AVIATION WEEK'S
Homeland SECURITY & DEFENSE
Weekly Intelligence for the global homeland security and defense community

July 30, 2003
vol. 2, no. 31

Inside:

In Brief:

The Department of Homeland Security (DHS) wants to create web-based training programs to help first responders prepare for potential terrorist scenarios, Penrose "Parney" Albright said July 29 at his Senate confirmation hearing to be DHS assistant secretary for plans, programs and budget in the Science and Technology Directorate. "It is not enough to create standards for homeland security equipment and... throw that equipment over the transom," he told the Senate Governmental Affairs Committee.

The McGraw·Hill Companies

Congress split on requiring screening of cargo shipped on passenger aircraft

Almost two years after the terrorist attacks of 9/11, one congressman is forcing Congress to confront what he calls a "gaping hole" in the U.S. security system for commercial airlines that could allow terrorists to smuggle a bomb aboard as cargo.

"Right now, on passenger jets going all across America at this time, air cargo is being put under the passengers which has not been screened [for explosives]," Rep. Edward Markey (D-Mass.) said at a recent hearing. "We have to take off our shoes, turn over our belts, but the air cargo is not screened."

The possibility of a terror attack using airplanes as weapons was reinforced over the weekend when the Department of Homeland Security (DHS) issued an advisory to the airlines about possible suicide hijackings sometime in the next few months.

Markey succeeded last month in adding an amendment to the DHS budget legislation that would require all cargo on passenger planes to be screened for explosives.

Cargo, Page 3

Designers installing 'intelligent' software in surveillance camera systems

The proliferation of surveillance cameras since 9/11 is spearheading a trend toward equipping them with software that enhances their capabilities, according to industry specialists.

"Intelligent" camera systems are being developed to help solve the human resources and data retrieval problems associated with the increasing use of cameras for homeland security.

"As cameras proliferate, it becomes increasingly impossible for people to monitor them," said Sandra Jones, a security technology consultant in Chardon, Ohio. "Rather than adding more bodies, you must build in intelligence" to the cameras.

The efficient retrieval of archived surveillance data also requires building information systems to store and process imagery from the camera.

"Current systems require autonomous human observation to interpret data," said Mohan Trivedi, director of an intelligent camera research project at the University of California-San Diego (UCSD). "We want to eliminate or minimize that as far as archiving goes."

Thus, rather than reviewing hours of tape, a system could be searched to retrieve an image of a person who fits a certain description.

The UCSD lab is working both on camera technology and its associated information systems. Trivedi and his team are developing an omni-directional camera with a 360-degree panoramic view as well as a networked technology system that would allow a series of cameras to communicate with one another.

Camera, Page 2

Editorial and Circulation Offices
1200 G Street N.W. • Suite 200
Washington, D.C. 20005
www.AviationNow.com

Editorial:
Tel: 202-383-2363 • **Fax:** 202-383-2438
E-mail: awhomeland@AviationNow.com

Circulation:
Tel 800-752-4959/202-383-2403 • **Fax** 202-383-7956
Customer Service: mailto:awgnews@mcgraw-hill.com

U.S. Editorial Staff
Editor-in-Chief, Lee Ewing
Managing Editor, Paul Hoversten
News Editor, Harvey Simon
Reporter, John M. Doyle
Copy Editor, Martin Sibley
Production, Ingrid Lee

International Correspondents
Prague:
Magnus Bennett, czechnews@quick.cz
London:
John Fricker, avia@mcmail.com
Moscow:
Dmitry Pieson, dpieson@mail.ru
New Delhi:
Bulbul Singh, bulbul.singh@indiatimes.com

Business Office
Mark A. Lipowicz, Publisher, tel 202-383-3681
lipowicz@AviationNow.com
Ani Luxner, Director of Marketing, tel 202-383-2391,
ani_luxner@AviationNow.com
Denise L. Almond, Director, Business Development,
tel 202-383-2399, denise_almond@AviationNow.com
Beth Cooperman, Advertising Manager, tel 800-660-0132/202-383-2467, beth_cooperman@AviationNow.com
Elizabeth Meyer, Classified advertising, tel 212-904-3675,
fax 212-904-3334, elizabeth_meyer@AviationNow.com

Subscription Pricing
$595 for single user delivered via print, web or e-mail. Discounted rates begin with the second user at the same postal or electronic address. Special rates and services available for enterprise licenses. To order call 800-752-4959; 202-383-2399 outside the U.S.; or online at: http://www.AviationNow.com/bis.

WEB ACCESS TO HOMELAND SECURITY & DEFENSE

Subscribers to the electronic version of Homeland Security & Defense can access the current issue and archive at: http://www.AviationNow.com/hsd.
AWIN subscribers go to: http://www.AviationNow.com/awin

AVAILABLE ELECTRONICALLY

For electronic delivery please call:
1-800-752-4959 in the U.S.,
or +1-202-383-2403 internationally.
mailto:aw_intelligence@aviationnow.com

ASCII PDF

Reprints
For reprints of Aviation Week Business Intelligence Articles, contact Wilda Fabelo at 212-512-4170 or mailto:aviatonreprints@businessweek.com

The McGraw·Hill Companies

Published weekly by Aviation Week, a unit of the Publication Services Group, The McGraw-Hill Companies, Inc., 2 Penn Plaza, New York, N.Y. 10121. (ISSN No. 0193-4597). Kenneth E. Gazzola, Executive Vice President, Aviation Week Group. Officers of The McGraw-Hill Companies, Inc.: Harold W. McGraw, III, Chairman, President and Chief Executive Officer; Kenneth M. Vittor, Executive Vice President and General Counsel; Robert J. Bahash, Executive Vice President and Chief Financial Officer; Frank D. Penglase, Senior Vice President, Treasury Operations. **Multiple copy discounts available, contact Denise Almond at tel 202-383-2399, denise_almond@aviationnow.com**

Camera, Page 1

"A network could track a suspicious vehicle that was observed moving in a certain direction," Trivedi explained, by having one camera communicate that information to another.

The lab is also tackling the problem of how to analyze information gathered from different perspectives and with differing resolutions and shadow patterns. "We believe we will be able to develop an algorithm to do that," he said.

The Department of Defense last month awarded $600,000 to Trivedi's lab for further development of intelligent camera systems.

