**David Berteau, our CAPITAL LETTERS columnist, takes on the White House's Homeland Security Council**

Page 23

GSN. Government Security News

**Cybertrust's CTO, Peter Tippett, shares some eye-opening ideas on cyber security**

Page 18

April 4, 2005 Vol. 3 Issue 7 | *The Newspaper of Record for Government Security* | A Publication of World Business Media, LLC

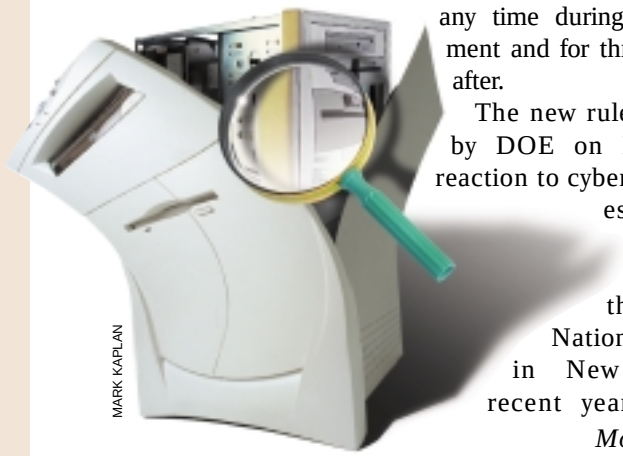
## INSIDE



# DOE wants right to inspect its employees' computers

**By JACOB GOODWIN**

In a sweeping set of proposed new regulations aimed at tightening cyber security, the Department of Energy plans to require all of its employees — and any employee of a DOE contractor who might communicate with a DOE computer — to agree upfront to allow "an authorized investigative agency" to inspect their computers at any time during their employment and for three years thereafter.



MARK KAPLAN

The new rules were issued by DOE on March 17 in reaction to cyber security lapses that have allegedly occurred at the Los Alamos National Laboratory in New Mexico in recent years. They will

*More on Page 26*

# DHS's new Nuclear Detection Office opens for business

*Vayl Oxford, of HSARPA, named acting director*

**By DAVID BATES**


The Department of Homeland Security (DHS) has officially launched its new Domestic Nuclear Detection Office (DNDO), which is dedicated to detecting and preventing the importation and use of nuclear or radiological devices by terrorists against the United States.

"We have an office that is staffed with transition team members," a DHS staffer told *GSN* just days after DHS Secretary Michael Chertoff signed a March 16 memo formally naming Vayl Oxford as acting director of DNDO.

Oxford also is acting director of DHS's Homeland Security Advanced Research Projects Agency and is a former director

*More on Page 17*

## GSN PERSPECTIVES

# Sector-wide ISACs have both critics and advocates

**By MARTIN EDWIN ANDERSEN**

Information Sharing and Analysis Centers (ISACs), the main channel for industry and the federal government to exchange security information, are the focus of renewed debate about their usefulness amid continued complaints by business executives that the Department of Homeland Security and other agencies fail

**Members of water & surface transport ISAC**

*More on Page 27*

# Surface transportation security: a status report

**By DAVID C. WALSH**

David Stone, head of the Transportation Security Administration (TSA), cites intelligence chatter and other data to bolster his assertion that of all the transportation sectors aviation remains the most at risk. As a result, for FY2006, 90 percent of the $5.6 billion TSA budget request is designated for aviation, while ground transportation (ports/maritime, commercial and passenger rail systems) at only $32 million gets less than the $115 million actually enacted in the 2005 federal budget, according to a White House "Budget in Brief."

*More on Page 13*

# FCC considers lifting its ban on cell phone use by airline passengers

MARK KAPLAN

The Federal Communications Commission (FCC) is considering a new rule that would replace or relax its current ban on the use of 800 MHz cell phones on airborne aircraft, but the Federal Aviation Administration (FAA) says it is likely to maintain its own separate prohibition on cell phones in order to prevent interference with an aircraft's navigation and communications systems.

The FCC's ban on 800 MHz cell phones, which was instituted in 1991,

*More on Page 28*

## *Covering Physical & IT Homeland Security Solutions*

www.gsnmagazine.com

Themal imaging camera from MSA North America can operate in temperatures above 300 degrees Fahrenheit
*Page 20*

Designer and builder Emmanuel Cabrera has developed a new airport facility with a more effective screening chamber
*Page 20*


VideoDefender from Lenel Systems International provides an IP-based digital video surveillance solution
*Page 20*

LG

The iris identity experts.™

# Look into the **Iris Recognition System** that's **generations ahead** of the rest

## IrisAccess™ 4000

Advanced Identity Authentication

## Now you've got more choices than ever before

LG, leader in deployed iris recognition platforms worldwide introduces LG IrisAccess™ 4000, third generation of the world's number 1 irisrecognition platform. It's available in a variety of configurations offering functionality and versatility you've never seen until now.

The new **two-eye camera** has a new **intuitive**, **interactive auto-focus imaging interface** enabling rapid capture of high-quality digital images of both irises, and lets you choose whether authentication will be left, right, either, or both eye-based. Every unit incorporates a **facial recognition-ready camera** and dedicated illumination. All variants incorporate the **anti-spoof countermeasures package** experts concede sets the standard for the industry, and offer other new security features as well.

Need **two-factor authentication**? IrisAccess™ 4000 is available with **optional device-embedded smartcard readers** that enhance the versatility of LG's "out of the box" iDentity☑ token authentication architecture. An **optional 16-element keypad** lets IrisAccess™ 4000 offer two-factor **PIN-based verification functionality** alone or in concert with other authentication modes and also makes the system an ideal choice for **workforce management applications**, especially when used with the **optional interactive 40 character vacuum fluorescent display**.

Look into IrisAccess™ 4000 and the options it offers. Like it says on the camera, it truly is advanced identity authentication, and it is only available from LG.


**LG Electronics U.S.A., Inc.**

Iris Technology Division

1095 Cranbury South River Rd., Suite #3

Jamesburg, NJ 08831

Tel. 609-819-IRIS(4747) Fax. 609-819-4736

www.lgiris.com


# Are your ads effective with Government Security Buyers?

***GSN: Government Security News has contracted with Larstan Business Reports to conduct its proprietary "Ad Effectiveness Study" on three different issues of GSN this year: dated April 18, July 18 and October 24. These studies will allow your advertisements to be measured by a third party, independent research firm. The results will help you plan your future campaigns.***

## Larstan's unique approach will tell advertisers:

- How effective is your ad compared with others in the same issue?
- Which ads draw the most attention?
- How does color influence ad recall and effectiveness?
- How well does a single page ad compare to a spread or an insert?

*Also included will be verbatim extracts from the Larstan interviews about your ad.*

---

**Book your ads in the April 18th, July 18th, and October 24th issues of *GSN* today.**

Contact your *GSN* representative for more information about an upcoming Larstan Ad Effectiveness Study. Orders must be received by the ad closing date of each issue.

GSN: Government Security News

LARSTAN BUSINESS REPORTS

GSN. Government Security News

# CONTENTS

## Front Page



## Features



## Departments




We help keep businesses running smoothly.

## Even one that serves **3.4 million customers a day.**

**The Washington, D.C. Metrorail can't afford interruptions.** So when it came time for necessary security upgrades, the Washington Metropolitan Area Transit Authority turned to ADT. Drawing on our unique resources and proven experience, we were able to create a system that integrates intrusion detection, access control and fire alarm into a single, cost-effective interface. And by helping streamline the Metrorail's security system, we did the same for their entire operation. To see how we've helped other large clients, visit us at www.ADT.com/homelandsecurity. Because when handling complex projects in today's environment, there's really no substitute for experience. **ADT Always There®**

tyco / Fire & Security

ADT®



For more information go to www.info.ims.ca/4758-013

# A message from Jacob Goodwin,
## *GSN's* Editor-in-Chief

Mom, apple pie, the American flag and homeland security.

Four beloved elements of contemporary U.S. society.

So beloved, in fact, that marketers go out of their way to associate their products with one or more of these revered symbols.

I can understand how "mom and apple pie" can pull at anyone's heart strings. (In fact, my late mother baked the *most delicious* apple pies in the world!)

And it is undeniable that marketing mavens have been wrapping themselves in Old Glory, and the patriotism it represents, for decades.

But this latest phenomenon of connecting one's product or service with the noble quest for homeland security can be carried a bit too far.

MARK KAPLAN

I'm reminded of an article we published two weeks ago about an interagency effort of the federal government to develop what's called the Integrated Ocean Observing System (IOOS) to monitor waves, current patterns, weather and potential tsunamis in the oceans of the world. In an effort to draw support for their billion dollar initiative, program officials went out of their way to note that the IOOS will "enhance national and *homeland security* in our coastal waters and ports…through improved observations and predictions of the ocean environments in which *homeland security* operations take place."

I'm no expert in ocean surveillance, but that seemed like a stretch to me.

The same trend can be discerned in the issue of *GSN* you're holding right now. If you turn to Page 1, you'll see an article describing how the Federal Communications Commissions is considering the notion of lifting its ban on the use of cell phones aboard airborne aircraft. Of course, the FCC is primarily concerned with the companies that provide telecommunications services and the consumers who use those services, but it didn't hesitate to cite the benefits to *homeland security* that might flow from the end to such a prohibition on cell phone use.

"We believe that allowing the use of wireless handsets during flight has the potential to benefit *homeland security*, business and consumers by adding to future and existing air-to-ground communications options…" the FCC explained in a Federal Register notice it posted March 10.

Again, I'm not a cellular communications guru, but the FCC's gratuitous reference to homeland security in order to drive its completely different agenda merits careful scrutiny.

I could tell that this trend had run amok when I received a press release the other day from the Invention Submission Corporation – "America's leading inventor service company" – touting the "ATM Anti-Terrorist Mailbox," which a Wichita, KS inventor has apparently developed and patented. "Even simple tasks like reaching in the mailbox for mail could cause some to worry about anthrax or smallpox," the press release explained. But there is little reason to worry. The Anti-Terrorist Mailbox can "purge the air" inside the mailbox and "diminish the potency" of any biological and chemical agents that might lurk inside. "The Anti-Terrorist Mailbox could also be produced with a fan-assisted air purging system, a remote control door opener and a built-in metal detector," the press release assured us.

Don't get me wrong. *GSN: Government Security News* is extremely interested in informing our readers about the genuine threats to our citizens and our critical assets, and we're eager to learn about – and write about – the truly innovative solutions to bona fide terrorist threats.

But I suggest it is also time for everyone to become a little bit more sensitive to the self-serving hype that some folks engage in when they employ the mystique of homeland security in completely unjustified ways. ■


GSN. Government Security News

Main Number: (212) 925-7300
Fax: (212) 925-8754
www.gsnmagazine.com

EDITOR-IN-CHIEF:
**Jacob Goodwin**
(212) 925-7300 x255
jgoodwin@gsnmagazine.com

SENIOR EDITOR:
**Teri Robinson**
(212) 666-9292
trobinson@gsnmagazine.com

ART DIRECTOR:
**Mark Kaplan**
(212) 925-7300 x322
mkaplan@gsnmagazine.com

WASHINGTON CORRESPONDENT:
**David Bates**
(301) 270-5396
dbates@gsnmagazine.com

CONTRIBUTING WRITERS:
**Martin Edwin Andersen, David Berteau, Steven Brier, Barbara DePompa, John Kamp, Skip Kaltenheuser, Rohit Mehra, Nicholas Roegner, Robert Schlesinger, Arpad Toth, Richard Tracy, Jan Wilson**

PUBLISHER:
**Edward Tyler**
(212) 925-7300 x232
etyler@gsnmagazine.com

DIRECTOR OF ADVERTISING:
**G. Scott Dinkel**
(212) 925-7300 x218
sdinkel@gsnmagazine.com

ADVERTISING SALES

**Vice President/New Business:**
Arnold Blumenthal
(516) 292-0674
ablumenthal@gsnmagazine.com

**Northeast Regional Mgr:**
G. Scott Dinkel
(212) 925-7300 x218
sdinkel@gsnmagazine.com

**NJ and PA Regional Mgr:**
Mike Madsen
(212) 925-7300 x 220
mmadsen@gsnmagazine.com

**Mid-Atlantic & Southern Reg. Mgr:**
Charlie Hull
(301) 987-0632
chull@gsnmagazine.com

**Midwest Regional Mgr:**
Chris Casey
(847) 223-5225 x14
chrisc@caseyreps.com

**Western Regional Mgr:**
Jim Craven
(626) 799-0036
jcraven@gsnmagazine.com

**Classified Advertising:**
Kelly Winberg
(215) 723-2861
kwinberg@attglobal.net

**International Sales Mgr (Europe):**
Dave Harvett
+44 121 705 2120
daveharvett@btconnect.com

CIRCULATION DIRECTOR:
**Ronald Moyer**
(609) 601-1298

FULFILLMENT/ WEB SUPPORT MANAGER:
**Anne Tyler**
(631) 275-0264

PRODUCTION ASSISTANT:
**Jermaine Brown**
(212) 925-7300 x297

PROMOTION DIRECTOR:
**Robert DiGioia**
(212) 925-7300 x274

PRODUCTION DIRECTOR:
**Joe Oakes**
(212) 925-7300 x260

CONTROLLER:
**Allen Frydrych**
(212) 925-7300 x206

GRAPHIC DESIGNER:
**Pat Monteleone**
(212) 925-7300 x321

ADVERTISING TRAFFIC MANAGER:
**Pedro Reyes**
(212) 925-7300 x264

*GSN: Government Security News* (ISSN 1548-940X) is published biweekly except once only in August and December (22 times per year) by World Business Media, LLC, 100 Avenue of the Americas, 6th Floor, New York, NY 10013. Telephone: (212) 925-7300. Periodicals postage pending at New York, NY and additional mailing offices. POSTMASTER: Send address changes to *GSN: Government Security News,* Subscription Department, P. O. Box 2037, Skokie, IL 60076-7937. For government decision makers and business executives involved with security products, systems and services. Qualified U.S. subscribers receive *GSN: Government Security News* at no charge. Non-qualified subscribers in the U.S. are charged $75.00 per year. Canadian and foreign subscribers are charged $140.00. International Airmail subscribers are charged $210.00. Single copy $10.00. The *GSN* Web site is: http://www.gsnmagazine.com



WORLD BUSINESS MEDIA, LLC
**Edward Tyler, President**

BPA WORLDWIDE

**POSTMASTER:**
Send changes of address to:
*GSN: Government Security News*
Subscription Department
P.O. Box 2037, Skokie, IL 60076-7937

**Editorial Reprints:**
Jackie Day
Phone (651) 415-2329
Fax (651) 484-1370
jjday@valeoip.com

**NEW SUBSCRIPTION REQUESTS:**
Write to *GSN: Government Security News*
Subscription Department
P.O. Box 2037, Skokie, IL 60076-7937
or call (847) 763-9617.
Subscribe online at **www.gsnmagazine.com**

**SUBSCRIBER ADDRESS CHANGES:**
Write to *GSN: Government Security News*
Subscription Department
P.O. Box 2037, Skokie, IL 60076-7937
If possible, include a copy of a current mailing label with your correspondence
or call (847) 763-9617.

**SUBSCRIBER INQUIRES:**
Please call (847) 763-9617 or fax (847) 763-9611 or e-mail gsnews@halldata.com

# Hot News

## United Kingdom & Canada will join U.S. for TOPOFF 3

The Department of Homeland Security's (DHS) next large-scale weapons of mass destruction (WMD) counter-terrorism exercise will be a tri-nation, intercontinental affair involving officials in the United States, Canada and, for the first time, the United Kingdom (U.K.).

