improve. A host of technologies and standards have been funded and developed for this task:

> The [cyber security] programs have been in three generations. The first generation is to prevent intrusions

---

19 GAO, "Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues," p. 7 (Sept. 17, 2003) (GAO-03-1165T) (www.gao.gov/homelandsecurity).

20 GAO, "Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD," p. 7 (July 24, 2003) (GAO-03-1037T) (www.gao.gov/homelandsecurity).

21 *Id.*, p. 1.

> and there have been a number of successes that have come out of this, including several sets of cryptographic tools, access control and multiple levels of security.
>
> In the second generation, if intrusions happen, how does one detect them and how does one limit damage? Examples of successful products, which came out of this, are firewalls, boundary controllers, intrusion detection systems, virtual private networks and a public key infrastructure.
>
> In the third generation, which we're now in the midst of, the goal is to operate through attacks and these goals are intrusion tolerance and graceful degradation. In my opinion, this is the space that we need to be in to able to have critical infrastructure systems that can weather attacks.[22]

Cyber security research priorities include systems that can modify themselves "on-the-fly" and coordinate information with other networks while under attack. Similarly, high-bandwidth, secure, digital communications systems generate a host of cyber security challenges when multiple organizations at many tiers must be interconnected.[23]

Legal Options

Outside of the cyber world, a contractor occasionally has advance notice of an impeding release of its trade secrets into the public domain. In such cases, the contractor may have rights to seek injunctive relief or to pursue administrative remedies.[24] In contrast, such secrets can be thrust into the public domain in a nanosecond by a breach of cyber security. In the event that the Government fails to take proper steps to safeguard such trade secrets, the contractor may have a damages remedy against the Government.[25] However, these waters are largely uncharted, leaving both the Government and contractor exposed to potentially substantial risks involving improper releases of trade secrets.

Spreading Technology

---

22 *Cybersecurity: Getting It Right: Hearings Before the House Subcomm. on Cybersecurity, Science, Research and Development,* 108th Cong., 1st Sess. (July 22, 2003) (statement of Dr. Sastry).

23 *Id.* (statement of Mr. Wolf, NSA Director of Information Assurance).

24 *Megapulse, Inc. v. Lewis,* 672 F.2d 959 (D.C. Cir. 1982) (injunctive relief); FAR § 52.227-14(e) (administrative protection for technical data).

25 *See, e.g., Ruckelshaus v. Monsanto,* 467 U.S. 986 (1984).

Nearly everyone agrees that technology is critical to the Homeland Security mission: "The old security paradigm in this country of guns, gates and guards is changing fast. And technology is going to replace it all."[26]

The Mandate to Develop and Deploy Technology

Technology represents a core asset that the Department must direct, fund, and conduct "national research, development, test and evaluation, and procurement of technology and systems" for fighting terrorism. Pub. L. No. 107-296, § 302. The Department has multiple arms to accomplish this mission:

- Federally Funded Research & Development Centers (§ 305)
- Homeland Security Advanced Research Projects Agency (§ 307)
- University Based Centers for Homeland Security (§ 308)
- Department of Energy National Laboratories (§ 309)
- Homeland Security Institute (§ 312)
- Technology Clearinghouse (§ 313)

Factors Driving Technology

For Fiscal Year 2004, the Information Analysis and Infrastructure Directorate receives $893 million, while the Science and Technology Directorate operates on a budget of $918 million, of which $874 million is directed to research, development, and acquisition.[27] Some of the key factors driving how the Department will spend such money include: (1) off-the-shelf availability; (2) force-multiplier capability; and (3) statutory requirements.

Off-the-Shelf Availability

In testimony before Congress, Secretary Ridge has emphasized his interest in technologies "that have immediate application."[28] Assistant Secretary McQueary recently stated that the Homeland Security Advanced Research Projects Agency (HSARPA) would give priority to existing technology:

> Perhaps 90 percent of HSARPA's efforts are focused on improving existing technologies that can be developed and deployed to the commercial sector quickly, while the

---

26 *Fiscal Year 2004 Appropriations: Homeland Security: Hearings Before the House Subcomm. On Homeland Security of the Appropriations Comm.*, 108th Cong., 1st Sess. (March 20, 2003) (statement of Rep. Wamp).