Some of the UCSD lab's work was tested at the Super Bowl earlier this year. Cameras set up around Qualcomm Stadium in San Diego were used to estimate crowd sizes and to aid in communications with police and other first responders in case of emergency.

A related development involves information systems that integrate data gathered by cameras and other security devices such as intrusion detectors and sensors. Seattle-based Vigilos, Inc. on July 3 won a contract with the Port of Seattle to install such a system there. Terms were not disclosed.

Vigilos' system allows data from various incompatible cameras and other devices to be viewed centrally through a virtual command and control program. The user sets rules so that situational awareness and response can be prioritized and escalated under various circumstances.

The system is designed so that data can be shared among organizations, and security measures such as lockdowns can be activated remotely.

"It converts the interaction of various devices from a tower of Babel to an efficient business process," Jones said.

The Port of Seattle will pay for the Vigilos system from a grant from the Department of Homeland Security's Operation Safe Commerce, according to port spokesman Mick Shultz.

Privacy advocates worry that intelligent cameras might infringe on citizens' rights. Cedric Laurant, a policy lawyer with the Electronic Privacy Information Center in Washington, D.C., said that the law provides none of the requirements — such as obtaining a warrant — for photographing citizens surreptitiously that it does for recording their conversations.

"There ought to be guidelines establishing for what purposes cameras could be used and where they would be located," Laurant said.

— Peter A. Buxbaum (pab001@aol.com)

FAA reauthorization includes limits on CAPPS II

Congress is on the verge of approving new restrictions on one of the Transportation Security Administration's (TSA) keystone aviation security programs, the second-generation Computer-Assisted Passenger Pre-screening System (CAPPS II).

Legislation (H.R.2115) reauthorizing the Federal Aviation Administration over the next four years requires the TSA to report to Congress on the effectiveness and fairness of CAPPS II before doing any major work on the program.

House and Senate conferees approved their report on the bill July 25. The House is expected to take up the report when it returns after Labor Day.

The bill requires the TSA to certify to Congress that: it has a procedure for passengers to appeal if they can't board a flight because CAPPS II deems them a security threat; the system will not mistakenly identify "a large number" of passengers as threats; it has established an internal oversight board; it has protected CAPPS II from hackers; CAPPS II presents no specific privacy concerns.

The TSA must also report to Congress on safeguards for CAPPS II data, including how long it will be retained and who can access it.

The Department of Homeland Security spending bill, which has gone to conference to iron out differences between versions approved in the Senate and House, also restricts development of CAPPS II *(story, Page 8).*

Cargo, Page 1

But the spending bill the Senate approved on July 24 does not contain that requirement, leaving the issue to a House-Senate conference to resolve.

An estimated 20-30 percent of all cargo shipped by air is flown on passenger aircraft, while the rest goes on all-freight carriers, such as FedEx.

"It's unfortunate we seem to be gearing all of our concern toward passenger airplanes, said David Wirsing, executive director of the Airforwarders Association in Alexandria, Va., who says the threat from explosives on all-cargo carriers is just as great.

Although the House and Senate have yet to agree on how to resolve the cargo issue, there is no disagreement that a disparity exists in today's aviation security system.

The Transportation Security Administration (TSA), for example, inspects all passenger bags, but not all cargo. Some cargo is inspected on a spot basis when it is evaluated as high-risk, but most is routinely put on board without being checked.

In April, the General Accounting Office reported that "vulnerabilities exist in securing the cargo carried aboard commercial passenger...aircraft."

DHS Secretary Tom Ridge also acknowledged a "deficiency" in the cargo security system during one of Markey's many face-offs with administration officials over the issue. Ridge said, "We recognize this vulnerability and that is a very high priority within [TSA chief] Adm. [James] Loy's shop presently. We focused on the baggage, we focused on the passengers and now we're beginning to focus on the cargo."

The DHS' Aviation Security Advisory Committee (ASAC) plans to issue recommendations for improving air-cargo security this fall.

'Glaring inconsistency'

Even the libertarian Reason Foundation, which opposes screening all checked luggage for explosives in favor of focusing on items that pose the greatest risk, has called the different standards TSA uses for cargo and luggage "a glaring inconsistency."

If the problem is clear, the solution has been elusive.

With no system in place for screening cargo, Markey's proposal would force passenger airlines to stop carrying cargo. And that would shut down the airlines, which are dependant on cargo revenue, Rep. Harold Rogers (R-Ky.) said recently. Cargo brings in an estimated $3 billion annually to the financially struggling airlines.

Also affected would be Massachusetts fishermen, who need to get their catch to the West Coast on the first flight of the morning, and auto manufacturers, who rely on just-in-time parts delivery to keep assembly lines moving, Wirsing said. All-cargo companies do not offer enough flights to fill the gap, he said.

Markey's approach is "ham-handed" and would cripple the movement of air freight, said John Amos, retired transportation and logistics chief for the Bechtel Corp. and a consultant in Pleasant Hill, Calif.

Then there is the question of whether the technology even exists to screen air cargo. While Markey claims the technology does exist— and is being used in other countries — to screen cargo, others disagree.

"Equipment able to accurately scan bulky, dense freight items does not exist," according to the Air Cargo Management Group in Seattle.

Ridge, in a June 9 letter to Markey, said, "Logistical and technological limitations on the processing capabilities of these machines will have to be overcome for large-scale deployment in the passenger air cargo area."

The answer may be that the technology exists to screen cargo — if it is broken down from pallet-sized loads to individual boxes and bags.

No technology exists to screen pallets of cargo for explosives, said Sergio Magistri, president and CEO of InVision Technologies of Newark, Calif. But 80 percent of the cargo that goes on passenger planes is in packages small enough to fit through the one-meter opening of InVision's explosive detection system machines, which are also used to screen checked luggage.

Cargo screening should be phased in, starting with a requirement to check 20 percent of what goes on passenger planes and increasing by 20 percent a year until 80 percent is checked, said Magistri, who was unable to estimate the cost of such a program. "This would allow for a rational implementation."

Also at issue has been the adequacy of the "known shipper" program, TSA's primary means of ensuring cargo security.

The known shipper program, which pre-dates 9/11, permits shippers that have established business histories with air carriers or freight forwarders to ship cargo on passenger planes. Other freight goes on all-cargo airlines.

The known shipper program can be penetrated, if you "bide your time and get established," according to Charles Edwards, an executive with Pinnacle Analysis and Logistics Services in Raleigh, N.C., who has experience in the freight forwarding and air cargo industries.