"The overall aim of the exercise is to test – through a jointly designed exercise – simultaneous U.K., U.S. and Canadian responses to internationally linked terrorist incidents," according to a spokesperson from Great Britain's Home Office.

The April 4-8 "TOPOFF 3" exercise marks the U.K.'s debut as a participant in DHS's international counter-terrorism exercise involving the top officials of each participant's government.

While U.S. participants will be conducting an "on-the-ground" simulation of terrorist attacks on U.S. territory, British and Canadian officials will simultaneously conduct associated table-top exercises in their respective countries.

The U.K. component – dubbed "Exercise Atlantic Blue" – will be a "command post exercise" rather than a live-action simulation in the streets, the U.K.'s Home Office spokesperson said via e-mail from London.

"A Command Post Exercise means there is no operational 'on-the-ground' play," she explained. "But 'live' play takes place at the strategic level."

The spokesperson said officials participating in Atlantic Blue would "respond to international play and content as part of the planned linked exercise."

"This is the best way for us to focus entirely on strategic-level communication issues, rather than on the management of live play at an operational level, which is regularly practiced around the U.K.," she said.

With a cast of hundreds, DHS's office of state and local government cooperation and preparedness will conduct simulated WMD terrorist attacks in Connecticut and New Jersey.

Role players simulate medical response in TOPOFF 2

Although Canadian officials have participated in previous TOPOFF exercises – which come complete with volunteer mass casualty "victims", emergency responders, senior federal and state officials, and even an artificial satellite news network – this year's exercise marks the first time they will be held with governments outside of North America.

At least 800 individuals from federal, state and local agencies stateside, as well as others in Canada and the U.K., are expected to participate in the preparedness event.

In Canada, federal officials and senior officials from the provincial governments of Nova Scotia and New Brunswick will hold their own command post exercise, called "Triple Play", to test and validate the protocols and procedures they would use in response to a terrorist event.

In the U.S., the exercise will simulate a series of terrorist WMD attacks in Fort Trumbull State Park and Ocean Beach in New London, CT.

Because senior government officials, including members of the U.S. Congress, will be participating, DHS has declared a safety and security zone around the New London waterfront areas to protect against accidents, sabotage or direct attacks on the high profile participants.

In the U.K., the Metropolitan Police Service will host the British component of the exercise. U.K. officials have sought to reassure British residents that the WMD exercises, "in no way reflects a specific threat to any of the participating nations." ■

## *Commercial screeners outperform TSA's screeners, say passengers*

The five U.S. airports that still rely on private commercial companies, rather than the Transportation Security Administration, to supply their security screeners consistently scored higher on customer satisfaction surveys of screener performance than the rest of the nation's airports that use federalized TSA personnel.

The survey results, based on random passenger "intercepts" conducted on TSA's behalf by **BearingPoint, Inc.**, of McLean, VA, and its subcontractors, took place between September 2004 and January 2005. Airline passengers at 25 representative airports spread across the country that use screeners employed by TSA and the five airports in a pilot program that use commercial screeners – in San Francisco, CA; Kansas City, MO; Rochester, NY; Jackson Hole, WY; and Tupelo, MS – were asked to complete and mail back customer satisfaction surveys containing eight questions.

On six out of the eight questions, measuring the courtesy and speed of both passenger and baggage screeners, the privately employed screeners received higher "positive" ratings and lower "negative" ratings than their federalized counterparts. On the other two questions, measuring thoroughness and confidence in the security process, the results for both screener groups were essentially identical.

However, in a fact sheet explaining the survey's results for the two different screener groups, TSA chose to ignore the apparent differences and accentuate the positive. "There was very little difference, which shows air travelers have confidence in TSA-trained screeners – federal or private," observed TSA.

Customer satisfaction with all screeners is quite high, says TSA

Under the Aviation and Transportation and Security Act, airports have had the right since last November to request a return to a privately screening force, but as of March 23, only one airport – in Elko, NV – has actually applied for such a change to commercial screeners. However, even the Elko airport is considering withdrawing its application, TSA spokeswoman Amy von Walter told *GSN*. "They thought they could save some money by having their screeners perform other function when they weren't busy screening," said von Walter,

Among the 30 airports evaluated by the BearingPoint satisfaction survey, Daytona Beach, FL, consistently showed the highest customer satisfaction scores while Los Angeles International Airport consistently ranked at or near the bottom.

The survey is part of TSA's broader Customer Satisfaction Index for Aviation Operations which is used by TSA for its annual performance planning and reporting. The complete effort, including survey planning and distribution, data collection and tabulation for all 30 airports, cost approximately $730,000, said TSA. ■

# EPA's inspector general criticizes agency for breaches in its cyber security

Managers at the Environmental Protection Agency (EPA) are catching some heat from the EPA's Office of Inspector General (OIG) after the OIG found several security breaches in the agency's remote data communications access points.

Of the agency's 32 BlackBerry and Web-Mail computer servers, EPA system administrators failed to configure 19 with proper security settings or failed to update them with the latest security patches to protect against outside threats, the OIG said in a recently released audit.

"Consequently, the confidentiality and integrity of EPA data, as well as the availability of the network, is at risk of unintentional or intentional exploitation," the OIG said.

The OIG minces no words when assigning blame.

"The weaknesses occurred because management did not implement processes to exercise proper oversight and provide detailed configuration settings," the OIG said.

OIG auditors also found that some of the agency's BlackBerry devices had no password enabled, permitted users to disable passwords, and in some cases were left unattended.

"These weaknesses occurred because management did not conduct a risk assessment or establish a process to consistently install BlackBerry devices," said the OIG.

EPA personnel may access their office e-mail accounts remotely via an Internet browser using the agency's Web-Mail application. Agency employees and contractors also may communicate using BlackBerry units, wireless handheld devices used to send and receive e-mail remotely.

More than 9,000 users access the EPA network remotely, according to a 2004 internal survey by the EPA's Office of Environmental Information.

"This many remote access connections increases the chances of intentional or unintentional exploitation of the agency's network and the supporting servers," the OIG warned.

The OIG proposed seven remedies, including establishment of new security processes, development of a new security-monitoring program, mandatory security training for system administrators, and a risk analysis of the agency's use of BlackBerry devices.

"They agree with most of our recommendations except the ones related to the BlackBerry issue," said OIG spokesperson John Manibusan. "We told them our concerns about how the agency hasn't conducted a risk assessment, and they don't think they should."

The agency's opposition to the risk analysis is a matter of resources, explained George Bonina, EPA's senior information security officer and director of technical information security staff.

"We pretty much know the risks, and should spend our resources on fixing the risks rather than confirming what we already know," he said.

When asked if updating security patches for EPA servers was routine at his agency, Bonina said his staffers "do that pretty reliably across the networks. The problem was that with this particular set of servers, we relied on the local administrators to do it.

"And in this particular case, we did not check up on them," he said, adding, "But we're fixing that."

The OIG has given the agency 90 days – until late June – to respond in writing with a corrective action plan.

"We can't compel the agency to do anything, but we would hope they would take our recommendations seriously," said Manibusen. "We're just going to have to see what their response is when it comes back in 90 days."

Bonina suggested his agency would move quickly to implement most of the OIG recommendations.

"We work very closely with the IG's office – they help us a lot, and sometimes they are able to surface vulnerabilities that we miss," he said. "Usually in audits like this, we will fix the problem well before the 90 days." ■

# *Nebraska tests digital watermarks for better license authentication*

The State of Nebraska has received nearly $260,000 in grant funding from the **Digimarc Corp.**, of Beaverton, OR, which had earlier won $1 million in funding from the National Highway Traffic Safety Administration to deploy and test its covert digital watermarks on state driver licenses.

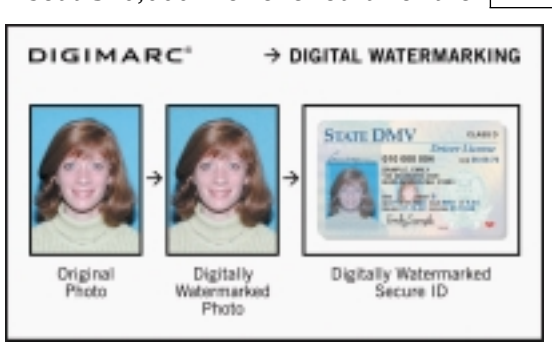
When applied as a covert layer of security to driver licenses, digital watermarks enable fast, machine-readable authentication of IDs, according to the company. The watermarks are imperceptible to the human eye, but not to the machine readers that will be deployed.

"I am genuinely pleased that we will soon have the ability to help protect against financial fraud and identity theft, prevent access to age-sensitive products and aid law enforcement agencies in homeland security efforts," Nebraska Governor Dave Heineman told a March 23 news conference.

The project in Nebraska will identify digital watermark readers and test their use from police cars during traffic stops, at retail locations (particularly to guard against under-age drinking), and at the state's department of motor vehicles.

All of Nebraska's driver's licenses and state identification cards issued since last May have had a digital watermark, said the state government. About 370,000 – or one-fourth of the state's current cardholders – carry a card with a digital watermark.

"Nebraska has been a leader in adoption of advanced safety features in their driver license to combat identity theft and improve roadway safety for citizens," said Digimarc's president, J. Scott Carr. "We are very pleased to engage in this program with Nebraska DMV to demonstrate how authentication of driver license credentials can further enhance traffic safety." ■




**Digital watermarks on licenses are invisible to humans but can be seen by specialized reading machines**

# Martin Consulting lands sole source award from threat office

A consulting firm headed by a former National Security Agency (NSA) official is on tap to win a Department of Homeland Security (DHS) sole source contract to assist in strategic planning for DHS's Threat Vulnerability and Threat Assessment (TVTA) program.


Frederick Thomas Martin

DHS has announced its plan to award **Martin Consulting Associates, Inc.** a sole source contract to help the TVTA "establish key technology partnerships" with other DHS offices, intelligence and law enforcement agencies, other U.S. government agencies, and state and local governments.

The goal of such partnerships will be "to establish awareness of threats against our nation," according to DHS' presolicitation notice.

The Columbia, MD-based consulting firm was founded by Frederick Thomas "Tom" Martin, a former deputy director of the NSA's information services group and currently the executive director of the nonprofit Government Emerging Technology Alliance, also based in Columbia, MD. The company provides consulting and business development services on advanced information technology applications for intelligence agencies, other government agencies and the private sector.

The TVTA program – located within DHS's Science and Technology Directorate (S&T) – receives threat data from various component agencies within DHS. TVTA personnel gather and analyze the data to help S&T make decisions about future projects, according to DHS spokesman Donald Tighe .

"This is a mechanism within Science and Technology to help bring vulnerability and threat awareness into the equation driving S&T investment priorities," said Tighe.

The S&T directorate has what Tighe called "two driving factors in the Science and Technology decision-making matrix."

On the one hand, he said, S&T priorities are based on direct input from DHS "operational elements" – component agencies that express their need for improved tools of entirely new technology.

On the other hand, S&T decisions are influenced by information on "the combination of threat and vulnerability" which is funneled to the directorate's decision makers via the TVTA program, Tighe said.

S&T plans to have Martin's firm evaluate technology in industry, academia and government laboratories; conduct needs analysis and program performance analysis; and provide some information management services, among several other duties.

"[The] contractor is required to have advanced scientific and technology credentials and experience with taking vaguely formulated scientific concepts and problems and transforming them into research and development programs that achieve breakthrough solutions to national security problems," DHS said in its announcement of the award.

Other potential bidders had until March 24 to contact DHS and explain why they should be considered for the contract. ■

# DHS plans to study contacts between militants and technologists

A Northern Virginia firm called the **Institute for Physical Sciences, Inc.**, will receive a sole source contract from the Department of Homeland Security to track "networks associated with suspicious contacts between militants and technologist (sic) worldwide," according to a notice posted on a federal business opportunities Web site.

When contacted at their McLean, VA, offices, two IPS officials declined to comment on the contract or describe their company's capabilities.

A DHS spokeswoman told *GSN* March 23 that commenting on the specifics of the sole source contract and the work entailed would be inappropriate because the contract has not yet been awarded.

"The overall goal of the program is to use IPS's novel, proprietary electronic intelligence collection capability and to fuse that capability with other collection means in support of DHS components and customers," the presolicitation notice states.

The project's presolicitation was posted as "fair notice," according to a federal procurement official with more than 20 years experience. It is a means to inform potential contractors that might have substantive interest and capabilities to perform the described task, and to prompt their proposal for the business.

"DHS has made a decision. They've already determined the only provider that can give them what they want," the federal procurement official added. "The notice is to say we're doing it and we want others to know we're doing it. They have made a decision."

The contract will expect IPS to "develop, identify, monitor overtime, characterize and discover the networks associated with suspicious contacts between militants and technologist worldwide."

In explaining the likely sole source contract, the federal procurement official said it is incumbent on DHS to provide the rationale as to why IPS should be the exclusive contractor, and why other potential firms are excluded.

"Why them? Why is their capability and infrastructure unique? Why are they proprietary?" the official asked. ■

# GAO's homeland security expert examines Coast Guard budget

Margaret Wrightson, the Government Accountability Office's director for homeland security and justice issues offered testimony about the Coast Guard's 2006 budget request to a Senate subcommittee on March 17 – suggesting improvements have been made, but much remains to be accomplished – which sounded all-too-familiar on Capitol Hill.

Wrightson noted that the Coast Guard's overall budget will have increased about 45 percent during the past five years, while the acquisition, construction and improvement accounts – which put money into contractors' pockets – have lept an extraordinary 81 percent during the same period.

Even with a lot more money to spend, however, the Coast Guard has not been all that successful in accomplishing its maritime security-related missions since 9/11, Wrightson testified. She identified three "big ticket" areas in which serious problems remain.

The Automatic Identification System (AIS), which identifies vessels traveling to or through U.S. waters, may cost more to implement than the Coast Guard can afford, she told the Senate Commerce, Science and Transportation Committee's subcommittee on fisheries and Coast Guard. "Consequently, we recommended that the Coast Guard seek and take advantage of partnerships with organizations willing to develop AIS systems at their own expense," she noted.

The Coast Guard estimates that implementing AIS nationwide could cost nearly $200 million, but the agency has been budgeted only $77 million thus far, "leaving a substantial sum to be financed," said Wrightson. The Coast Guard has a contract with **PETROCOMM**, a communications provider in the Gulf of Mexico, but feels it is too early to discuss AIS partnerships with PETROCOMM or any other companies because the Coast Guard is still developing its operational requirements.

The Government Accountability Office is also not happy with the way the Coast Guard has organized itself to assess vulnerabilities and security measures at the nation's 55 most economically and militarily strategic ports. The Coast Guard's efforts in this area lacked a defined management strategy, specific cost estimates and a clear implementation schedule, Wrightson testified. "A major factor of the program – a computer-based geographic information system that would provide information to personnel in charge of port security – was developed in such a way that gaps in port security postures could be overlooked," she observed.