27 "Homeland Security Appropriations," *Congressional Quarterly Action Report No. 108-6*, pp. 12-13 (Sept. 24, 2003).

28 *Fiscal Year 2004 Appropriations: Homeland Security: Hearings Before the House Subcomm. on Homeland Security of the Appropriations Comm.*, 108th Cong., 1st Sess. (Mar. 20, 2003) (statement of Sec. Ridge).

> remaining 10 percent address revolutionary long-range research for breakthrough technologies.[29]

During his confirmation hearing for the position of Assistant Secretary (Plans, Programs and Budget) in the Science and Technology Directorate, Dr. Penrose Albright also underscored a preference that "we rapidly field available technology where it is cost effective to do so" and "provide upgrades using near-term technologies available from the labs and private sector."[30] Accordingly, these public statements of senior Homeland Security officials leave little doubt that off-the-shelf technology will have an inside track for many of the Department's purchases.

Force-Multiplier Capability

Doing more with less has been a theme during many Congressional hearings. With 95,000 miles of shoreline and 7,500 miles of land borders, the Department will never have enough people to guard every entry point without the help of technology.

> [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.[31]

For this reason, Congress focused upon "the force multiplying nature of technology."[32] Similarly, some components of the Department, such as TSA, are under Congressional pressure to reduce personnel, while upgrading technology. According to the chairman of the House Transportation and Infrastructure Subcommittee on Aviation, "TSA has spent too much money on salaries and personnel at the expense of technology."[33] For these reasons, technology that increases productivity, while keeping trade moving, will be at a premium for the Homeland Security mission.

Legislative Requirements

Legislation drives some of the technology choices. For example, the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. No. 107-173, § 302) establishes biometric requirements for screening foreign visitors. Similarly, the USA Patriot Act (Pub. L. No. 107-56, § 414) provides for the development of technical

---

29 DHS Press Release, "Remarks by Dr. Charles McQueary Before the 7th Annual Executive Symposium on Emerging Business Opportunities in Photonics," p. 2 (Nov. 13, 2003) (www.dhs.gov/dhspublic).

30 *Homeland Security and OMB Nominations: Hearings Before the Senate Governmental Affairs Comm.*, 108th Cong., 1st Sess. (July 29, 2003) (statement of Dr. Albright).

31 *Senate Border Technology Hearings,* (Sen. Kyl).

32 *Id.*

33 Strohm, "House chair urges TSA to spend less on people, more on technology," *Government Executive Magazine,* (Nov. 24, 2003) (www.govexec.com).

standards for the entry and exit system. For information technology, the Homeland Security Act (Pub. L. No. 107-296, § 509) includes a preference for off-the-shelf equipment.

Intellectual Property Rights

In recent announcements, the Department has touted its Other Transactions authority ("to license intellectual property – but not own it") and the Small Business Innovation Research (SBIR) program as being contractor-friendly means for protecting intellectual property rights.[34] Furthermore, to the extent that the Department proceeds with giving priority to buying off-the-shelf equipment, the FAR establishes a presumption that such commercial items have been developed exclusively at private expense, thus according substantial protection to the contractor's technical data rights. *See* FAR § 12.211.

Forging Interoperability

Without interoperability, much of the technology and intelligence data may be wasted.

The Mandate for Interoperability

Bipartisan support exists for interoperability. For example, Senator Kennedy emphasized the importance not only for "getting the best technology," but also "having it interoperable."[35] Secretary Ridge described interoperability as one of the "highest priorities" of his department.[36] In addition, the Enhanced Border Security and Visa Entry Reform Act of 2002 specifies the development and implementation of an interoperable law enforcement and intelligence data system for visas, admissions and deportations. Pub. L. No. 107-173, § 202.

History supports the need for interoperability, as one of the firefighters testified before Congress:

> After the 1993 attack on the World Trade Center, evaluations conducted by emergency planning organizations identified lack of communication between police helicopters and the incident commander as a significant impediment to effective response. Tragically,

---

34 *See* DHS Press Releases, "Remarks of Dr. Charles McQueary Before the 7th Annual Executive Symposium on Emerging Business Opportunities in Photonics" (Nov. 13, 2003) and "HSARPA Issues Solicitation Seeking Research Proposals from Small Businesses" (Nov. 14, 2003) (www.dhs.gov).