But Wirsing, a member of the ASAC Cargo Working Group, said the TSA has made improvements to the known shipper program that he could not discuss for security reasons. The working group will recommend further enhancements, he said.

— Harvey Simon (harvey_simon@AviationNow.com)

Committee OKs Fire Administration

The House Science Committee on July 22 approved legislation (H.R.2692) to reauthorize funding for the U.S. Fire Administration (USFA) for the next three years. The authorization covers such areas as training, fire research and public education. One of the USFA's major concerns is communications interoperability for firefighters, David Paulison, head of the agency, told the committee's Science Research Subcommittee on July 17. The USFA became part of the Department of Homeland Security on March 1, as part of the Federal Emergency Management Agency.

Cooperation, not regulation, key to better security, report says

The federal government should consider a collaborative approach with industry on homeland security that is based on risk analysis, rather than regulation, according to a new white paper by The Business Roundtable.

The paper, *Terrorism: Real Threats, Real Costs, Joint Solutions* (http://www.brtable.org), warns against excessive use of traditional regulatory practices, saying that one-size-fits-all cannot fulfill changing security needs with critical infrastructure industries.

"Because industry has only so many resources that it can dedicate to security challenges, we need to make sure they are used in the right way," said Marian Hopkins, director of public policy and manager of the Roundtable's security task force, which wrote the paper.

The Roundtable, which released the report July 23, is an association of CEOs of leading U.S. companies with a combined work force of more than 10 million employees and annual revenues of $3.7 trillion.

Neither business nor government alone can adequately manage security risk, the report says. Where government must intervene, policymakers should consider such measures as tax incentives, priority-setting and public-private partnerships rather than outright regulation.

Frederick Smith, chairman and CEO of FedEx and chairman of the Roundtable's security task force, cited as an example the way Customs worked collaboratively with industry to increase security of shipping.

When Customs sought the installation of radiation detectors at offshore locations, it allowed private companies to decide how to do that, he said in a statement accompanying the report.

"Industry has a responsibility for securing its own facilities, but if there are costs above and beyond a company's ability to cover, and if there's a national security interest at stake, then it's appropriate for the federal government to step in," Hopkins said in an interview.

She said there already are government regulations for just about every company involved in the critical infrastructure network, which includes such industries as banking, telecommunications and utilities.

Since 9/11, the federal government has added numerous regulations for the aviation industry and may add new regulations for the chemical, transportation and information technology industries, Hopkins said.

Should another terrorist attack occur, she said, "there's always a concern...the federal government is going to regulate in response to public fears."

— Paul Hoversten (paul_hoversten@AviationNow.com)

Congress weighs regulation for corporate cybersecurity

Despite opposition from the private sector, businesses may be facing legislative mandates regarding the security of their information systems, according to industry officials.

The Cybersecurity Subcommittee of the House Select Committee on Homeland Security conducted hearings earlier this month that explored the roles of government and business in securing cyberspace. The technology subcommittee of the House Government Reform Committee has set a similar hearing for September.

Meanwhile, security technology providers have formed a consortium to plug gaps in critical infrastructure security technology while standards are being developed.

Industry representatives appearing before the cybersecurity panel July 15 and July 22 strongly opposed regulation, saying information sharing between business and government through such means as the Information Technology Information Sharing and Analysis Center was enough to protect critical infrastructure.

Philip Reitinger, senior security strategist at Microsoft Corp., called for government to lead by example by securing its own information systems, providing more federal funding for cybersecurity research and development, beefing up laws against cybercrime and increasing the flow of information to the private sector.

"The government must be a provider as well as a consumer of valuable threat information," he said at the hearing.

Daniel Wolf, director of information assurance at the National Security Agency, said at the July 22 hearing that the best way to protect cyberspace is through "an interoperable authentication system deployed widely throughout the federal, national-security, first-responder and critical-infrastructure community."

Despite private-sector protests, "government may need to step in somewhere," said Tucker Anderson, a staffer to subcommittee Vice Chairman Pete Sessions (R-Texas). "We are trying to define where and how much."

Shannon Kellogg, director of security at the Business Software Alliance, a Washington, D.C., trade group, insisted that regulation is not necessary.

"There are already laws on the books...that require that certain security measures be taken," he said. "The issue is getting CEO-level attention, so we don't think any additional laws are necessary."

Some security experts say industry needs to take matters into its own hands because the departure of government cybersecurity experts created a vacuum, slowing the potential progress of a public-private partnership.

Ronn Bailey, CEO of Vanguard Integrity Professionals in Las Vegas, Nev., cited the departures of Richard Clarke, the special White House adviser for cybersecurity; Howard Schmidt, the vice chairman of the president's critical infrastructure board; Ron Dick, the director of the National Infrastructure Protection Center; and John Tritak, director of the Critical Infrastructure Assurance Office.

Bailey and other security vendors formed a coalition called the Technology Alliance that is designed to develop and distribute a stronger and simpler security system for mainframe computers.

— Peter A. Buxbaum (pab001@aol.com)

Cargo container checks depend on risk assessments, Coast Guard says

The Coast Guard will not disclose how many cargo containers will be checked for tampering while in U.S. ports, according to a top agency official.

The percentage of containers to be checked will be based on the outcome of security risk assessments at individual ports and will not be the same at every facility, Rear Adm. Larry Hereth, Coast Guard port security director, said July 23.

The inspections are required as part of the Maritime Transportation Security Act (MTSA), which was signed into law in November 2002. Hereth spoke to reporters during a break in a meeting in Washington, D.C., on interim Coast Guard rules for implementing the legislation. A final rule is to be issued in October.

The interim rules, which went into effect July 1, require port owners or operators to check cargo container "[door] seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility."

"A broken seal would alert the port facility that the container has been tampered with, and that it needs to be carefully inspected before entering a facility or being placed on a vessel," Robert Remar, general counsel for the International Longshore and Warehouse Union, told the House Transportation and Infrastructure Subcommittee on Coast Guard and Maritime Transportation on July 22.

Remar called on the Coast Guard to "ensure that these practices start as soon as possible."

Containers can be quickly and easily entered without damaging the seal or leaving any obvious signs of tampering, law enforcement officials say (*HSD*, July 23).

Hereth called checking the door seals "one part of a process that has to involve many things."