Another Coast Guard security initiative that caught the GAO's critical eye was "Rescue 21," a new coastal command and control system composed of very-high-frequency-FM radios, communication towers and communication centers which is way behind schedule. Wrightson said earlier problems in developing the system software for Rescue 21 had largely been overcome, but large risks still remain in locating sites for about 330 towers that must be built. The construction of these towers must comply with the National Environmental Policy Act of 1969 (NEPA), and that could open a huge can of worms. "Towers can have environmental effects; for example, when they are built in migratory bird locations, birds can fly into the towers or their supporting wires," said Wrightson. The NEPA process represents the greatest risk to Rescue 21's implementation schedule, according to a program official, Wrightson testified. ■

# Around the Country

## CALIFORNIA

Dan Sutherland, an advisor to the Secretary of Homeland Secretary, Michael Chertoff, held meetings with Islamic leaders in Los Angeles, CA, on March 16 and March 17. Among the groups represented at the meetings were the Shura Council of Southern California, Ban al-Wardi, the American-Arab Anti-Discrimination Committee, Salam al-Marayati, the Muslim Public Affairs Council and the Iranian-American Lawyers Association. The sessions were meant to provide a forum for discussing the protection of civil rights and liberties, addressing issues such as racial profiling and creating alliances in the war on terror.

## TEXAS

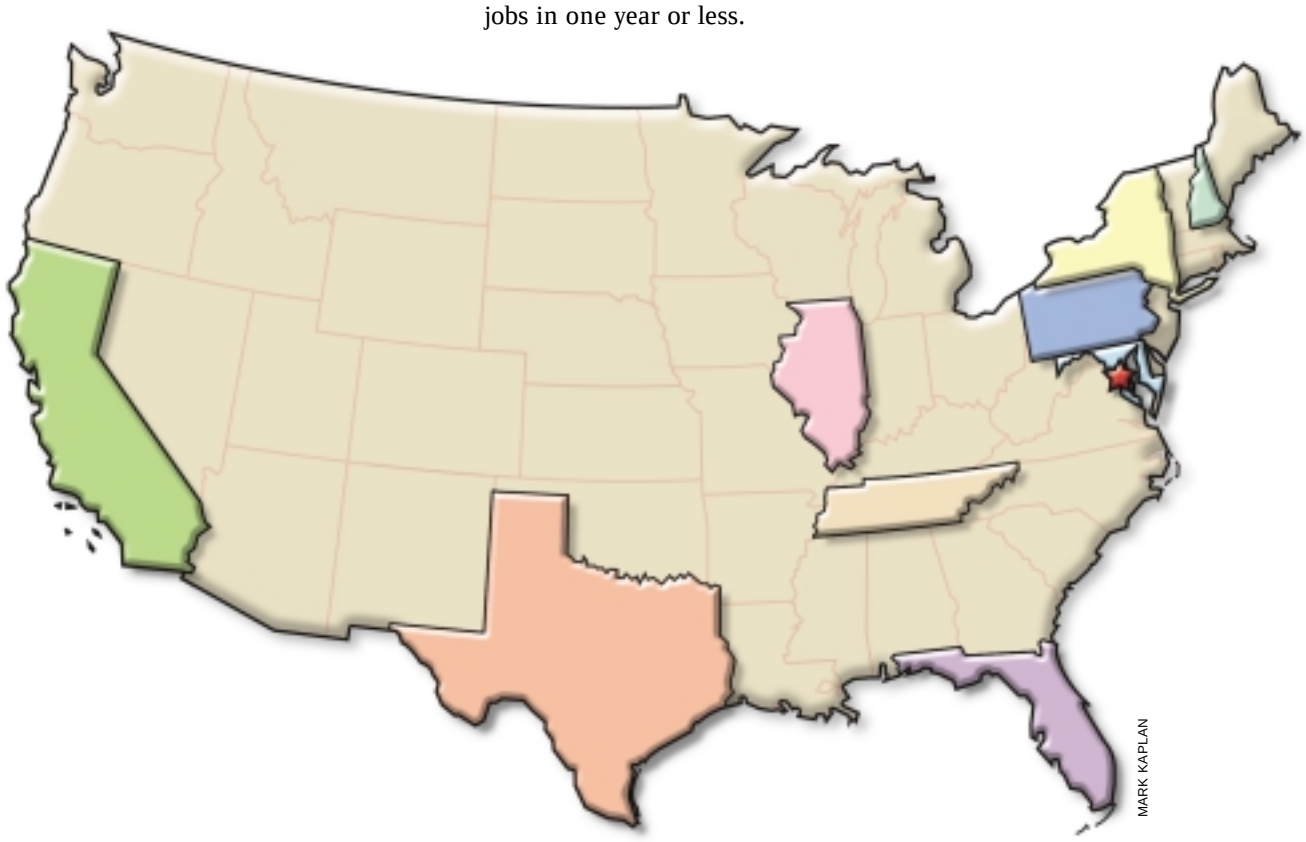
**ADT Security Services, Inc.**, a division of **Tyco Fire & Safety**, of Boca Raton, FL, has donated a digital video surveillance and recording system to Elgin High School, a 950-student public campus in Elgin, TX. The company claims the surveillance system will demonstrate how electronic security technologies can assist school administrators in building positive learning environments. ADT is donating 22 high-resolution day/night cameras and a digital video management system that offers video-based motion detection, object search and digital video enhancement. An observation monitor will be housed in the front office to display selected views from the cameras.

## ILLINOIS

The Illinois House of Representatives human services committee has passed a homeland security bill, called the "Anti-Terrorism and Aviation Protection Act," to keep terrorists from using .50 caliber sniper rifles to shoot down civilian airliners during landings or takeoffs. The bill was sponsored by Rep. Elaine Nekritz (D-57th) and Rep. Beth Coulson (R-17th) who have started a bipartisan initiative to keep terrorists from securing .50 caliber rifles, which were designed to puncture armor, and attack personnel carriers and fuel tanks during battle.

## NEW YORK

According to a report from the Public Advocate's Office, the standards for New York City's private security officers are extremely low. The study included interviews of more than 100 privately contracted security officers in 29 major Class A commercial buildings. It found that, despite the heightened interest in security after September 11, most officers have minimal training and that there are limited enforcement of training requirements, leaving New York with an ill-prepared private security force. The study found wages to be low and health benefits either unaffordable or non-existent, with resulting personnel turnover, not surprisingly, being high. Nearly 25 percent of the officers leave their jobs in one year or less.




## NEW HAMPSHIRE

Worldwide Information, Inc., a wholly owned subsidiary of **LocatePlus Holdings Corp.**, of Beverly, MA, has partnered with the State of New Hampshire Department of Safety to implement WWI's technology to integrate an Intranet-based database of the state's department of motor vehicles, including drivers' license records. State and local law enforcement agencies as well as federal government personnel will be able to remotely access the highly specialized database.

## PENNSYLVANIA

Rep. Bernie Thompson (D-MS), ranking member of the House Homeland Security Committee, is looking into a recent no-bid contract awarded by the Department of Homeland Security to Mercyhurst College, in Erie, PA, to train intelligence analysts. The college has a close association with former DHS secretary Tom Ridge and even plans to name a building after him so the no-bid contract was bound to raise a few eyebrows, Thompson said. "The Department cannot pay patronage games when America's security is in question," he explained. In a letter to Secretary Michael Chertoff, Thompson gave DHS 14 days to respond to a list of questions regarding the contract award "to better understand the department's rationale" He noted that there was "simply no excuse for not providing details of the contract."

## TENNESSEE

In a March 4 decision, the Government Accountability Office has sustained a protest lodged by **Keeton Corrections, Inc.**, of Panama City, FL, which objected when the Federal Bureau of Prisons awarded a contract to a rival company, **Dismas Charities, Inc.**, of Louisville, KY, to provide "employment and residence development" services to federal offenders living in a halfway house in Nashville, TN, known in government parlance as a Comprehensive Sanction Center. The Comptroller General determined that the contracting officer for the bureau of prisons did not adequately evaluate the "past performance" of both candidates, which was considered the most important selection criteria for this contract. "We conducted a hearing in this case because the evaluation documentation prepared by BOP did not adequately explain the agency's evaluation and selection of Dismas's proposal for award," said the GAO's decision.

## FLORIDA

The JAXPORT seaport in Jacksonville, FL will be able to expand its use of a wireless security program provided by **I.D. Systems, Inc.**, of Hackensack, NJ, that tracks the location and status of several hundred vehicles at the port. With additional funds from the Transportation Security Administration, the Florida port will be able to move into a Phase II expansion of a program initiated in July 2004. "Using local area networks, wide area networks, and the Internet, the company's systems enable management to control and track the location and status of their assets – from forklifts and cranes to automobiles and trucks – in real time," said I.S. Systems in a March 24 announcement.

## WASH., D.C.

The U.S. Departments of Justice, Homeland Security and Transportation, in addition to three leaders in Congress, have voiced their opposition to the District of Columbia's ban on the transportation of hazardous materials. The opposition to the ban came down on the side of CSX Transportation and the railroad industry, which would like to see the ban rejected. The departments and congressional leadership claim that the ban actually makes it more dangerous to transport hazardous materials by increasing the time and distance the materials must travel.

## MARYLAND

The Maryland Emergency Management Agency (MEMA) has turned to WeatherBug from **AWS Convergence Technologies, Inc.**, of Gaithersburg, MD, to provide a common weather intelligence platform to be used by all emergency management officials. The 290 WeatherBug Tracking Stations scattered across the state gather live local weather data that MEMA can use to enhance its analysis and responsiveness in daily operations and emergency situations. By standardizing on WeatherBug Streamer, MEMA, the state Emergency Operation Center (EOC), county management coordinators and Baltimore City and Ocean City emergency managers can get advanced warning and detailed information on severe weather conditions, gather more accurate data for plume modeling, and more timely information to make emergency responses more effective.

*For submissions to this section, please e-mail detailed information to:* around@gsnmagazine.com

From Page 1

# Some experts say urban transport has been shortchanged

David Gaier, a consultant and former vice president of the security services division of New York-based **Urbitran Associates**, said bluntly of the huge funding disparities, "TSA might as well be 'The Commercial Aviation Security Administration.' The government really ignores transit."

And, ultimately, this means that cash-strapped cities might be left to pony up the dollars to eliminate the discrepancy.

The harsh truth is that "there isn't nearly enough money to do everything we'd like to do," a New York City transit official told *GSN*. And that's likely to leave a real gap in security, considering that non-aviation travel makes up the bulk of transportation in this country. Of the billions of journeys that take place daily, the American Public Transportation Association says that 16 times as many trips are made by rail and bus as by airplane. Safeguarding the nation's gigantic rail, bus, and maritime infrastructures, then, has become an alarming numbers game.

As head of the 215-member Bay Area Rapid Transit (BART) police, San Francisco Transit Police Chief Gary Gee is not convinced that aviation security should be funded at the expense of surface modes. Referring to the DHS/TSA funds for metropolitan systems like his, Gee told *GSN*, "Grant awards are sent to the states and divvied up among the counties. That leaves transit systems, like BART, which are separate government entities, groveling for handouts."


And cities and regions must compete with each other for priority. For example, among the presumed terrorist targets in San Francisco are the Golden Gate Bridge and many federal and local government facilities. However, notes Gee, "The West Coast and SF Bay Area are vulnerable as 'soft targets,' largely because New York City and Washington DC are fortresses in comparison." Gee said he is "even more concerned" by proposals that "DHS Urban Area Security Initiative funding for the West Coast will be cut further and diverted to the East Coast." He emphasized that while less than $200 million is to be parsed out nationwide for public transit, "BART's wish list alone for security and target-hardening, most of which would be for technology, is almost $100 million."

Lack of funding is only part of the problem of ensuring non-aviation security. Many cities are simply slow in spending their security dollars. Said Gaier, "Some of the larger transit systems are sitting on security money, wringing their hands. New York City's MTA has almost $591 million of which they've only spent a fraction. Their spokesman said that MTA is taking its time to ensure that it's spent wisely, but there are a dozen proven best practices that could and should have been put in place long ago: roving security inspections, more canine teams, intrusion detection and monitoring; and passenger awareness programs, to name just four."

In addition, the rail systems of New York and other cities "haven't even begun to deal with the issue of passenger evacuation and station fire protection, "said Gaier. "This is a huge vulnerability to the massive loss of life in otherwise survivable events. A former high-ranking New York City DOT official told me recently that he tried to get the city to deal with the issue of evacuating passengers from the East River bridges 10 years ago, and nothing has been done."

Gaier ticks off more things that transit operators could be doing, citing what Boston's WMTA has pioneered: "Roving inspections, where they get on and off trains, so people can't time the inspections. And you do that sometimes with bomb-sniffing canines. But we don't have nearly enough canine teams. Part of best practices is just walking through trains and asking, 'Is that your package?'"

He also called for better deployment of National Guard personnel who have been seen in New York and other systems. A former U.S. Marine and U.S. State Department security agent, Gaier observed that the National Guard aren't "trained as transit police, and there often appears to be no solid chain of command. Military people aren't trained to take orders from civilians, and vice versa. They're not law enforcement officers and, frankly, they aren't security officers."

He noted that "security and law enforcement aren't the same thing. The whole idea that putting bodies in uniform with some guns and having them stand around in clusters drinking coffee makes our transit system safer – I don't believe that for a moment."

Said Gaier, "We have put about $12 billion in commercial aviation security and yet it's no more secure than it was 17 years ago, according to the GAO and the DOT's own inspector general (recently fired). Think about what just a quarter of that money could do for public transit."

But even air security still has a potentially fatal flaw – one shared by ground transport, according to Gaier: "We're only inspecting 10 percent to one-quarter of all the cargo on passenger airplanes, a major gap left unaddressed. But we're checking each passenger's boarding pass and driver's license four times."

BART's transit police chief Gary Gee (l) and consultant David Gaier

Similar problems persist in the maritime domain, he said. "Just upping the number of inspections of cargo ships and containers – currently about five percent of the total – to 15 percent would help." As for universal screening of passengers and baggage in commuter rail, that is "impossible for the foreseeable future, given existing infrastructure and passengers' intolerance of delays and inconvenience." Former DHS under secretary Hutchinson agreed, calling full screening "impractical" – a conclusion perhaps only a significant fatal attack is likely to change."

Besides the daunting logistics of cargo screening, Gaier suggests that an equally big obstacle to effective security – in the air and on the ground – is lack of strategic planning pegged to risk assessment. "TSA and the airlines treat everyone the same, rather than using a risk-based approach. That's why white-haired grandmothers of Norwegian extraction from Minneapolis and 4-year-old kids wearing Blues Clues T-shirts get the same treatment" as likelier high-security risks. Random screening "is just madness. It doesn't make us more secure, it just makes traveling unpleasant. And transit security professionals often have the same one-size-fits-all approach to risk evaluation and management."

Gaier added, "A deputy police chief of a major transit system told me, 'We see everything as a weakness and don't emphasize one thing over another.' That's just not smart security. We can't protect every person or asset from every source of harm, nor should we try. But if transit operators can't or won't prioritize, then security and safety are just a crap shoot."

The status quo is less than reassuring. "We're really just trying to narrow the odds" in favor of protection, said Gaier. "It's a numbers game."

As San Francisco's transit police chief Gee concludes, "Until there are transit-specific allocations, like there were for aviation post-9/11, transit systems will continue to struggle." ■

# Business Opportunities

*Recent and upcoming government solicitations*

## Federal Protective Service to Buy Veterinarian Services for Canines

**Buyer:** Immigration and Customs Enforcement-Federal Protective Service
Third & M Streets, S.E.
Southeast Federal Center
Building 136
Washington, DC 20528

**Scope:** Veterinarians are needed to care for canines housed at FPS for a base of one year with two optional 12-month periods. The contractor will provide veterinary services for 15-30 dogs during each year of the contract.