35 *Senate Border Technology Hearings,* (statement of Sen. Kennedy).

36 *Investing in Homeland Security: Streamlining and Enhancing Homeland Security Grant Programs: Hearings Before the Senate Comm. on Governmental Affairs,* 108th Cong., 1st Sess. (May 1, 2003) (statement of Sec. Ridge) (hereinafter "*Senate Investing in Homeland Security Hearings*").

> this exact same lack of communication hindered our response on September 11th.[37]

Given the legislative, management, and practical impetuses behind interoperability, both the Department and contractors face Herculean challenges in connecting divergent systems not only between federal agencies, but with state, local, and private entities as well.

Practical Challenges to Interoperability

As a practical matter, a considerable gulf separates the ideal and the actual implementation of interoperability. For example, if the schedule drags out while two federal agencies dicker over the details of interface requirements, how will the cost and risk be allocated under the contract for making two disparate systems interoperable? As the number of parties multiply, the challenge for interoperability will likely grow exponentially. For example, the Integrated Wireless Network "will create interoperability among local, State and Federal public safety agencies in 25 cities."[38] Under these circumstances, the difference between a well-managed, on-time, successful project and a costly, endless disaster may well depend upon how well the parties nail down the interfaces and requirements in the beginning.

Going Global

Although Homeland Security is primarily a domestic mission, the border and transportation functions necessarily involve international matters.

International Cooperation

The US VISIT "program will use photographs and fingerprints to log entries and exits at major U.S. airports and seaports."[39] A similar Canadian system will link Canada's law enforcement system and its overseas ports, allowing users "to share information with the United States to protect the common border: "Officials from both nations now must ensure the systems are interoperable – a task complicated by the differing technical standards that the countries use."[40] Thus, the need for foreign agreement and interoperability will raise the bar of difficulty for both the Department and contractors involved in such international ventures.

Pushing Out the Borders

---

37 *Senate Investing in Homeland Security Hearings,* (statement of Capt. Bowers).

38 *Strength Through Knowledge: Hearings Before the House Subcomm. on Cyber Security, Science and Research and Development,* 108th Cong., 1st Sess. (Oct. 30, 2003) (Dr. Ambrose)

39 Eggen, "U.S. Set to Revise How It Tracks Some Visitors," *Washington Post,* p. A1 (Nov. 21, 2003).

40 Michael *et al.*, "Diplomacy spotlights border systems," *Federal Computer Week,* pp. 1-2 (June 16, 2003) (www.fcw.com).

For companies with international partners and supply sources, obtaining parts "just in time" has become easier with e-commerce systems for managing inventory and transportation. However, heightened restrictions on moving cargo threaten to drive up costs, inventory levels, and transportation times. In an effort to speed up the flow of cargo, the Customs Office has struck bilateral agreements with 16 foreign governments covering 22 of the largest seaports to allow container inspections before high-risk cargo leaves foreign shores. However, Customs has yet to deploy inspection teams to many ports, due to lack of foreign-speaking inspectors, readiness of foreign ports, and other factors.[41] As a result, international ventures and partnerships may suffer through this transition.

International Challenges

International cooperation and business alliances may trigger a host of issues, as the clamp down on terrorism affects how companies do business. Areas to watch include the following

- Export controls on technology and data
- European privacy restrictions
- Inconsistent international technical standards
- Facility and personnel security

Funneling Funds to State and Local Governments

Few aspects of the Homeland Security Act have generated more scrutiny and blown air than moving grants to the state and local level.

The Mission to Support State and Local Efforts

Section 801 of the Homeland Security Act establishes "within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments." Pub. L. No. 107-296, § 801(a). However, the political action swirls around the Office of Domestic Preparedness (ODP) that "shall have the primary responsibility within the executive branch of Government for the preparedness of the United States for acts of terrorism." *Id.*, § 403(c). Aside from various tasks of "coordinating preparedness," "consolidating communications," and "providing agency-specific training," ODP hands out the grant money.

ODP Grants: The Money Train

Everyone wants to take credit for loading up funds for state and local Homeland Security grants. For example, the Whitehouse website included the bolded news that

---

41 GAO, "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors," pp. 18-20 (July 2003) (GAO-03-770).