The Coast Guard estimates the first year cost of implementing the MTSA at $1.5 billion.

Over 10 years, the cost is estimated to be $7.3 billion, according to the Coast Guard. The final figure is likely to be twice that amount, according to Chang Guan, a professor of logistics and intermodal transportation at the U.S. Merchant Marine Academy.

— Harvey Simon (harvey_simon@AviationNow.com)

Briefs

DHS awards grants for port security

The Department of Homeland Security (DHS) has awarded $28 million in Operation Safe Commerce grants, the department announced July 24. Operation Safe Commerce is a pilot program involving private industry, ports, and government at the local, state and federal levels to analyze procedures and technologies for securing cargo entering the country. Funding was given to the Port of Seattle/Tacoma ($14.2 million), the Port Authority of New York and New Jersey ($7 million) and the port of Los Angeles/Long Beach ($5.4 million). The three ports will test new technologies and procedures for improving security while loading containers, and for securing and monitoring containers.

Identix to study 3D facial recognition

Prime contractor Unisys Corp. has selected Identix Inc. of Minnetonka, Minn., to help research 3D facial recognition technology for the Department of Defense, Identix said July 29. The value of the award to Identix exceeds $1.2 million. The objective of the DOD program is to develop integrated biometric systems for physical access control, border crossing security and user authentication for computer networks. Identix will research whether 3D facial geometry algorithms prove to be more accurate than two-dimensional models.

Smith & Wesson, ISDS team on training

Handgun maker Smith & Wesson of Scottsdale, Ariz., has formed a partnership with Israeli security company International Security & Defense Systems (ISDS) to provide advanced counter-terrorism training courses for military, law enforcement and security personnel, the companies said July 23. The courses, to be taught at the Smith & Wesson Training Academy in Springfield, Mass., include instruction on detecting and defeating suicide bombers, VIP protection and physical protection of infrastructure. All ISDS personnel are former members of Israeli counter-terrorism units such as Mossad.

Verint gets interception system order

Verint Systems Inc. of Melville, N.Y., has received a multimillion-dollar order for its Reliant Communications Interception Solution from a new U.S. government agency, the company said July 23. Terms and the name of the agency were not disclosed. Reliant enables the user to intercept and analyze voice and data communications for a variety of investigative purposes, including gathering intelligence in order to identify and prevent criminal activities and to obtain evidence to convict criminals, the company said. The technology complies with standards established by the Communications Assistance Law Enforcement Act in the United States.

Armor to buy Simula for $110.5M

Armor Holdings Inc. of Jacksonville, Fla., which makes police and military equipment, has signed a letter of intent to buy safety technology equipment manufacturer Simula Inc., of Tempe, Ariz., for $110.5 million, the companies said July 23. The companies expect to sign a formal merger agreement by Aug. 29 and complete the transaction in the fourth quarter. Armor, which makes such equipment as bulletproof vests, batons and drug identification kits, said the deal would help it diversify its product line. Simula's core technologies include lightweight blast kits for military vehicles and personal protective equipment such as military body armor.

DHS opens competition for first university-based research center

The Department of Homeland Security (DHS) has begun setting up a network of university-based homeland security research centers to spur development of anti-terror technologies.

The DHS issued a broad agency announcement (BAA) on July 23 soliciting proposals for the first of the Homeland Security Centers of Excellence.

"The purpose of these centers is to provide a locus to attract and retain the nation's best and brightest academic scholars in pursuit of homeland security-related disciplines," according to the BAA, which closes Aug. 11.

The DHS has a Nov. 25 deadline for establishing the first center. More information about the BAA is available at http://www.dhs.gov and at the web site of Oak Ridge Associated Universities, http://www.orau.gov/dhsuce.

The DHS plans to establish up to 10 centers to augment homeland security research and development already underway at Energy Department laboratories, the DHS' Science and Technology Directorate and in programs contracted out to industry.

The centers will be "the last step we've been waiting for" in the DHS' overall R&D plan, said Kei Koizumi, director of the R&D budget policy program at the American Association for the Advancement of Science in Washington, D.C. The private sector may also have a role in the centers by partnering with universities, he said.

A recent survey for the DHS found that at least 80 universities were doing homeland security research. The Association of American Universities (AAU) and the National Association of State Universities and Land Grant Colleges conducted the poll of 170 institutions.

The survey probably underestimated the number of schools with homeland security research, according to Toby Smith, a senior federal relations officer with the AAU in Washington, D.C.

"Some didn't respond that do have a lot of things going on," Smith said.

The research included areas such as prevention, detection, identification and responses to potential nuclear, biological, radiological, chemical and conventional explosive attacks.

The survey also found work in support of first responders, in the protection of critical infrastructure, in cyber security, in forensics, and in biometric identification.

There was also social science research being done into the motivations for terrorism.

Social science will also be the focus for the first homeland security center. It will emphasize "risk-based modeling, with a particular emphasis on economic aspects...with the goal of developing predictive tools to assess vulnerabilities and potential responses to attacks...and to identify the costs and benefits of alternate countermeasures," according to the BAA.

These areas were singled out in a 2002 National Research Council report, *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism.*

In the fall, the DHS will also try to spur university research into homeland security by funding 50 two-year undergraduate scholarships and 50 three-year graduate fellowships.

Smith compared the DHS scholarships to the much larger National Defense Scholarship program established in 1958, the year after the Soviet Union launched Sputnik, the world's first satellite.

Congress approved $3 million in fiscal 2003 for the first homeland security center.

The fiscal 2004 spending bill that the Senate approved July 24 includes $55 million for additional centers and scholarships, but the House only approved $35 million. The Bush administration proposed $10 million.

The centers are modeled on university centers dedicated to Defense Department research, such as the Applied Physics Laboratory at Johns Hopkins University in Laurel, Md., according to Koizumi.

Eventually, the centers could help shift the DHS' R&D focus from an emphasis on short-term development to longer-term research, he said. Still to be worked out, Koizumi said, was the extent to which the DHS would determine the centers' research agenda.

— Harvey Simon (harvey_simon@AviationNow.com)

DHS says it's on schedule to meet U.S. VISIT deadline

The Department of Homeland Security (DHS) is on track to meet a year-end deadline to screen foreign visa-holders at the largest U.S. ports of entry with biometric identifiers like fingerprints and photographs, according to a top DHS official.