**Status:** Responses are due April 12, 2005.

**Contact:** Claire Cashwell, contracting officer
202-205-2817
202-205-9527 9 (Fax
clairej.cashwell@dhs.gov

## DHS Needs Support for Human Resources Operations

**Buyer:** Department of Homeland Security
Washington, DC

**Value:** $60 million over five years

**Scope:** DHS headquarters is seeking full-service personnel operations support for about 2,250 employees during FY2005. Approximately 400-450 positions must be recruited and filled by September 30, and additional policies and procedures must be performed. The contractor will supply strategic recruitment and placement services and help shape policies to comply with laws, regulations, procedures and financial requirements. The contractor will also be involved in managerial and employee training as DHS transitions to a pay-for-performance system in FY2006, and should also be able to support payroll processing, employee and labor relations, retirements and benefits and time and attendance.

**Status:** The notice was originally posted on February 23 with responses due back March 11, 2005.

**Contact:** Leah Wilson, contract specialist
202-357-8328
202-357-0016 (Fax)
carolyn.smith@dhs.gov

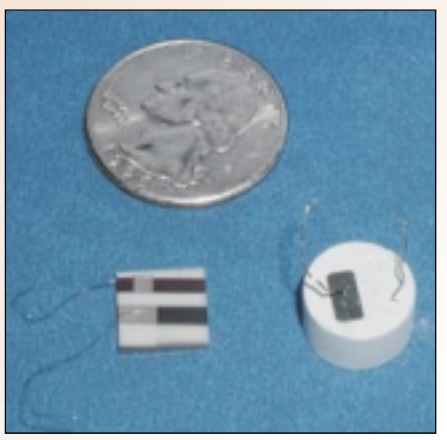
## DHS Private Sector Office Seeks Help with Operations Management Roundtable, Information Risk Executive Council

**Buyer:** DHS – Office of Chief Procurement Officer
Washington, DC 20528

**Scope:** The Private Sector Office needs contractor to research unlimited access to certain proprietary strategic research as well as manage an annual executive retreat, staff briefings, provide access to custom project library of proprietary research, provide unlimited, unrestricted access to a password-protected Web site and perform other analysis and technical assistance that can help the PSO support its programs.

**Status:** Request was posted on March 11 with responses due back by March 25, 2005.

**Contact:** Carolyn Smith,
contracting officer
202-205-4515
202-772-9729 (Fax)
carolyn.smith@dhs.gov



## Los Alamos National Laboratory Needs Companies for Licensing and Collaborative R&D on Solid State Gas Sensors

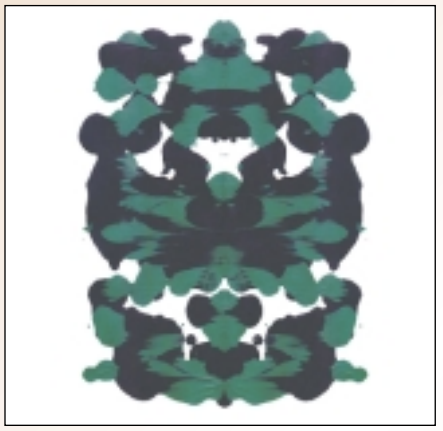
**Buyer:** Department of Energy
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545

**Scope:** The University of California, the contractor that runs Los Alamos, is looking for companies to participate in licensing and collaborative research and development with Los Alamos National Laboratory in the area of solid state gas sensor technology. Among the applications is explosives detection.

**Status:** Letters of interest were due April 1, 2005.

**Contact:** Charles Gibson,
licensing associate
505-667-8087
505-665-0514 (Fax)
charliegib@lanl.gov





## ICE Looking for Psychological Testing Evaluation Services

**Buyer:** Immigration & Customs Enforcement
425 I Street, N.W.
Washington, DC 20536

**Scope:** ICE is seeking psychological testing evaluation services to help Cyber Crimes Center and Law Enforcement Support Center personnel identify problems that keep employees from effectively and consistently performing required tasks.

**Status:** The RFP was expected to be posted by March 31, 2005.

**Contact:** Ronald Jean-Baptiste, contract specialist
202-307-9935
202-514-3353 (Fax)
ronald.jean-baptiste@dhs.gov

## U.S. Coast Guard Requires Custom On-site IntruShield Training

**Buyer:** U.S. Coast Guard
USCG Telecommunications & Information Systems Command
7323 Telegraph Road
Alexandria, VA 22315-3940

**Scope:** The Coast Guard Computer Incident Response Team, which monitors the Coast Guard's networks for intrusion detection and security analysis needs an advanced IntruVert training course for operators of the "IntruVert Intrusion Detection & Prevention System" from McAfee, Inc.

**Status:** Responses were due March 22, 2005.

**Contact:** Jay Shively, contract specialist
703-313-5466
703-313-5458 (Fax)

*For submissions to this section, please e-mail detailed information to:* **opportunities@gsnmagazine.com**

# People

Pelican Products, of Hyrum, UT, has named **Scott Ermeti** vice president of marketing and international business development in charge of the company's global marketing, advertising and new business initiatives. He will also head Pelican's European and Canadian business units. With more than 20 years of strategic marketing, sales and general management experience, Ermeti was most recently managing director and vice president of Pelican's European operations. He holds a masters degree in business administration from the University of Chicago and a bachelor's degree from Indiana University.

**Howard Schmidt**, formerly White House cyber security advisor as well as the chief security officer at Microsoft, has joined the board of directors at PatchLink Corp., of Scottsdale, AZ. Joining him on the board is **Irfan Salim**, a security industry executive. Schmidt also was chairman of the Critical Infrastructure Protection Board in the current Bush administration. He has also served as a supervisory special agent and director of the U.S. Air Force Office of Special Investigations Computer Forensic Lab and Computer Crime Information Warfare Division. Salim has more than 10 years experience in developing Internet-based network security offerings.

SAFLink Corporation, of Bellevue, WA, has named **Asa Hutchinson** to its board of directors. A founding member of the Department of Homeland Security, Hutchinson became under secretary of DHS for border and transportation security in January 2003. Before joining DHS, Hutchinson headed the U.S. Drug Enforcement Agency for two years and was a three-term member of the House of Representatives. He became the youngest U.S. Attorney in 1982 when President Ronald Reagan appointed him to the Western Arkansas region.

Armor Holdings, Inc., of Jacksonville, FL, has moved **Scott O'Brien** from Armor Holdings's Safariland, Inc., where he was president and COO, to the company's products division, where he is now president. He replaces Steve Croskrey, who is leaving Armor Holdings. O'Brien joined Safariland in 1974 and became president and COO in 1993.

**Jack Lyons** has been named vice president and chief financial officer at Integral Technologies, Inc., of Indianapolis, IN. With more that 14 years of industry experience, Lyons has a background in security. He holds a bachelor of science degree in accounting and business administration from the University of Indianapolis. He is a CPA as well as a member of the American Institute of Certified Public Accountants and the Indiana Society of Certified Public Accountants.

Strategy X Inc., of Harrison, ME, has appointed **Wayne Hawkins** as senior vice president and director of operations (SIIM) division in the Crestview, FL, location. Hawkins brings to the position more than 30 years of experience in physical security. He will be responsible for the daily management of the Crestview operations and will assist in long-term planning, negotiating projects and developing teaming agreements among his other duties. He is a 20-year veteran of the U.S. Air Force. He was chief of security systems analysis for the Strategic Air Command (SAC), where he performed antiterrorism assessments and conducted force-on-force exercises for all SAC installations. In addition, he developed the Air Force's first Antiterrorism Threat Condition Program.

**Joe Whitley** has resigned as general counsel in the Department of Homeland Security. The first general counsel of DHS, sworn in on August 1, 2003, Whitley submitted his letter of resignation to President Bush in early March and no resignation date has been set. Whitley served as associate Attorney General under President George H.W. Bush, and holds the distinction of being the only Senate-confirmed U.S. Attorney ever to be appointed in two different federal judicial districts. Homeland Security Secretary Michael Chertoff called Whitley a friend who "played an important role in furthering the progress and critical mission of this new department, while ensuring that our efforts to secure the nation have been consistent with the rule of law."

**Lieutenant General Patrick Hughes (Ret.)** has become vice president of homeland security at L-3 Communications, Inc., in New York City. He will coordinate efforts in the company to capitalize on synergies between products and divisions so that L-3 can meet the needs of the expanding homeland security market, law enforcement and government agencies. His last post in the U.S. Army was as director of the Defense Intelligence Agency. He has a bachelor's degree in commerce from Montana State University and a master's degree in business management from Central Michigan University.

**Michael Jackson** was confirmed by the U.S. Senate as deputy secretary of the Department of Homeland Security. Secretary Michael Chertoff swore him in on March 11. According to Chertoff, Jackson's "management experience in public and private service will be extremely valuable to the Department and its vital mission."

*For submissions to this section, please e-mail detailed information to:*
people@gsnmagazine.com

# Contracts

## GE InVision Wins TSA Contract for EDS Maintenance

**Issued by:** Transportation Security Administration
Washington, DC

**Issued to:** GE InVision, Inc.
Newark, CA

**Value:** $36 million

**Scope of Work:** GE InVision, Inc. has landed a contract with TSA to provide maintenance for about 800 GE EDS machines. The contract will run through September 30, 2005 and has four one-year options. The company will be responsible for both scheduled and unscheduled maintenance for existing EDS equipment in airports as well as for those machines that will be purchased during the course of the contract.

**Announced:** March 14, 2005

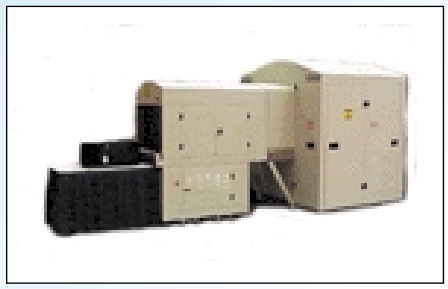
## TSA Intends Sole Source Contract with Grant Thornton to Continue ABC Study

**Issued by:** Transportation Security Administration
Arlington, VA 22202

**Issued to:** Grant Thornton, LLC
Chicago, IL

**Scope of Work:** ITSA intends to award a sole source contract to Grant Thornton to continue its initial Activity-Based Costing study. The agency is looking for data to further validate the original findings by adding airports to the model that has been developed. Fifteen airports were included in the original study, which represents only three percent of all airports with a TSA presence. The data collected will be used to evaluate the true cost of operations for airports that apply for the Screening Partnership Program.

**Announced:** March 11, 2005



## L-3 Communications Lands TSA Contract for EDS Maintenance

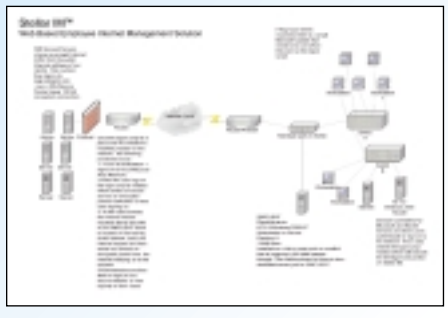
**Issued by:** Transportation Security Administration
Washington, DC

**Issued to:** L-3 Communicatons, Inc.
New York, NY

**Value:** $28 million

**Scope of Work:** L-3 Communications has landed a contract with TSA to provide maintenance for about 500 L-3 EDS machines. The contract will run through September 30, 2005 and has four one-year options. The company will be responsible for both scheduled and unscheduled maintenance for existing EDS equipment in airports as well as for those machines that will be purchased during the course of the contract.

**Announced:** March 14, 2005



## Cook County Selects Stellar Technologies to Provide Internet Management Solution

**Issued by:** Cook County, Illinois

**Issued to:** Stellar Technologies, Inc.
Naples, FL

**Scope of Work:** Cook County, IL, the second largest county in the U.S., has chosen Stellar Technologies, Inc. to provide Stellar IM to serve as the county's Internet management solution of choice. Stellar IM will help county officials manage instant message communications and Web usage throughout the county. Officials will be able to monitor employee Web browsing and IM activity. Stellar IM offers secure online reporting that features role-based access, high scalability and ease of use.

**Announced:** March 4, 2005

## TSA Selects CSC to Support Vetting and Credentialing HazMat Truck Drivers

**Issued By:** Transportation Security Administration
Washington, DC

**Issued To:** Computer Sciences Corp.
El Segundo, CA

**Value:** $16 million, if all options are exercised

**Scope of Work:** CSC will provide support for TSA's office of transportation vetting and credentialing, which conducts security threat assessments for commercial truck drivers seeking a hazardous materials driver's license. CSC, along with subcontractor Trinity Technology Group, of Fairfax, VA, will provide approximately 40 security adjudication professionals for support.

**Announced:** February 22, 2005

## Performance Assessment Network to Land Single Source Contract from TSA

**Issued by:** Transportation Security Administration
Arlington, VA

**Issued to:** Performance Assessment Network, Inc.
Alexandria, VA

**Scope of Work:** The TSA plans to award a contract to Performance Assessment Network to support the Federal Flight Deck Officer Program. PAN has already developed from scratch the information technology infrastructure that meets the needs of the FFDO program. The new contract will include the maintenance of the online infrastructure, which serves as the underpinning of all phases of the program's assessment, selection and operational processes.

**Announced:** March 10, 2005

## U.S. Secret Service Negotiates Sole Source Contract with Harlan Consulting Services for Diversity Training

**Issued by:** U.S. Secret Service
Washington, DC

**Issued to:** Harlan Consulting Services Inc.
Houston, TX

**Scope of Work:** The U.S. Secret Service intends to award a sole source contract to Harlan Consulting Services to continue diversity training at the agency.

**Announced:** March 9, 2005

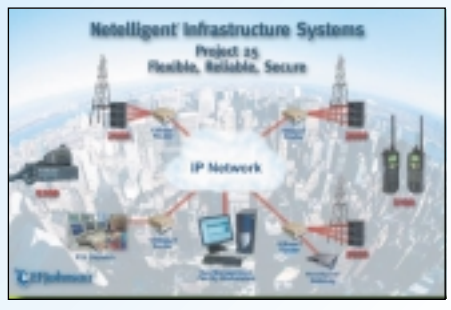
## U.S. Coast Guard Set to Award Sole Source Contract to CoCo Communications for Hardware, Software Modifications

**Issued by:** U.S. Coast Guard Research & Development Center
Groton, CT

**Issued to:** CoCo Communications Corp.
Seattle, WA

**Scope of Work:** The U.S. Coast Guard Research & Development Center plans to award a sole source contract to CoCo Communications to modify its existing hardware and software to provide U.S. Coast Guard boarding teams with uninterruptible communications while they are inside ships. The terms of the contract require the hardware and software to comply with 802.11 wireless specifications and must protect both the data and the path.

**Announced:** March 10, 2005




## EF Johnson Lands $1.3 Million Order from Illinois Emergency Services Management Association for National Terrorism Task Force

**Issued by:** Illinois Emergency Services Management Association
Chicago, IL

**Issued to:** EF Johnson - EFJ, Inc.
Irving, TX

**Scope of Work:** EF Johnson has been awarded a contract to provide the Illinois Emergency Services Management Association with its "Netelligent" infrastructure system, radios and repeaters. The equipment will be used for the National Terrorism Task Force efforts in Illinois. The offerings will be used in nine trailers deployed across the state and outfitted with repeaters, portable and mobile radios, satellite uplinks and other equipment.

**Announced:** March 10, 2005

*For submissions to this section, please e-mail detailed information to:* **contracts@gsnmagazine.com**

From Page 1

# Nuke detection office opens

of the Defense Nuclear Agency's Counterproliferation Program Office.

"DNDO will be developing, acquiring and supporting the deployment of a domestic system to detect and report attempts to import, assemble, or transport a nuclear explosive device, fissile material or radiological material for illicit use," said the DHS staffer, who requested anonymity.