"We'll meet that deadline," Michael Garcia, DHS assistant secretary of the Bureau of Immigration and Customs Enforcement, said July 23 in a speech at The Heritage Foundation in Washington, D.C.

"It's a tremendous undertaking, gaining control of the ports of entry," Garcia said. "It will take tremendous technology to do that, but it's very much a priority of DHS."

The U.S. Visitor and Immigrant Status Indication Technology (U.S. VISIT) program, which calls for biometric screening of all foreign visitors at major U.S. airports or seaports by January 2004, is the first step of the Enhanced Border and Visa Security Act.

The DHS has said it plans to issue a request for proposals by Nov. 30, receive proposals in January and then award a contract in May to a prime contractor to implement the later phases of U.S. VISIT.

By Oct. 26, 2004, the program also calls for passports issued to visitors applying for entry into the United States to be machine-readable and tamper-resistant and have multiple biometric identifiers.

By Dec. 31, 2004, the system is expected to be in place at the 50 largest U.S. land ports and at all remaining land ports by the end of 2005. The DHS plans to spend more than $325 million in fiscal 2003 on the program.

— Paul Hoversten (paul_hoversten@AviationNow.com)

Policy group gives White House 'D' on homeland security efforts

A policy group has given the Bush administration a 'D' for its homeland security efforts, but one counterterrorism expert says that's not really a bad grade, considering all that had to be done in a short time.

The Progressive Policy Institute (PPI), which issued the grade July 23, is a non-profit with links to moderate Democratic causes. The group bills itself as an advocate for a "third way" beyond liberal or conservative politics.

The PPI's report card included: a D for intelligence gathering and analysis; a D-plus for protecting critical facilities; a C for safeguarding against bioterrorism; an A for nuclear plant security.

The group said it studied seven categories and 28 subcategories of homeland security policy, assigning grades after analysis by PPI staff and discussion with outside experts and government employees.

Homeland security analyst Michael Scardaville of The Heritage Foundation called the report card "pure politics." PPI shares Web site space with the Democratic Leadership Conference.

The report card acknowledged the help of Rep. Jane Harman (D-Calif.), ranking member of the House Intelligence Committee, and Rep. Jim Turner (D-Texas), top Democrat on the House Select Homeland Security Committee.

"I don't see a very serious analysis here," Scardaville said. He noted the report criticizes the second-generation Computer-Assisted Passenger Prescreening System on privacy grounds while faulting the administration for not being tough enough on passenger screening.

Erik Floden, director of the Terrorism Prevention Project at the Center for Arms Control and Non-Proliferation, said a 'D' wasn't necessarily bad, "considering that we're just two years out from 9/11 and that the Department [of Homeland Security] has been set up for only six months."

Of greater concern, Floden said, "is whether the administration has the approach and attitude necessary to get things done five, six years down the road."

James Lewis, senior fellow at the Center for Strategic and International Studies, said he would give the White House a 'C' and said the report card showed homeland security was now a "political football."

"The implicit argument is that the other side [Democrats] would be doing better and I'm not sure that's right," Lewis said.

— John M. Doyle (johnm_doyle@AviationNow.com)

Customs needs better staffing plans for CSI, C-TPAT, GAO says

The Customs Service does not have adequate staffing plans for its two major programs aimed at preventing terrorists from smuggling weapons of mass destruction into the United States, according to a congressional report.

Customs "has not taken adequate steps to incorporate factors crucial to the ... long-term success and accountability" of the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), according to a July 28 report from the General Accounting Office.

CSI is a cooperative program with foreign ports to screen high-risk cargo containers. C-TPAT is a voluntary industry program to improve global supply-chain security.

Under the CSI, the United States has signed up 19 of the world's top 20 ports. China's ports of Shanghai and Shenzhen became the latest to join, signing up July 29.

U.S. inspectors are already working under the CSI at 15 ports, including Antwerp, Belgium; Genoa, Italy; Halifax, Nova Scotia, and Yokohama, Japan.

But Customs has not developed a systematic plan to recruit or train CSI staff for long-term assignments in foreign ports, "some of which may require unique language capabilities and diplomatic skills," according to the report (available at http://www.gao.gov).

And there is no C-TPAT plan for managing a planned 16-fold expansion, from 10 to 160 staff members, the report found.

Nor has Customs developed any effective way to determine whether C-TPAT has improved supply-chain security for participating companies, the GAO found.

Customs agreed with the report that it needs better personnel planning and noted that it is making progress developing performance measurements for C-TPAT.

— Harvey Simon (harvey_simon@AviationNow.com)

OMB commits $5 million to FDA for food security research

The Department of Health and Human Services (HHS) is starting a new $5 million security research program to develop technologies for protecting the nation's food supply, the department announced July 23.

The program plans to develop technologies to assess foods for contamination with chemical, biological and radiological agents. Research on technologies to prevent and control contamination will also be funded.

The White House's Office of Management and Budget is making the funds available to the Food and Drug Administration (FDA) from the post 9/11 Emergency Response Fund.

Research projects will, in part, try to determine the stability of certain chemical threats in foods and the effect of food processing. They will also try to develop enrichment techniques for isolating certain microbial agents from high-priority foods.

The work will be divided between FDA labs and private contractors. On June 25, the agency issued a request for applications to assist in its research.

Since 9/11, the FDA has boosted the number of inspections of imported foods, from 12,000 in fiscal 2001 to 62,000 so far this year. The agency, part of HHS, has increased the number of ports with food inspectors, from 40 to 90, and has hired 655 new food security and safety personnel.

Hill negotiators to take up DHS' fiscal '04 spending bill

House and Senate negotiators will begin work to narrow their differences on fiscal 2004 funding for the Department of Homeland Security (DHS) after the Senate July 24 passed a $28.5 billion budget for the DHS.

Senate Democrats, in a series of amendments, had sought to add billions of dollars to the bill, including additional funding for first responders and security at chemical plants and seaports. Majority Republicans defeated the amendments, citing budget constraints.

The House passed its version of the bill (H.R.2555), appropriating $29.4 billion, on June 24.

The Senate version lacks $5.6 billion for a 10-year funding of Project BioShield, including $890 million to be spent in 2004. The House had approved the BioShield money, which would subsidize research and development into bioterrorism antidotes.

The bill — the first for the DHS since it became a department — includes about $2.9 billion for state and local governments, including $750 million for high-threat cities.

Through various amendments, the Senate also voted to require DHS to:

- Report to Congress by March 1 on progress in developing countermeasures for commercial aircraft against shoulder-fired missile systems. Both the House and Senate version have appropriated $60 million toward research and development of such countermeasures.
- Provide a classified report to Congress by March 1 on costs incurred by state and local officials due to security requests from the Secret Service in protecting and transporting U.S. and foreign officials.
- Report to Congress within 90 days after passage of the budget bill on the status of the Homeland Security Advisory System, the five-color national threat alert system.
- Report to Congress within 120 days on vulnerabilities at 250 large U.S. sports and entertainment facilities.
- Report to Congress within 180 days on problems with the Student Exchange Visitor Information System (SEVIS) program and corrective actions.
- Report to Congress on efforts to redesign the research and development arm of the Coast Guard.
- Delay work on the Transportation Security Administration's Computer-Assisted Passenger Prescreening (CAPPS II) until the General Accounting Office (GAO) studies privacy protections of the program. The GAO is to report to Congress either within 60 days of passage of the budget bill or 60 days after DHS Secretary Tom Ridge publishes privacy notices for CAPPS II in the *Federal Register*.

— Paul Hoversten (paul_hoversten@AviationNow.com)

Cox says his bill would cut steps needed to fund first responders

Rep. Christopher Cox (R-Calif.), chair of the House Select Committee on Homeland Security, says he plans to introduce a bill after Labor Day that would cut the current 12-step process for first-responder grant applications to two steps.

"The 12-step process is 10 steps too many," Cox told a breakfast roundtable at the Capitol Hill Club July 23, sponsored by The Heritage Foundation.

Cox said first responders and local government now have to navigate a "complex and duplicative" dozen-step process that involves their state governments, the Department of Homeland Security (DHS) and vendors.

Under Cox's proposal:

First, states must develop a comprehensive security plan. That plan should include a risk assessment, a strategy for interoperable communications, descriptions of first-responder training programs and equipment, a roadmap for improved coordination among police, fire and public health authorities and a format to promote regional cooperation.

Second, the DHS will conduct threat-based evaluations of the applications, using data from the DHS' Information Analysis and Infrastructure Protection Directorate.

"We can have one-stop shopping" for first-responder grants under the bill, he said.

Cox's planned bill also would transfer the two offices that manage the largest first-responder grants, now located within separate DHS directorates, to the Office for State and Local Government Coordination within DHS Secretary Tom Ridge's office. Those offices are the Office for Domestic Preparedness, now in the Border and Transportation Security Directorate, and the Firefighter Assistance Grant Program, now in the Emergency Preparedness and Response Directorate.

Sen. Susan Collins (R-Maine), chair of the Governmental Affairs Committee, has introduced similar legislation (S.1245 and S.796) in the Senate.

Ridge told a first-responders conference in Arlington, Va., July 28 that after the House and Senate reconcile their fiscal 2004 DHS appropriations bills, "by the end of the year there'll be about $7.5 billion available for our partners in state and local government."

Ridge also said that starting in fiscal 2005, "we will make sure" the money gets to local first responders through statewide homeland security plans that are "state-coordinated but driven from the local government up."

Funding for first responders has increased more than 1,000 percent since fiscal 2001, with $20.8 billion approved, Cox said.

"Things are starting to work. But first responders say, 'Where's the money?' The truth is, we don't know where in the world it is," he said. "The purpose of this bill is to get the money out to where it's needed most and where the biggest threats are."

The bill, he said, also would allow first responders to use some of the money to reimburse for overtime incurred as a result of heightened national security alerts.

"What we don't want to do is have grants for overtime...But we do want to leave them free to [pay] that" if the state considers that a critical need, Cox said.

— Paul Hoversten (paul_hoversten@AviationNow.com)

New European forum will push biometric technology roadmap

PRAGUE — The European biometric industry has launched a new organization to develop a roadmap for using biometric technologies to improve security.

The European Biometrics Forum, which was set up July 21 in Dublin, Ireland, with funding from the European Commission, will help European countries implement biometrics and improve their security procedures.

Dermot Ahern, Irish minister for communications, said at the inaugural forum conference at Media Labs Europe in Dublin that there was now a solid base for the future development of an environment across Europe that could support biometric technology.

"The implementation of biometrics by member states and other countries worldwide will lead to standardization in the industry, improved border security control procedures, heightened security processes both within and outside the member states, and more efficient credentialing systems for citizen ID programs," he said.

The forum will carry out and support research, part of which will be the development of a roadmap for the European industry between 2003 and 2010. A center of excellence will be established in Dublin to provide a range of applications of biometric technologies in various environments.

A number of expert special interest groups will also be set up to share expertise in areas such as technology and applications, standards, testing and certification, and education and training.

The forum's board of directors includes representatives from the Centre for Mathematics and Science of the Netherlands, TeleTrusT of Germany and Consiglio Nazionale delle Ricerche of Italy. Principal members include the University of Applied Sciences Giessen-Friedberg in Germany, the National Physical Laboratory of Britain, University College London and the U.K. Association for Biometrics.

Martin Walsh, forum chairman and head of regulatory and legal affairs at Daon, said the group was working with the widest possible group of focused and experienced organizations to provide advice sought by government and industry in Europe.

"In the long term, we intend that our work will support and help lay the foundations for biometric standards worldwide," he said.

— Magnus Bennett (czechnews@quick.cz)

Calendar

Aug. 4-7 — Transportation Security Administration, Innovative Technologies in Maritime Security Conference, Charleston Convention Center, Charleston, S.C., www.ndia.org

Aug. 14-15 — Scentczar Corp. and Science Applications International Corp., First Toxic Industrial Chemical/Toxic Industrial Material Symposium, Virginia Commonwealth University School of Engineering, Richmond, Va., www.ticsandtims.com

Sept. 3-4 — International Biometric Group and IDG World Expo, BiometricsWorld Executive Conference, ExCel (Docklands), London, England, www.biometricsworldseries.com

Sept. 8-10 — Terrapinn, Transport Security World Europe 2003, Hilton Hotel, Amsterdam, Netherlands, ww.transportsecurityworld.com

Sept. 10 — NDIA, Interagency Homeland Air Security National Capital Region Demonstration Industry Day, Kossiakoff Center, Laurel, Md., www.ndia.org