As currently envisioned, the DNDO will focus on two major activities. "DNDO will have a basic systems development and acquisition group and a different group that's doing transformational technology," the staffer told *GSN*.

The transformational technology group will conduct basic research into new concepts that might be developed and deployed at a later date, he explained.

The new office will operate within DHS and be staffed with personnel from DHS and the Departments of Energy (DOE) and Defense (DoD) and the Federal Bureau of Investigation. The DNDO staff will coordinate its work with the Departments of Justice and State, intelligence agencies and other governmental departments.

Just two days after Chertoff formally opened the new office for business, DNDO officials issued a "sources sought" notice, seeking to identify firms capable of providing a broad array of engineering services.

According to the notice, DHS intends to award a five-year blanket purchase agreement (BPA) under which the contractor must have the ability to provide DNDO with an extensive list of services, including: strategic planning; concept development; requirements analysis; systems engineering; testing and evaluation, and acquisition management. The winning contractor would perform specific tasks as needed throughout the period of performance.

Under the BPA, the vendor will "assist us in developmental product specifications, product tests, and reviews of product delivery — that whole gamut of things that are typical in the DoD model," he said.

"They will not be assisting in standing up the office. They're really being hired to do the acquisition part of this work," the staffer emphasized. "They're going to be doing the nuts and bolts engineering, research, systems specifications — not delivering the product, but defining what we need."

He acknowledged that DNDO will likely be looking for a large systems integrator capable of doing the work. "We have a fairly large skill set that we're looking at," he said.

The staffer said he could not reveal the dollar value of the contract until DHS issues the solicitation, probably in the second or third week of April.

Although the new office is up and running and will soon issue its first major solicitation, the DNDO does not yet have its own budget to fund the upcoming contract award. "Most of it will be paid from next year's dollars, but I imagine there will be some seed money from this year's dollars," said the staffer.

According to Donald Tighe, spokesperson for DHS' science and technology directorate, the new DNDO is currently being funded from S&T's radiological and nuclear countermeasures portfolio.

But the DNDO would see a major increase in funding next year under President Bush's proposed FY06 budget. "The '06 budget proposes $227 million for it. In the '06 budget, approximately $114 million of that is new," said Tighe.

About $113 million of the proposed DNDO FY06 budget would come from S&T's radiation and nuclear countermeasures portfolio, he explained. DNDO's programs would be supplemented by the budgets of some of the DHS operational units involved in protecting against a "rad/nuke" terrorist attack, such as CBP and TSA, which will be purchasing some radiological and nuclear materials detectors with their own funds, said Tighe.

Among the more significant of DNDO's planned projects will be the creation and operation of a new data integration center to receive, monitor and analyze nuclear and radiological risk, threat and vulnerability data on a real-time basis, said Tighe.

"The DNDO will establish and manage a Joint Center for Global Connectivity — a hub of situational awareness integrating information from domestic and international detection systems," he said "The job of that unit will be to integrate all of that information." ■

# Ask The Expert

Peter Tippett,
Chief Technology Officer at Cybertrust Inc.

Within 30 seconds of meeting Peter Tippett, the provocative chief technology officer at **Cybertrust Inc.**, of Herndon, VA, it becomes obvious Tippett is an original thinker who doesn't hesitate to call things as he sees them. Having earned both MD and PhD. degrees from Case Western Reserve University, Tippett studied under two Nobel Prize laureates at Rockefeller University. Something of an IT security visionary, Tippett helped create the first commercial anti-virus product, which later became Symantec's Norton Anti-Virus. *GSN's* Jacob Goodwin began a conversation with Tippett trying to understand why software is so often plagued with security vulnerabilities, but Tippett quickly took the discussion far beyond that initial query.

**Q Why are there so many security flaws in software?**

A It's a mindset. It's like asking the question, "Why are there so many flaws in automobiles or airplanes?" You say, "Well, what if I were to drop a bowling ball off of a tall building and it hit the roof of a car, wouldn't that kill the driver?" The answer is, "Yes." People would throw up their hands and say "Oh my God, Ford has got inherent flaws in its automobiles, why aren't they thinking about this?" And they'd say "Well, because we've discovered this new vulnerability, we'll put titanium roofs on all cars."

Then, somebody would come out and say, "Well, yeah, but what if I saw a laser through the windshield. Isn't that an inherent flaw in the car? Wouldn't it blind the driver and then he would crash? Oh my God, we'd better put out laser proof windshields."

What we've focused on is vulnerabilities in computers instead of risks. If you focus on vulnerabilities, you're going to come up with thousands a year, no matter what you're talking about – cars, airplanes, anything.

**Q So are you suggesting that this obsession with vulnerabilities is misplaced?**

A Misguided.

**Q Why is it misguided?**

A It's misguided because it's crazy. Of the 4,000 vulnerabilities we "discover" and publish every year, less than one percent are ever actually used in any attack against any company anywhere in the world. So, although they exist, it's like the bowling ball hitting the car, who cares? Are you going to fix every car in the world because somebody might drop a bowling ball off the Empire State Building? I don't think so.

**Q So what do you do to address the fact that a small percentage of the vulnerabilities are exploited in measurable ways with measurable financial impacts?**

A It boils down to this: the right approach to computer security is the same as the right approach to automobile and airline safety. You can't prove a negative. You can't make a safe car. You can't make a safe airplane. A safe airplane would be one that could run into a mountain at 600 knots and everybody gets home and says, "Well, we spilled the drinks back there a few hours ago. Lousy pilot." That would be a safe airplane.

Or a safe car that could run off a cliff and drop three thousand feet into a granite wall and everybody says, "I'm sorry we're late for the party." Those would be fundamentally safe, but there's no such thing as a safe car, a safe airplane or a safe computer and there never will be. There's a coding flaw for every hundred lines of code written over the whole length of time that we've ever written code. We can get that down to one flaw per thousand lines, but we're never going to get it to zero.

**Q Is it a worthwhile effort to go from one per hundred to one per thousand or one per ten thousand? Are people who are trying to push for better and better code misplaced and misguided, or is that an appropriate goal?**

A It is one of many things to do. It's like saying, "Airplanes ought to have stronger wings because in one out of 50,000 attacks, the wing strength is involved." Okay, that's true, so should they strengthen the wings in all airplanes? What we really need to do is identify what things will be the most powerful to reduce the most risk for the most people.

In cars, for example, it turned out to be seatbelts, which reduce the likelihood of dying about 50 percent. If you go to a computer security guy and say, "I'm going to give you something that will cost you a dollar and it will reduce your likelihood of being hacked by 50 percent," he'll tell you it's a worthless thing. The other 50 percent won't work. In cars, we say it's a great thing. It reduces your likelihood of dying by half.

**Q What role do you see for the government in understanding what you're describing and implementing improvements along those lines?**

A I think the government's role boils down to figuring out which metrics work – how to measure risk in a reasonable way. Not how to make a list of things that people think you ought to do. Almost half the things that are on the list that we all tell each other we ought to do have no value in reducing risk. Longer passwords don't reduce actual attacks. Encrypting Internet traffic doesn't reduce actual attacks. Those things don't actually work. Instead of just arbitrarily listing things that we think ought to work, we ought to do what we do in cars and airplanes, which is figure out which things do work.

For example, half an hour's work on the routers in your company reduces the likelihood of hacking by 80 percent. Do people do this? No. Why not? It's only 80 percent effective. Well, 80 percent effective reduces the likelihood of having an attack by 80 percent.

**Q Do you think the government is anywhere near seeing it this way?**

A No. This is an "Earth is round / Earth is flat" problem. The government and everybody else are into "Earth is flat" thinking. We're all following each other off the cliff, trying to do whatever anybody says is the right thing to do, instead of figuring out which things work better and which things are cheaper and which things are more efficient and which things are more effective.

At an organizational level, this is incredibly important because there isn't infinite money and if you want perfect security you need infinite money. So, given that we have finite money, we have to decide where we're going to spend it. In making those choices, it's incredibly important to understand how risk metrics work. That's something that Cybertrust does, of course. We determine which risk metrics work and where to put the few dollars that you've got.

**Q What conclusions have you reached as to where to put the next dollars?**

A For organizations – whether they're government agencies or other organizations – it tends to be simpler things that tend to work 60 or 70 or 80 percent of the time for a particular threat scenario, instead of the things that seem to work 99.99 percent of the time, but cost you a lot more money and energy. Almost everybody wants to buy a box that's a better firewall or a better intrusion detection system or a better intrusion protection system or to update their anti virus stats, or whatever. It turns out none of those things actually reduces risk in a reasonable way, compared to doing the simpler things that are cheaper, like changing your settings, having some policies, having a program that gets people doing the right kinds of things.

Teaching pilots to be better pilots, getting people to drive on the right side of the road, encouraging them to stop at stop signs. These things all reduce the likelihood of dying in automobiles. Adding force fields around the drivers might help, but it's certainly not as easy and as cheap as doing the simpler things.

**Q Why is the IT security industry going in one direction when, by your logic, it should be going in another direction?**

A It's like the classic "Earth is flat" problem. The IT security industry and all computer security people are focused on things that are single-computer oriented. If you ask how to do something, they think in terms of a single computer. They're binary thinkers. We think that computers are binary; therefore security must be binary. Therefore, if you show me something that's perfect, I'll like it. If it's not perfect, I won't like it. But risk isn't binary. They are binary single-computer and vulnerability-oriented thinkers.

We worry about vulnerabilities alone when we really ought to worry about vulnerabilities that are also associated with logical threats, that is, "Will bowling balls really be falling?" If you take those concepts together, and use that as a risk model for your thinking, it turns out that most vulnerabilities aren't worth fixing because there will be no threats associated with them. ■

# New Products, Systems & Related Services

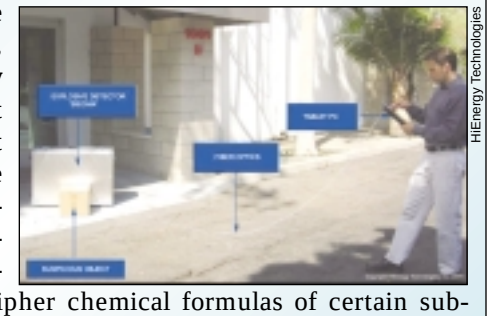
## PHYSICAL SECURITY

### MSA Advances Thermal Imaging Camera Technology

A new thermal imaging camera (TIC) from **MSA North Americ**a, of Pittsburgh, PA, employs high-quality imaging that operates in temperatures in excess of 300 degrees Fahrenheit. The company claims it will substantially enhance firefighter safety and effectiveness in life-threatening situations. The "Evolution 5200" TIC features the widest "high-sensitivity" temperature range, the company claims. MSA cites industry research that suggests firefighters spend 80 percent of their time in structural fires in temperatures between 150 degrees Fahrenheit and 300 degrees Fahrenheit. But traditional TICs could only function in high-sensitivity mode in temperatures below 190 degrees Fahrenheit. The MSA camera automatically switches into a low-sensitivity mode when temperatures exceed 320 degrees Fahrenheit. The camera imagery also incorporates shaded, heat-seeking color pixels, so that firefighters can determine the intensity and direction of a fire. The differences in color shading ranges from light yellow to very dark red, indicating changes in structural temperature.

**For more information go to www.info.ims.ca/4758-013**

### HiEnergy Conducts Live Blind Tests of Homemade Bomb Detector



HiEnergy Technologies

At the 7th International Defense Exhibition & Conference in Abu Dhabi, United Arab Emirates, **HiEnergy Technologies, Inc.**, of Irvine, CA, put its Siegma 3E3 bomb detector to the test at the conference's desert test site. The Siegma 3E3 is designed to detect suitcase-borne homemade bombs. It incorporates the company's Stoitech technology, which, says the company, can decipher chemical formulas of certain substances and can determine if a target is explosive. It can also identify the type of explosive, remotely and through steel or concrete. The device works without human intervention and takes between 30 seconds and three minutes to detect an explosive substance. The company claims it is 95 percent accurate.

**For more information go to www.info.ims.ca/4758-014**

### Emmanuel Cabrera Shows Model of Security and Screening Facility

Emmanuel Cabera

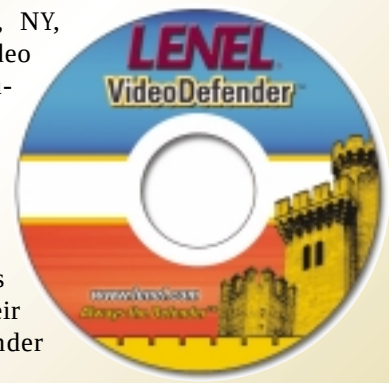
Designer and builder **Emmanuel Cabrera** has designed a new airport security and screening facility which includes a more effective screening chamber. The chamber can be installed and used without altering significantly the airports, federal buildings, hospitals or commercial buildings that will house them. Cabrera has presented his designs for the new chamber to the Department of Homeland Security and to President Bush. He also submitted a proposal for building a prototype. Cabrera noted that the design "could be produced and tested almost immediately." He maintained that "in light of the current threat level that faces us all every day it is unfortunate that we aren't making better use of the technology that is literally right at our fingertips."

**For more information e-mail charlie@charliezabarte.com**

*For submissions to this section, please e-mail detailed information to:* products@gsnmagazine.com

## IT SECURITY

### Lenel VideoDefender Offers IP-based Digital Video Management




**Lenel Systems International**, of Rochester, NY, has taken the wraps off an IP-based digital video surveillance and recording management solution, Lenel VideoDefender. The new management solution is based on an open architecture and can be custom-tailored to a company's unique needs and environment. Lenel VideoDefender is designed to work with various IP cameras, storage media and computers used as network recorders. Customers have their choice of buying only the Lenel VideoDefender software or a full turnkey system.

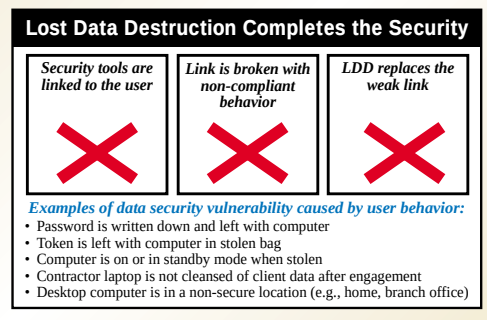
**For more information go to www.info.ims.ca/4758-016**

### BlueSecure Intrusion Protection System 3.1 for WiFi Guards Against Rogue APs and Client Devices

The BlueSecure Intrusion Protection System version 3.1 is a dedicated wireless LAN monitoring and intrusion protection solution designed to protect an organization's network from wireless-based attacks. This newest iteration of BlueSecure from **Bluesocket, Inc.**, of Burlington, MA, offers active containment of rogue devices, and advanced RF spectrum analysis. Its enhanced reporting meets the deployment requirements for wireless LANs issued by the Department of Defense. A new client-server architecture means that the system can scale to larger, multi-site deployments. The 802.11 b/a/g radio frequency sensor is priced at $695, and the BlueSecure Server starts at $2,250. Wireless Gateway and RF Sensor bundles start at $7,750.

**For more information go to www.info.ims.ca/4758-017**

### Beachhead Solutions Unveils Lost Data Destruction Software




After a number of enterprise pilots, **Beachhead Solutions Inc.**, of Santa Clara, CA, has released version 1.0 of its "Lost Data Destruction" software, which automatically destroys specified data on lost or stolen laptop and desktop computers. Not reliant on user compliance or involvement to work, this software is aimed at banks, insurance companies, medical institutions and other government and business entities that handle and store confidential data. Using preset behavior-based triggers, the software recognizes when a device has been lost or stolen, and then destroys designated files, file types, folders or encryption tags. Sensitive data is eliminated even if an unauthorized user never logs onto the Internet. "Protecting our clients and their data is a top priority for our firm and we wanted more than just passwords and encryption to protect against a security breach," said Clare Piech, chief operations officer, Mohler, Nixon & Williams, a CPA firm currently using LDD. "We also wanted a solution that would not disrupt productivity or inconvenience our partners and staff."