Sept. 10-12 — Terrapinn, Transport Security World Asia 2003, Suntec Singapore, Singapore, www.transportsecurityworld.com

Sept. 15-16 — SMi, Critical Incident Recovery, The Hatton, London, England, www.smi-online.co.uk

Sept. 15-19 — AFCEA, The C4IEWS Path to Transformation and Homeland Security, Atlantic City Convention Center, Atlantic City, N.J., www.afcea-ftmonmouth.org

Sept. 16-18 — AIM and Frontline Solutions, International Supply Chain Week Conference & Expo, McCormick Place, Chicago, Ill., www.aimglobal.org/calendar

Sept. 23-25 — Homeland Security Summit Foundation, Homeland Security Summit 2, The Renaissance Waverly, Atlanta, Ga., www.securitysummit.org

Sept. 24-26 — E.J. Krause & Associates, 3rd Annual Conference & Expo on Nuclear, Biological, Chemical Terrorism, Marriott Wardman Park Hotel, Washington, D.C., www.bioterrorism-defense.com

Oct. 1 — American National Standards Institute, Homeland Security: Collaboration, Innovation and Standardization, Marriott Metro Center, Washington, D.C., www.ansi.org

Oct. 1-2 — E.J. Krause & Associates, Maritime Security Expo & Conference Europe, Congress Center, Hamburg, Germany, www.ejkrause.com

Oct. 2-3 — The Shephard Group, Night Vision USA 2003, Crystal Gateway Marriott Hotel, Arlington, Va. www.shephard.co.uk.htm

Oct. 8-10 — International Aviation Fire Protection Association, Aviation Fire Asia 2003, Singapore Expo, Singapore, www.iafpa.org.uk

Oct. 10-12 — Reed Exhibitions and SG Five, Training & Gear Extreme Expo & Interactive Conference, Mandalay Bay Convention Center, Las Vegas, Nev., www.tagexpo.com

Oct. 14-17 — Spatial Technologies Industry Association, GEO-INTEL 2003: Geospatial Intelligence & Information for the Nation, New Orleans Marriott, New Orleans, La., www.geointel.org

India deploys electronic warfare systems to intercept signals

NEW DELHI — The Indian government has deployed electronic warfare systems to fight terrorism in the northern state of Jammu and Kashmir and in India's seven northeastern states, according to Indian military officials.

Code-named Rikki-II and Rikki-III, the systems are designed to detect and intercept the source of radio transmissions from suspected terrorist groups, the officials said.

The Indian Army is equipping its soldiers in Jammu and Kashmir with hand-held thermal imagers to spot intruders and suspected terrorists. The electronic warfare systems then could detect, intercept and record communications between those groups and their command headquarters.

An early version of the system, Rikki-I, is being used in limited fashion to jam suspected terrorist transmissions.

Electronic sensors have also started to arrive for installation along the border with Pakistan, according to the officials. India has purchased about $7 million worth of sensors from U.S. and Israeli manufacturers.

The sensors can detect intruders crawling, walking or running in any weather and can operate at ranges beyond those of conventional sensors.

— Bulbul Singh (bulbul.singh@indiatimes.com)

Federal business opportunities

Selected federal business opportunities from www.fedbizopps.gov

Title: Structural Response to the World Trade Center Towers
Contracting Agency: Department of Commerce, National Institute of Standards and Technology
Solicitation Number: SB1341-03-R-0044
Posted Date: July 21, 2003
Response Date: August 18, 2003
Description: NIST is conducting a national building and fire safety investigation of the World Trade Center disaster. More information about NIST's investigation may be found at the NIST Web site http://wtc.nist.gov. This solicitation will contribute to completion of the objectives of Project 6, Structural Fire Response and Collapse. Specific information for Project 6 may be found by following this link to the NIST Web site http://wtc.nist.gov/media/WTCplan_new.htm#proj6. The objective of this solicitation is to determine the probable structural collapse initiation sequences for each WTC tower through analysis of the structural response of each building, both with and without impact damage, to structural temperatures from internal fires. The tasks include analysis of: (a) floor and column components and subsystems for service loads and time-temperature histories for ASTM standard test fires and representative building fire conditions; (b) the effect of the largest possible fire(s) in a tower without impact damage on the global stability of the structure, and (c) the contribution of probable fire paths in each tower with impact damage on the global stability of the structure. The analyses shall include the effect of elevated temperatures, component and/or subsystem failures, and the resulting load redistribution in the structure up to the point of global instability. The structural models and sequences of collapse initiation must be consistent with the video and photographic records, and other documented observations of the event. Details of this requirement will be provided in the solicitation. The requirement will be for a period of eight months. Award of a commercial indefinite delivery/indefinite quantity contract is anticipated with firm fixed price task orders to be issued. It is anticipated that a single solicitation will be issued on or about July 28, 2003 at www.fedbizopps.gov.
Points of Contact: Elizabeth Simon, Contract Specialist, phone (301) 975-5106, fax (301) 975-8884, email elizabeth.simon@nist.gov — Sandra Febach, Sup. Contracting Officer, phone (301) 975-6326, fax (301) 975-8884, email sandra.febach@nist.gov.

Title: Aerosol Collector Technology
Contracting Agency: Department of Energy, Lawrence Livermore National Laboratory (DOE Contractor)
Solicitation Number: FBO000032-03
Posted Date: July 16, 2003
Response Date: Aug. 18, 2003
Description: Lawrence Livermore National Laboratory, operated by the University of California under contract with the U.S. Department of Energy, is seeking one or more industrial partners to commercialize LLNL's high air volume to low liquid volume aerosol collector technology. Various licensing opportunities are available. Scientists and engineers at LLNL have developed a compact, low power consumption, and high efficiency aerosol collector that collects airborne particles and microorganisms from a large volume of air into a small volume of liquid. Continuous air monitoring, such as in detecting airborne pathogens and other pollutants, needs an aerosol collector that continuously collects air samples and concentrates the airborne materials into a liquid sample for subsequent preparation and analysis. Most commercial aerosol collectors now available for field use are large, power consuming, and produce collected sample into large volumes of liquid, typically more than 10 mL. When using them, the sample volume must be sub-sampled, effectively diluting the sample, resulting in a loss of sensitivity of detection. Emerging miniature detection systems analyze much smaller sample volumes, typically less than 1 mL. LLNL's invention is a new technique for the design of the new aerosol collector. It can collect particulates at a high airflow rate and deliver them into a liquid volume of 1 mL or less. The unique features of the new aerosol collector make it an ideal next generation air sampler for continuous air quality monitoring and airborne pathogen detection.
Point of Contact: Connie Pitcock, Administration, phone (925) 422-1072, fax (925) 423-8988, email pitcock1@llnl.gov.

Title: Evaluation of the Private Screening Pilot Airports
Contracting Agency: Department of Homeland Security, Border and Transportation Security, Transportation Security Administration
Solicitation Number: DTSA20-03-Q-01877
Posted Date: July 9, 2003
Response Date: None Given
Description: In accordance with the Aviation and Transportation Security Act (ATSA), TSA chose five airports to represent different airport categories in a pilot project of private security screening. TSA seeks to implement a sound process for measuring the performance of federal versus non-federal screeners. TSA seeks an efficient means of deploying resources while maintaining a high level of security. An effective evaluation process will provide guidance on private versus federal security and associated cost requirements for TSA executives, the administration, Congress and the nation's taxpayers. Under the ATSA, a key criterion for determining whether an airport can use private screeners is that the level of screening services is equal or greater than those provided by the federal government. TSA is required to provide reports to OMB on private screener performance. TSA wishes to be able to accurately and articulately respond to questions and inquiries from policy makers and the general public regarding the security and efficiency implications of private versus federal security screening operations. Therefore, the TSA's objective is to retain the services of a qualified and capable evaluator to implement a fair and impartial process for analyzing private and federal screener performance.
Point of Contact: Heather Morvant, Contract Administrator, phone (571) 227-1592, fax (571) 227-2913, email heather.morvant@tsa.dot.gov

Aviation & Aerospace's most comprehensive source for business-critical data

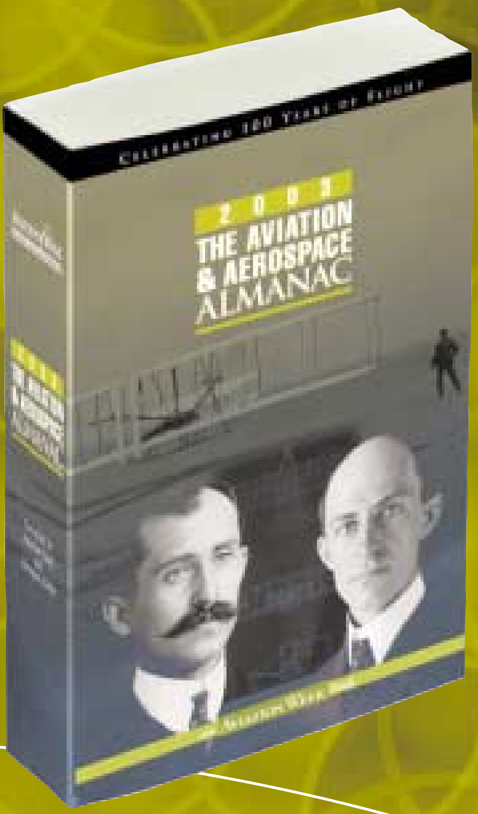
New 2003 Edition

New for 2003:

● **Homeland Security:** budgets, liaisons with other government agencies, organizational tables. ● **Eurocontrol:** — information on the air traffic control system of Europe. ● **Comparisons — pre- and post- 9/11:** – aerospace, airline, airport , traffic, freight, revenues, fares and others by state, region and nationally. ● **Who's Who in Homeland Defense** and where to find them. ● **Expanded** commercial and military aircraft forecasting.

The Almanac has the information you're looking for

- **Domestic, regional and international airlines traffic,** markets, operating expenses, revenue, fleet analyses, more
- **Airports top international 500 ranking** by passengers, movements, cargo
- **Specifications** of every national, international, military and civilian aircraft, missile, space vehicle and electronic system produced worldwide
- **Complete inventory** of military aircraft and missiles from every available country.
- **The global aerospace industry in summary** – production, shipments, R&D, comparison with other industries, export-import trade balance, export-import values, specifications of aircraft , missiles legislation.
- **ATC/ATM activity** – growth, airport improvement program, market share, forecasts forecasts of aircraft production, airline inventory, hours, air traffic facility information and traffic predictions, import-export information.
- **General Aviation** – inventory, hours flown, shipments forecasts, pilot licenses.
- **U.S. Government agencies** – organization charts, budget authority, facilities and equipment funding, procurement, contract awards, more. Dept. of Transportation, Federal Aviation Administration, National Transportation Safety Board, Departments of Defense, Air Force, Army, Navy, National Aeronautics and Space Administration.


Celebrating 100 Years of Flight
2003
The Aviation & Aerospace Almanac
Aviation Week Book

Special Offer

Save $10 off the regular price.

AVIATION WEEK
PROFESSIONAL BOOKS

○ Send me _____ copies of the 2003 edition of *The Aviation & Aerospace Almanac* at the introductory price of $119 each. ***I save $10 off the regular price of $129.*** Add $6 per copy for shipping to continental U.S. Other destinations add $25 shipping for the first book, plus $6 for each additional book.

Total enclosed:
US$ ___________

Five easy ways to order:

Fax:	202-383-7956
Call:	1-800-752-4959/202-383-2403
E-mail:	aw_intelligence@AviationNow.com
Online:	www.AviationNow.com/ professionalbooks

Or mail to:
The Aviation & Aerospace Almanac
c/o Aviation Week BIS
1200 G St. N.W., Suite 200
Washington, D.C. 20005-3815

NAME		
TITLE		
COMPANY		
STREET ADDRESS (CANNOT DELIVER TO P.O. BOXES)		FLOOR/SUITE
CITY	STATE/PROVINCE	ZIP/POSTAL CODE
COUNTRY	E-MAIL	
PHONE (REQUIRED FOR DELIVERY)	FAX	

PAYMENT: □ Check enclosed (U.S. funds, payable to Aviation Week Newsletters)
□ Credit Card □ VISA □ MasterCard □

CARD NO.	EXP. DATE
CARDHOLDER (PLEASE PRINT)	SIGNATURE (REQUIRED)

CAL37HDE

Aviation Week Business Intelligence Services
1200 G Street N.W. · Suite 200 · Washington, DC 20005-3815 · www.AviationNow.com/professionalbooks

The McGraw·Hill Companies