**For more information go to www.info.ims.ca/4758-018**

# Calendar

## APRIL 2005

| SUN | MON | TUES | WED | THURS | FRI | SAT |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

**Orlando, FL,** InfoSec World Conf. & Expo 2005, MIS Training Institute, 508-879-7999 www.misti.com/virtprog/program.asp

**Washington, DC,** FOSE 2005, FOSE, 202-772-5746, www.fose.com

**Singapore,** Black Hat Briefings & Training Asia, Black Hat, 65-6899-6115, www.blackhat.com

**Las Vegas, NV,** ISC Expo West 2005, Reed, www.iscwest.com

**San Diego, CA,** SANS 2005 West, The SANS Institute, 301-654-7267, www.sans.org, **through 4/12/05**

**Las Vegas, NV**, 15th Annual CardTech/SecurTech Conf., CTST, 800-442-2878, www.ctst.com

**San Diego, CA,** Software Security Summit, BZ Media LLC, 415-785-3419, www.S-3con.com

**Copenhagen, Denmark,** ASIS Int'l 4th European Conf., ASIS Int'l, 703-519-6200, www.asisonline.org

**Tampa, FL,** Security Solutions 2005, Telos Corp., 800-708-3567, http://securitysolutions.telos.com

**Quantico, VA,** Force Protection Equipment Demonstration V, U.S. DoD, 703-704-2416, www.fped5.org

**London, UK,** Infosecurity Europe, Reed, 44-(0)208-271-2130 www.infosec.co.uk

**Chicago, IL,** Security Solutions Seminar, Smith Detection, 973-830-2037, www.smithsdetection.com, **4/27/05 Only**

**Boston, MA,** R&D Partnering Conference, DHS Science & Tech. Directorate, www.homelandsecurityresearchconference.org, **4/27–4/28 only**

**Las Vegas, NV,** Conf. On Mobile & Wireless Security, MIS Training Institute , 508-879-7999, www.misti.com/01/mws05eb1hp.html

**Singapore,** Biometrics World Asia 2005, Terrapinn, 65-6322-2700, www.worldofcards.biz/2005/bwa_sg

Government Event | Education/Assn Event | Commercial Event

*For submissions to this section, please e-mail detailed information to:* calendar@gsnmagazine.com

## MAY 2005

| SUN | MON | TUES | WED | THURS | FRI | SAT |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | | | | |

**Las Vegas, NV,** BICSI Spring Conference, BICSI, 800-242-7405, www.bicsi.org

**Boston, MA,** RFID Tech Conference, The Conference Board, 212-339-0345, www.conference-board.org

**San Diego, CA,** GSA Expo 2005, GSA, 888-272-5565, www.expo.gsa.gov

**Las Vegas, NV,** Emerging Trends in Security, ASIS International, 703-519-6200, www.asisonline.org

**Dallas, TX,** DallasCon 2005 – Professional Cyber Defense, DallasCon Infosec Adademics, 775-278-8911, www.dallascon.com

**Arlington, VA,** Homeland Security Contracting Opportunities, Bureau of Nat'l Affairs, 800-401-5937, www.ioma.com/homelandsecurity05

**Kissimmee, FL,** NCSC Annual Conference & Expo, Nat'l Cargo Security Council, 410-571-7913, www.cargosecurity.com, **starts 5/13/05**

**San Francisco, CA,** Gartner Symposium ITXPO, Gartner, 800-778-1997, www.gartner.com

**Minneapolis, MN,** Aviation Security for Law Enforcement Officers, Am. Assn. of Airport Executives, 703-824-0500, www.airportnet.org

**Washington, DC**, Security Risk & Assessment Management, USPDI, 866-998-7734, www.uspdi.org/SecurityRiskAssessment

**Washington, DC,** Gov't Security Market, The Security Institute, 703-371-1711, www.thesecurityinstitute.org

**New York, NY,** Security & Systems Solutions Expo, Infinity Expo Group, 203-925-0004, www.infinityexpo.com

**Washington, DC,** GOVSEC, National Trade Productions, 703-683-8500, www.govsecinfo.com

### GSN ALLIANCE PARTNER EVENTS

**InfoSec World Conference & Expo 2005** • Apr 4–6, '05 • Orlando, FL • MISTI • 508-879-7999 • www.misti.com/infosecworld
**Force Protection Equipment Demonstration V** • Apr 26–29, '05 • Quantico, VA • U.S. DoD • 703-452-3760 • www.fped5.org
**ISC Expo West** • Apr 6–8, '05 • Las Vegas, NV • Reed • www.iscwest.com **FOSE 2005** • Apr 5–7, '05 • Washington, DC • FOSE • 202-772-5746 • www.fose.com **Security Risk and Assessent Management** • May 17–19, '05 • Washington, DC • USPDI/University of Maryland University College • 866-998-7734 • www.uspdi.org/SecurityRiskAssessment

# "Page 22"

*A news roundup from the 22 federal agencies and offices that were consolidated into the Department of Homeland Security...as well as other government units*

## NIST Finalizes Guidelines on Computer Security Controls for Federal Systems

The fourth and final version of recommended security controls for federal information systems has been released by the Commerce Department's National Institute of Standards and Technology (NIST). Those guidelines will become the foundation of a proposal for a Federal Information Processing Standard (FIPS) that NIST will propose later in the year. The agency is hoping that the guidelines will help federal agencies adopt a risk-based, cost-effective approach to choosing and implementing security controls. NIST entertained more than 1,200 comments on earlier drafts in developing the final guidelines. The controls encompass 17 key areas of security, including risk assessment and contingency planning.

## DHS Offers $91.3 Million in Grants to Protect Buffer Zones Surrounding Critical Infrastructure Facilities

The Department of Homeland Security has made $91.3 million in grants available to states to secure the areas surrounding critical infrastructure facilities such as dams, nuclear plants and chemical facilities. The Buffer Zone Protection Program aims funds at states and local jurisdictions so that they can acquire equipment to protect the areas outside the perimeters of these facilities. States will present buffer zone plans and equipment purchasing plans to the department's Office of Domestic Preparedness by the end of this month. ODP will then review the proposals while the Information Analysis and Infrastructure Protection (IAIP) directorate examines the technical aspects of the plans. The funds are broken down by state and vary widely. For example, Louisiana has a little more than $2.5 million in BZPP funds available to it while Wyoming has just $50,000. The biggest slice of the pie, not surprisingly, goes to California at nearly $13 million with New York a distant second at nearly $5.8 million.

## GAO Study Finds Agriculture Still At Risk

According to a recent report from the Government Accountability Office (GAO), the Departments of Agriculture and Homeland Security took significant steps to protect the nation's agricultural initiatives and food supply, but still face challenges when it comes to being prepared to respond to a potential attack against livestock. The study notes that the USDA would not be able meet a presidential directive to deploy animal vaccines within 24 hours of an outbreak. The nation currently only stores vaccines for foot and mouth disease, which must be sent to the U.K. for activation. Management problems, too, could hamper efforts to respond quickly and appropriately. The number of agricultural inspections has dropped since inspectors were transferred from the USDA to the DHS in 2003.

## New Legislation Aims $11 Billion in Grants at Anti-Terrorism Programs

Legislation in Congress recommends that $11 billion be spent on technology-focused initiatives meant to prevent terrorist attacks and shore up security vulnerabilities, according to **Input**, the Reston, VA-based research firm. For instance, the "Rail and Public Transportation Security Act of 2005," or House Bill 153, focuses about $7.5 billion over the next five years on the nation's rail and public transportation systems. The bulk of the money will go toward ensuring that communications and infrastructure aren't seized by terrorists and toward responding to a wide variety of attacks. Among its recommendations, the bill includes a requirement for interoperable communications systems.

## Homeland Security Chairman Cox Questions Suitability of Separate ICE and CBP

Rep. Christopher Cox (R-CA), chairman of the House Homeland Security Committee, recently told the subcommittee on management, integration and oversight that "anecdotal evidence suggests that the division of customs and immigration inspectors from their related investigative colleagues may be building administrative walls and hampering cooperation and information sharing between ICE and CBP in critical mission areas." Cox noted that "some observers also have suggested that the distinction between the 'interior enforcement' activities of ICE and the 'border security' functions of CBP are artificial constructs that contribute to needless administrative overlaps, programmatic turf battles, mission gaps, and sometime dangerous operational conflicts."

Cox also said it appeared that some of "ICE's very troubling budget shortfalls" in the last two years may have occurred because of "erroneous budget allocations that occurred upon the division of CBP and ICE into two discrete components of the Border and Transportation Security Directorate."

## TSA Broadens Items Prohibited Beyond Airport Checkpoints to Include Lighters

The Transportation Security Administration has banned all lighters – butane, absorbed-fuel, electric/battery-powered, novelty and the like – from the sterile areas of airports and onboard airplanes. The action is a result of a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, which was signed into law by President Bush last December. The TSA will begin enforcing the policy on April 14.

## Five Federal Agencies Brief Homeland Security Committee on Nuclear, Bio Attack Prevention

Officials from the departments of Homeland Security, Defense, Energy, Justice and State went before the House Homeland Security Committee's subcommittee on prevention of nuclear and biological attack in March to fill in members on efforts among federal agencies to help prevent both nuclear and biological attacks. "Each department contributes to this mission," said John Linder (R-GA), chairman of the subcommittee. "Today's news that a suspected terrorist charged in New York sought to sell uranium for the purposes of attacking New York's subway system underscores the urgency of our work. We must do everything in our power to ensure that the U.S. government succeeds in this mission."

## Cox Voices Support of Supplemental Appropriations

Rep. Christopher Cox (R-CA), chairman of the House Homeland Security Committee, noted recently that the Fiscal Year 2005 Emergency Supplemental Appropriations Act aimed money at several critical areas. Noting that the spending bill would be incorporated (procedurally) with the REAL ID Act approved by the House on Feb. 10, Cox said, "We cannot effectively fight terrorism if we cannot verify the identity of people boarding airplanes, entering nuclear power plants, visiting the White House or gaining access to any of the countless places a terrorist could use as a stage to multiply the effect of an attack. Accurate identification of individuals before permitting them access to critical infrastructure is a prerequisite to success." Cox explained that the spending bill also aimed money at keeping the nation's borders safe. "To secure our nation from nuclear attack, legislation includes $55 million to detect nuclear material at foreign ports," said Cox. "The Megaports Initiative is designed to interdict illicit traffic in nuclear and other radioactive materials." The country's ports will be able to monitor and check a higher volume of shipping containers. The bill also allots $38.97 million for the Terrorist Screening Center.

*For submissions to this section, please e-mail detailed information to:* **page22@gsnmagazine.com**

From: David Berteau


# Is the White House's Homeland Security Council Falling Short?

What is the Homeland Security Council? Is it doing its job? How can we tell, and why have we heard so little of them? Let's take a look.

The Homeland Security Council, or HSC, was set up right after the September 11 terrorist attacks, in parallel with the naming of Tom Ridge as Special Assistant to the President for Homeland Security. Patterned after the National Security Council, the HSC is chartered to coordinate homeland security across the federal government and to bring decisions to the president in a timely manner. In a sense, it's a traffic cop responsible for not only keeping the cars flowing, but also for making sure they get where they need to go on time.

After DHS was created two years ago, the HSC and its staff remained in the White House – but their role is now shared. The HSC staff of 50 supports the Council itself, composed of cabinet officers like the Secretaries of DHS, HHS, Transportation, Treasury, and Defense and subcabinet members like the CIA and the FBI. They also support Policy Coordinating Committees, known as PCCs, who wrestle with the coordination and decision issues.

Early on, the HSC stepped in to resolve inter-agency problems such as the one that occurred with the National Response Plan (NRP). The NRP is a key building block for response to attack or disaster. Two years ago, when the initial NRP from DHS failed to meet the mark, the HSC staff got it back on track – although that took nearly an extra year to resolve.

Later, though, the HSC's role became more sidetracked. Disputes between DHS and other federal agencies, like the fight with the FBI over control of the terrorist threat center, should have been refereed by the HSC, but it apparently stood by silently and did little. Ultimately, Congress stepped in and resolved this problem in the intelligence reform legislation passed last fall.

The HSC is headed by Fran Townsend, the latest in a succession of homeland security advisors who have held the position since Ridge moved to DHS two years ago. Even among Washington insiders, people have difficulty identifying the last time they read Townsend's name associated with any major policy issue.

This is not necessarily a bad thing – anonymity can be an essential part of success in bureaucratic infighting. But in the case of the HSC, that success is either missing or has remained invisible. It raises the question of whether the HSC is even moving issues toward a timely decision.

Twice last year, hundreds of state and local first responders gathered in Washington, DC, to provide their input to the latest evolution of homeland security planning. Their meetings quickly reached near-mutiny, as DHS's plans were roundly rejected by all sides. Both the plans themselves and the process for their review were panned. What were these controversial plans and how did matters reach that state?

Essentially, the first responders felt the White House was moving too fast on the draft "Target Capabilities List" released by DHS. This list covers 36 areas that local communities are expected to be proficient in and is tied to another list, the "Universal Task List," which lays out tasks the federal government will undertake. Both of these lists flow from 15 frightening threat scenarios, recently revealed in the New York Times after they were inadvertently posted on a state disaster planning Web site.

There are 87,000 local jurisdictions with first responder duties, and the effort to link all these entities into a national integrated plan with assigned tasks is enormous. The comments expressed worries that DHS and the HSC were moving too fast, perhaps trying to meet artificial deadlines rather than to get the plans right.

DHS is trying to develop these documents in response to direction from Congress and the president as part of the new National Preparedness Goal. Under Homeland Security Presidential Directive number 8 (HSPD-8), the president called for this goal to be written and approved as part of the budget currently under review by Congress. A well-defined set of goals will help DHS and Congress prioritize the use of funds for homeland security. Until now, the fight over homeland security funds has often been a pork barrel exercise in which DHS has not set out clear priorities.

It's a simple concept – make sure the nation is ready for the next major disaster, whether a terrorist attack or a natural calamity. The directive refers to these disasters as "all-hazards preparedness" because being ready to respond is largely independent of the nature of the event itself.

Preparedness means that we have plans, procedures, policies, training, and equipment in place to prevent, respond to, and recover from major events. There is a legitimate question as to whether we need to prepare for terrorist attacks in the same way we prepare for natural disasters, but there is no question that we need to be better prepared across the board. The nation should expect no less from its government.

Ever since September 11, there has been widespread agreement that previous plans and procedures were weak and inadequate in the face of new terrorist threats. We all know the nation remains on high alert and threats are periodically reported in the news media and by government officials. The millions of first responders across the country need to know what work is expected of them and what they can expect from the federal government.

Billions of dollars are being spent under the guise of improving readiness, and beginning next year, DHS will make funds contingent on local communities being in compliance with key parts of the National Preparedness Goal. Yet the goal has not yet even been defined!

Former Virginia Governor Jim Gilmore told *GSN* some months back that the Homeland Security Council is not such a bad institution but that the president's main advisor on homeland security should be the DHS secretary. This is the same arrangement that has been in place for decades under the National Security Council, where the secretaries of Defense and State are the president's principal advisors for national security and foreign policy. The NSC and the National Security Advisor play a critical role in defining issues and pushing them forward to resolution.

The question is, can the HSC be like the NSC? Can it be the coordinator of issues that leads to real decisions? Reports from the White House indicate concern that the HSC is not fulfilling its purpose. Consideration was given to folding the HSC under the NSC. As Michael Chertoff moved to replace Tom Ridge as DHS secretary, it would have been an excellent opportunity to make that change.

Yet nothing was done. Perhaps the White House felt that folding the HSC into the NSC would signal a lessening of the commitment to homeland security. Would it? Not in my view, because the real issue is not whether preparing for terrorist attacks is different than preparing to respond to natural disasters. The real issue is that we cannot put an artificial boundary around terrorism and separate domestic threats from national security and foreign policy. Yet under the current organization we do just that.

Others are also looking at this question. The Center for Strategic and International Studies, as part of the second phase of its ongoing study called "Beyond Goldwater Nichols," is expected to suggest some ideas to improve the interagency process that covers homeland security and national defense. It will issue its report and recommendations later this April.

The real test of an organization is not how it is set up. The real test is how it performs, and the HSC either needs to step up and meet its responsibilities, or changes need to be made. The hundreds of first responders who made their objections clear last year deserve no less. ■

David Berteau is a defense and homeland security consultant for Clark & Weinstock in Washington, DC, and an adjunct professor for the Maxwell School of Syracuse University. His 30 years of government and business management experience include 12 years as a senior Pentagon official, serving four secretaries of defense. He can be reached at dberteau@cwdc.com

Guest Columnist

ROHIT MEHRA

# Why WiFi? Five steps to robust wireless communications

What is causing the growth of WiFi networks in the public sector? And what is limiting that growth?

The first question is easy to answer. Who wouldn't want to have the freedom of moving between work places without wires? Or carrying a laptop or handheld device between floors of a building so you could gain access to information stored on local servers or hop onto the Internet? The benefits of WiFi are well understood.

But, when it comes to the inhibitors to wireless growth in the public sector, one of the key issues is the lack of knowledge about WiFi protocols and encryption standards. That's understandable. These 802.11 standards are forever changing. As Isaac Asimov once said, "If knowledge can create problems, it is not through ignorance that we can solve them." A combination of changing standards, new regulations, security concerns and lack of training conspire to limit WiFi adoption.

Some say the government employs too few top-quality wireless LAN engineers, with many unable to discern the difference between an edge, core or mesh topology. The good news is that five-day certification classes are available to WLAN engineers. The not-so-good news is that today every network has to be certified as secured.

Last April, the Department of Defense issued a policy requiring wireless data encryption to be implemented end-to-end over an assured channel and validated against Federal Information Processing Standards (FIPS). Cellular, PC, radio frequency and infrared wireless devices are allowed in areas where classified information is discussed, stored or transmitted only with special approval.

However, new wireless encryption protocols have given network managers a false sense of security because as mobility increases across the enterprise, security threats increase as well. Fortunately multi-layered, "client-less" solutions have emerged, which promise to tackle new threats without sacrificing mobility.

With the arrival of new wireless encryption protocols, such as WPA and 802.11i, government agencies are worrying more about security these days and less about other issues, such as capacity, quality of service, coverage, and radio interference. Yet encryption is only one piece of the wireless-security puzzle.

Rohit Mehra is director of product management at Bluesocket Inc., of Burlington, MA, a developer of wireless LAN management and security products. He can be reached at: rmehra@bluesocket.com.

The Dell'Oro Group, of Redwood City, CA, predicts that wireless LAN infrastructure shipments will almost triple in size by 2007. This growth is being spurred by a mindset that prioritizes access over protection.

Another indication of WiFi growth within government – especially the DoD – is that vendors are rushing to add WiFi products to the GSA Federal Supply Schedule and to achieve FIPS 140-2 Level 2 certification from the Commerce Department's National Institute of Standards and Technology (NIST). The standard defines security requirements for cryptographic tools used to protect information within IT systems.

## FIVE STEPS TOWARDS SECURE MOBILITY

In a wireless network, security issues are magnified because the air itself becomes part of the network, and "untrusted" airwaves penetrate right through the walls, exposing computer networks to all sorts of new risks. Multi-layered, "client-less" protection is needed because of the diverse nature of mobile users and the fact that mobile devices access today's agency networks and applications.

If encryption is but one piece of the wireless-security puzzle, what does the rest of the puzzle look like? Security is a process, and there are five basic steps that can be followed to ensure robust mobile security.

## STEPS 1 & 2: AUTHENTICATION AND ENCRYPTION

The first two steps towards secure mobility – authentication and encryption – are combined because most government WLANs have already addressed them. Users must log into networks and be authenticated in order to gain access. Once on the network, their traffic over the air is encrypted to protect it from the eyes of would-be eavesdroppers. Now that the nightmare days of WEP are behind us, there are several good encryption and authentication standards to use, including WPA, 802.11i (WPA2), AES, and EAP.

Unfortunately, authentication and encryption are where most agencies stop. Outsiders can still enter the network through physical-layer attacks. Users often employ weak passwords, and many WLANs are deployed with encryption turned off.

Network administrators also have little or no control over what devices enter their WLANs. The increasing diversity of client devices throws a kink into the enforcement and authentication game. Unlike in the wired world, today's wireless networks must support a heterogeneous, mixed-device world where appropriate encryption and authentication schemes may vary from device to device – meaning that a one-size-fits-all policy will not suffice. Government WLANs need a fine-grained approach to their user policies.

## STEP 3: POLICY ENFORCEMENT

Before policies can be enforced, they must be established. Such policies should take into account the access rights to the network determined by the individual's role within the agency. With proper policies in place, certain users can receive higher quality of service (QoS) and bandwidth priority over other users, such as temporary workers or visitors. More sophisticated policy schemes can enable location- or VLAN-based policies. Considering that most agencies have spent a lot of time building LDAP and Active Directory databases, a WLAN policy engine could facilitate the application of these existing policies on the wireless network.

Once policies are in place, it becomes a matter of enforcement, which is where many WLAN solutions fall short. Consider a user who takes a laptop out of the building, visits a public network in a coffee shop, forgets to update virus signatures, and returns to the agency with a worm.

A WLAN policy engine could do two things to head off a problem: (1) it could enforce a rule that says any device entering the network must undergo a vulnerability assessment before being granted entry, and (2) it could monitor a user's TCP connections. For example, suppose a policy dictates that each user is allowed only 15 TCP connections. If a malicious worm tries to set up hundreds of TCP connections, the WLAN security system would notice and act to protect itself. The user could be put into quarantine and the worm could be curtailed before it had a chance to impact performance or bring down the entire network.

## STEP 4: PROTECTING AGAINST WORMS & VIRUSES AT THE NETWORK LEVEL

Since users come into the enterprise through multiple points of entry and with various roles – including visitors and part-time workers – desktop-based protection is not sufficient. It is hard to apply policies to guests, outsiders and mobile users.

Traditional virus and worm protection relies on clients. What happens when a PDA with an infected file is attached to the network? Not all PDAs possess virus monitoring solutions, nor do mobile phones, scanners and cameras, yet all are accessing government networks. With so many different clients entering the network, what is needed is client-less, or network-based, protection.

Essentially, network-based virus and worm protection are extensions of policy enforcement. Once a policy is developed, it must be enforced. This requires monitoring based on user behavior to identify roles and to allocate bandwidth dynamically, based on those roles. Once user-behavior monitoring is in place, it can be broadened so that traffic anomalies trigger a security response. Thus, back-door worms can be headed off before they can propagate.

Another way to protect the network is to validate those devices that are coming into the network. Such a monitoring solution should look at the device itself, check to see what ports are enabled and perform a quick scan for the most prevalent worms and viruses. Devices should be permitted into the network only after an automatic vulnerability assessment is run and it has been determined that the machines are conforming to security policies.

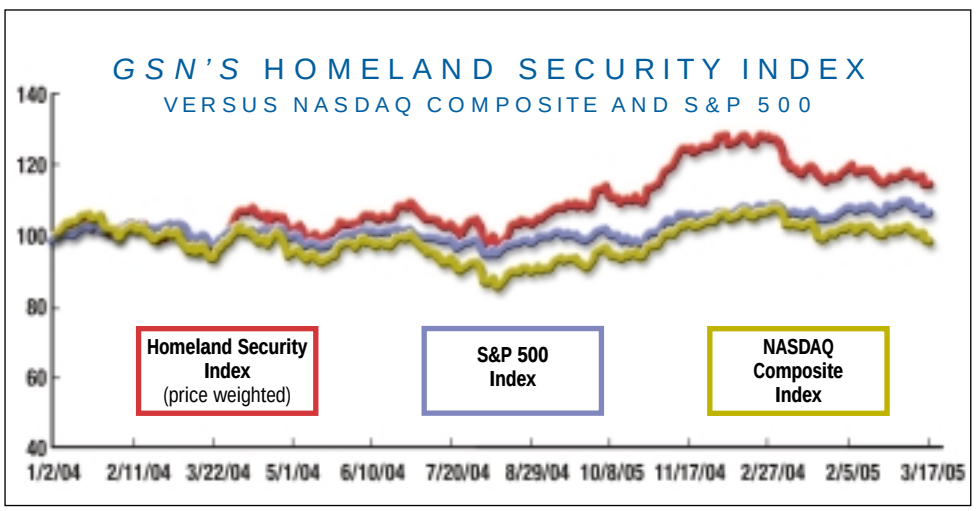
## STEP 5: MONITORING THE AIR ITSELF

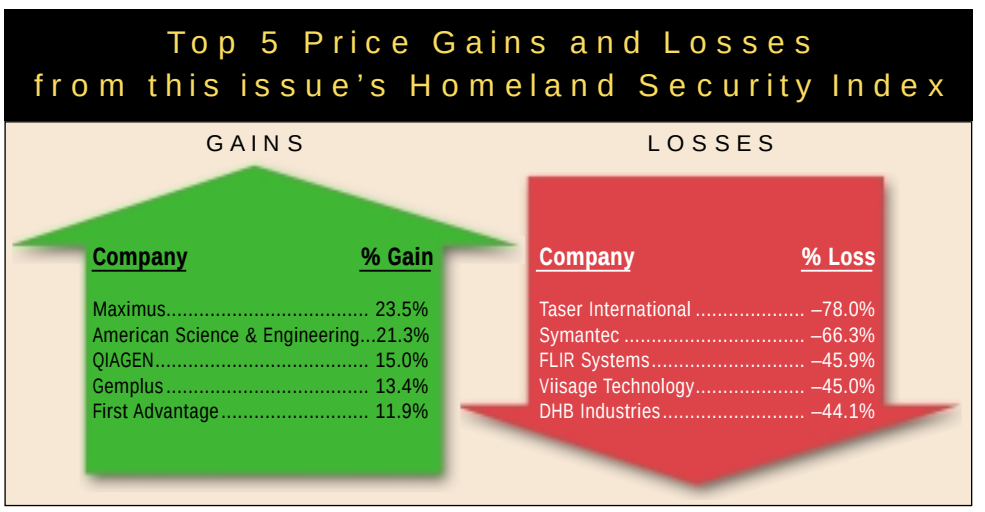
In a wired network, a degree of security is provided by the fact that traffic must traverse wires. In the wireless world, this is not the case. Network administrators are faced with the daunting task of defending the air itself.

In a traditional access point-only network this is nearly impossible to do. Even with new switch-based architectures that use the same APs as air monitors, such monitoring can lead to a degradation of performance. There is a third way, however, by deploying an overlay RF monitoring network, administrators can gain a real-time, 24/7 view of the airwaves.

Rogue access points (and rogue clients as well) represent some of the new threats that WLANs must deal with, threats that wired networks needn't worry about. Off-the-shelf access points are becoming so inexpensive that any tech-savvy employee or motivated outsider can tap into an unsecure WLAN. Even well-meaning employees who simply want access in an area not currently covered could open a huge hole into the network. ■

# Wall St. Close-up


THE HOMELAND SECURITY INDEX MEASURES FIFTY STOCKS FROM FIVE CATEGORIES:

**(1) Homeland Security Plays:** ActivCard (ACTI), American Science & Engineering (ASEI), Armor Holdings (AH), Cogent Systems (COGT), CompuDyne (CDCY), Digimarc (DMRCE), LaserCard (LCRD), First Advantage (FADV), FLIR Systems (FLIR), Identix (IDNX), Mine Safety Appliances (MSA), OSI Systems (OSIS), TASER International (TASR), Verint Systems (VRNT), and Viisage Technology (VISG)

**(2) IT Systems Integration / Gov't Consulting:** Affiliated Computer Services (ACS), Anteon International (ANT), CACI International (CAI), Computer Associates (CA), Computer Sciences (CSC), Electronic Data Systems (EDS), ManTech International (MANT), Maximus (MMS), McAfee (MFE), Net IQ (NTIQ), and Unisys (UIS)

**(3) Defense Contractors:** Boeing (BA), Cubic (CUB), DHB Industries (DHB), DRS Technologies (DRS), General Dynamics (GD), General Electric (GE), Honeywell (HON), L-3 Communications (LLL), Lockheed Martin (LMT), Northrop Grumman (NOC), and Raytheon (RNT)

**(4) Data Integrity / Network Security:** Check Point Software (CHKP), ChoicePoint (CPS), Gemplus (GEMP), Internet Security Systems (ISSX), RSA Security (RSAS), Secure Computing (SCUR), Symantec (SYMC), Titan (TTN), Verisign (VRSN), and Watchguard (WGRD)

**(5) BioTerrorism / Pharmaceuticals:** Applied Biosystems (ABI), Cepheid (CPHD), and QIAGEN (QGENF)

The "Homeland Security Index" historical pricing chart and the price gains and losses chart were provided by Morgan Keegan & Company. www.morgankeegan.com

# Marketing Moves

## BMC Selects IPLocks Information Risk Management Solution

**BMC Software, Inc.**, of Houston, TX, has chosen the IPLocks Information Risk Management Platform from **IPLocks, Inc.**, of San Jose, CA, to ensure the privacy of, as well as protect, its financial data. The platform adds continuous database monitoring, assessment and forensic audit analysis as safeguards for information and to help it meet regulatory requirements. The company plans to use IPLocks to uncover and assess vulnerabilities in its databases.

## OSI Systems Consolidates Security Brands into Rapiscan Systems

**OSI Systems, Inc.**, of Hawthorne, CA, has combined all of its OSI Security brands – Rapiscan, Metorex, Ancore and ARACOR – to form Rapiscan Systems. The new company will offer a wide variety of security products to a diverse customer base. Company president Ajay Mehra noted that the groups for years "have operated, while in cohesion, as separate brands." The consolidation should help the company build its brand in the industry.

## A4Vision, In-Q-Tel Join Forces in Strategic Development Deal

**A4Vision, Inc.**, of Sunnyvale, Calif., and **In-Q-Tel**, a private venture group funded by the CIA, have inked a deal whereby A4Vision's core 3-D facial biometric imaging and identification technology will be used in new applications for both the government and commercial markets.

## Markland Buys Technest Holdings, Genex

**Markland Technologies, Inc.**, of Ridgefield, CT, has purchased majority ownership of Technest Holdings Inc. as part of a multipart transaction. Technest Holdings did not have operations before the acquisition took place but it was traded on the OTC bulletin board. The deal was followed by the purchase by Technest of **Genex Technologies, Inc.**, of Maryland, for $3 million in cash and $7 million in Markland Technologies stock.

## Freeman Nabs ASC Outstanding Achievement Award

Jonathan Freeman won an Outstanding Achievement Award from the American Society of Cinematographers (ASC) for his original movie for broadcast television, "Homeland Security," which appeared on NBC.

## Global Secure Completes $20 Million Purchase of Virtual Alert

**Global Secure Corp.**, of Washington, DC, has purchased **Virtual Alert, Inc.**, of Sacramento, CA, for $20 million in cash and stock. Virtual Alert president Eric Shaffer notes that the acquisition is a good one, citing Global Secure's "focus on state and local government market, its nationwide distribution channels, its training capabilities, and its operational infrastructure."

## Astrata Group Wraps Acquisition of SureTrack

**Astrata Group Inc.**, of Los Angeles, CA, has finalized its purchase of SureTrack. Solaris, previously known as SureTrack's Global Telemetry Monitoring System, blends satellite communications capability with Astrata's Geo-Location Platform, which is referred to as Sirius outside of the U.S. As a result, the company now offers a complete remote fleet management and vehicle monitoring solution that includes real-time tracking and monitoring capabilities. Solaris can interface with a number of on-board devices.

*For submissions to this section, please e-mail detailed information to:*
marketingmoves@gsnmagazine.com

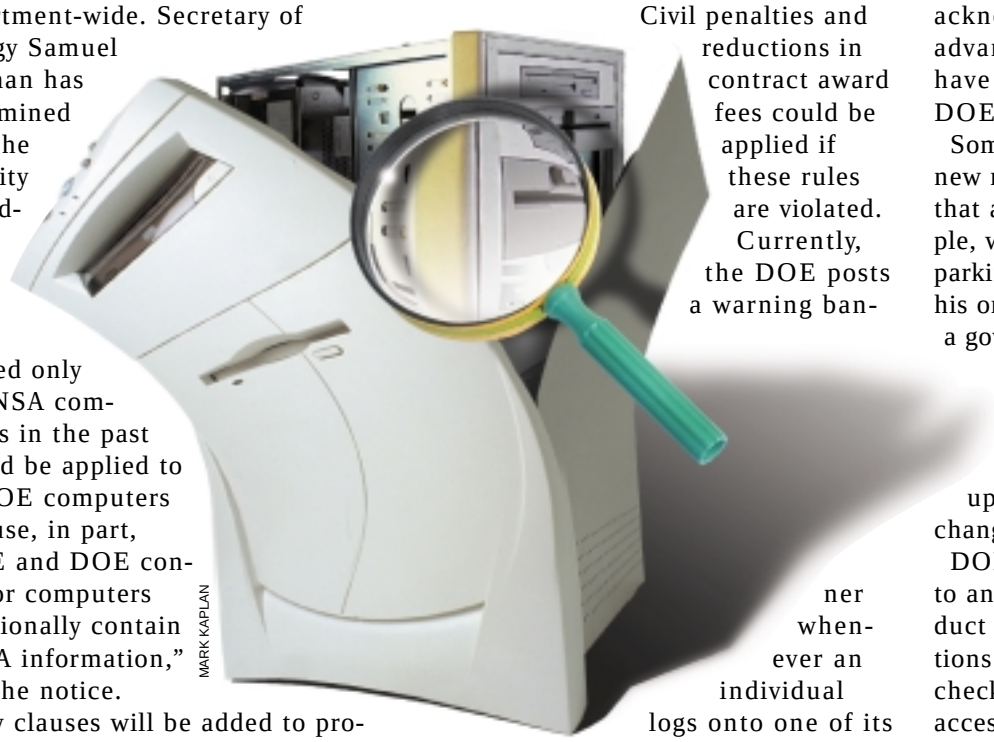
From Page 1

# Employees must sign consent forms in advance

apply not only to employees and contractors of the department's National Nuclear Safety Administration (NNSA), which oversees security at national laboratories and nuclear weapons production facilities, but to all DOE employees and to any employee of a DOE contractor or subcontractor who uses a desktop, laptop, or computer network "owned by, leased by or operated on behalf of the DOE."

The rules would be embodied in a new part added to the code of federal regulations that implement the National Defense Authorization Act for Fiscal Year 2000. The Federal Register notice posted March 17 by DOE cites a section of the new rule that might have an impact on personal privacy. "This section makes clear that no user of a DOE computer, including any person who sends an e-mail message to a DOE computer, would have any expectation of privacy in the use of that DOE computer," said the DOE.

The new rules would be added to a long laundry list of security regulations that have been piling up at DOE since the mid-1990s. But these will be the first to require written consent in advance that will apply department-wide. Secretary of Energy Samuel Bodman has determined that the security considerations that had applied only to NNSA computers in the past should be applied to all DOE computers because, in part, "DOE and DOE contractor computers occasionally contain NNSA information," said the notice.



MARK KAPLAN

New clauses will be added to procurement contracts awarded by DOE requiring contractors to comply with these new security rules. "Every DOE and contractor employee subject to the rule would be required to sign a written acknowledgement and consent form…," the notice explains.

Civil penalties and reductions in contract award fees could be applied if these rules are violated. Currently, the DOE posts a warning banner whenever an individual logs onto one of its computer systems, informing users that their communications are subject to interception, monitoring, recording and disclosure. The new rules would carry that process one step further by insisting that all potential users acknowledge this practice in advance and agree in writing to have their computers inspected, if DOE deems it necessary.

Some observers may consider this new rule similar to the understanding that a motorist might have, for example, when entering a U.S. Government parking garage; the expectation that his or her vehicle might be subject to a government inspection. Others may feel that the new requirement that all DOE employees and many contractor employees must sign a written consent form upfront represents a substantial change in DOE policy.

DOE investigators might want access to an individual's computer to conduct counterintelligence investigations or to perform background checks on individuals proposed for access to classified information, said the notice.

DOE officials will receive comments on the proposed new rules until May 16. ■

From Page 1

# Should the federal gov't finance ISAC operations?

to provide adequate and consistent support for them.

Proponents of the ISACs say that their mission, to provide 24/7 threat warning, incident reporting, and analysis and protection of private industries' sensitive and proprietary information, is vital because it is something that the government itself cannot accomplish.

Recently, however, 9/11 Commission member and former Deputy Attorney General Jamie Gorelick charged at a security conference in San Francisco that the industry-led ISACs are ineffective, saying that the concept should be abandoned or reformed if national security is to be safeguarded.

At the same forum, former White House security adviser Richard Clarke referred to the ISACs as "version 1.0," saying that four years after al-Qaeda's deadliest attack, the centers were "still getting started."

"I don't think the model of ISACs works," Gorelick said. "Asking industries to fund their own ISACs as they wish and in a disorganized fashion will not get us where we need to go."

Gorelick added that the centers ended up having to "pass the hat" to raise operating funds. "You need personnel who have their job from year to year, and don't need to beg for their salary from constituent members."

Several ISAC spokespeople consulted by *GSN* vigorously disputed Gorelick's characterization, saying that her views were outdated and misinformed. "I don't believe she's been active in this community for some time," said Guy Copeland, president of the Information Technology ISAC, "and therefore is really not up to speed on the accomplishments we have achieved."

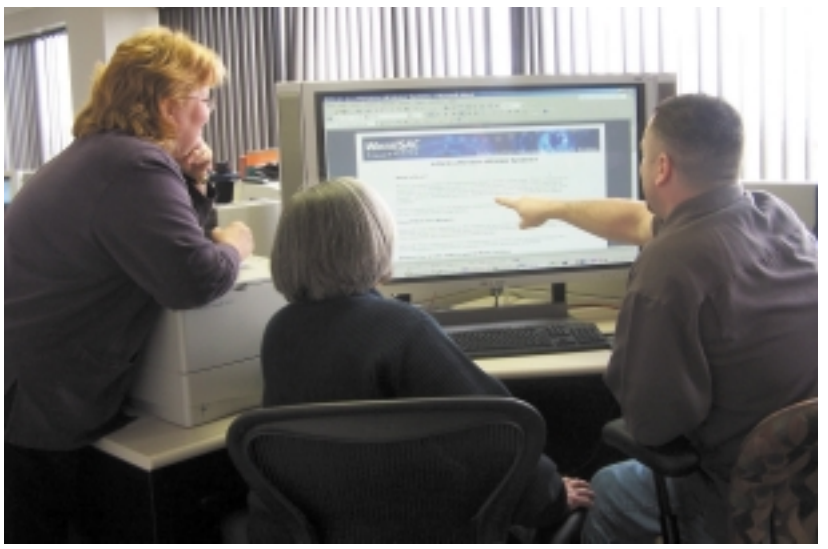
"The ISACs have developed differently, they have different missions and different maturation cycles," noted Don Rondeau, director of the Highway ISAC. "As people start to look at and understand the goals and capabilities of each individual ISAC, they will understand that no one statement can speak to all of the ISACs."

Creation of the ISACs grew out of Presidential Decision Directive 63, issued by President Bill Clinton in 1998, which named them as a means of fostering critical infrastructure sector cooperation, including information-sharing, with the federal government.

After the terrorist attacks of September 11, 2001, the ISACs shifted their principal focus from cyber security to broad concerns over the threats posed by terrorists to the physical infrastructure of the more than 80 percent of the U.S. economy that is privately owned.

Today there are more than a dozen ISACs for sectors ranging from IT, telecommunications and financial services to food, water, chemical, energy and surface transportation. Although they vary in terms of funding, organization, and relations to the federal government, all of the centers seek to directly and rapidly bring together expert members to examine vulnerabilities, threats or incidents as these rise to levels that require sector expertise and coordination.

The centers' often cutting-edge contributions to critical infrastructure protection, ISAC proponents say, include their reach into the maw of the sectors they represent. Thus, they able to help both industry and the government detect and analyze real-time and potential security threats, as well as create and sustain the trusted relationships needed for cross-sector information sharing.



The deep and broad bench many ISACs bring to analyzing threat information cannot be matched anywhere in the federal government, ISAC defenders say. Nor can the government, hobbled by various pre-9/11 laws and regulations mandating the public disclosure of information, guarantee the protection of sensitive and proprietary data.

The Highway ISAC, which operates under a cooperative agreement with the Transportation Security Administration and the Office of Domestic Preparedness, is an example of the extensive network within a sector – transportation -- that serves as the robust foundation for receiving, analyzing and disseminating threat information, Rondeau noted. "We see these emerging threats as they happen."

Located within the Transportation Security Operations Center in Herndon, VA, the "connectivity" between the Highway ISAC and its industry peers, Rondeau added, has been a boon for its non-sector partners as well. "We get a lot of information that may have to do with the surveillance of an infrastructure that may have nothing to do with highways," Rondeau said, "but it is a member of the highway community that is reporting a potential surveillance on chemical, a potential surveillance on water, things of that nature."

The Energy ISAC proved invaluable for determining the causes and the reach of the August 14, 2003 mega-blackout, recalled Louis Leffler, a spokesman for the ISAC. "We literally had almost 200 people working on a detailed analysis to figure out exactly what had happened. You may not always need that many people, but you do need to reach out to industry to find the people who know what is going on to understand it," he said.

These positive achievements, however, must be weighed against other recent developments that appear to have provided Gorelick's comments with resonance.

Despite the ISACs' contributions to critical infrastructure protection, their operators and proponents appear to be dogged by funding realities. While the Financial Services ISAC reported a 1,300 percent growth during the last year, money remains an issue for many ISACs. Gorelick's comments, for instance, came just weeks after the nation's Public Transportation ISAC announced it was in danger of folding after federal support dried up.

"Jamie (Gorelick) said that they are not funded properly – and they are not funded properly," said Suzanne Gorman, president of the ISAC Council, a coalition of all the ISACs. "Part of the problem is that the sectors' sponsoring agencies for each of these ISACs have to become engaged again. I do not think that a lot of them are."

Gorman's remarks echoed a report issued last August by the White House's National Infrastructure Advisory Council, which recommended – to date without much success – that DHS "recognize and endorse" the ISACs.

Instead, as recently as late last year, DHS officials were offering industry groups PowerPoint presentations that emphasized perceived limitations of the ISACs, including service fees which many believe stymie the recruiting of new members, and interoperability and cost issues that inhibit cross-sector information-sharing.

One slide claimed that the ISACs were "not effectively resourced for information collection, analysis and dissemination of sector-specific incident and vulnerability trends."

ISAC defenders counter by saying that the DHS criticisms risk becoming a self-fulfilling prophecy. The ISACs' attempts to develop self-funding models and grow their private-sector memberships are hindered by the government's inability or unwillingness to voice its support of the centers and develop clear information-sharing protocols that recognize their value.

DHS's failure to use its "bully pulpit" on behalf of the ISACs comes amid continued confusion and turmoil over the centers' relationships with the federal government. Some ISACs have been able to maintain strong ties with their sector partner -- the Financial Service ISAC's longstanding liaison with the Treasury Department is an example of a rock-solid relationship. Others, such as the Water ISAC, labor with increasing frustration to get any useful information from DHS, despite having received a $2 million shot-in-the-arm in the fiscal 2005 omnibus appropriations bill (PL 108-447).

The ISACs have also struggled to retain their roles among a jumble of private sector information-sharing programs within the federal government and private organizations whose mission is also to promote the sharing of security-related information.

What's more, when DHS created "sector coordinating councils," designed to drive sectors' overall infrastructure strategies and policies, it cut the operational ISACs out of the loop regarding its plans to create the parallel policy organizations until the decision already was made, according to several ISAC sources.

"The growing pains of organization and reorganization within DHS definitely inhibits some of the information sharing on the private side," noted Rod Nydam, associate director of private sector programs at the George Mason University's Critical Infrastructure Projection Project. The university's critical infrastructure program forms part of a contract with DHS under which George Mason offers support services to both the ISAC Council and the sector-coordinating councils.

"In general, the ISACs play a very important information-sharing and related operational role, one that cannot be played by the government in every sector," Nydam added.

"The ISACs bring analytical expertise than cannot be replicated anywhere else," said Paul Wolfe, vice president of **EWA Information and Infrastructure Technologies, Inc.**, a Herndon, VA, firm that manages three ISACS. "They are a wonderful gift that was presented to the nation.

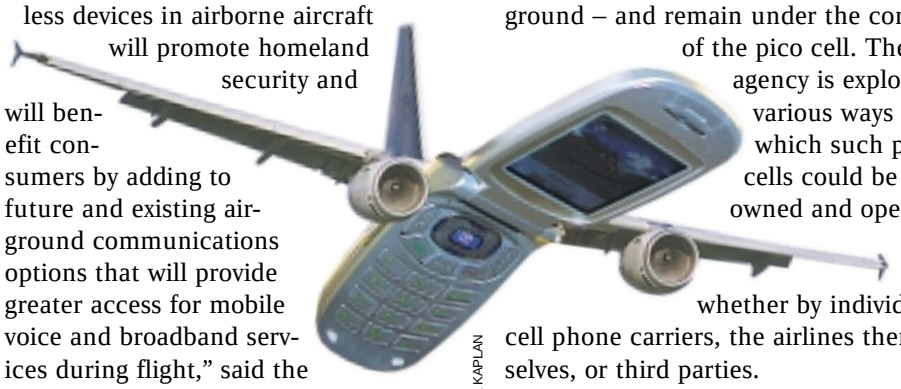
"They just need to be used." ■

From Page 1

# FAA still concerned about cell phone interference with avionics

prevents the use of such phones carried onboard by passengers or crew members or installed permanently on both private and commercial aircraft. The ban was designed to prevent cell phone transmissions from interfering with "terrestrial" cellular networks located on the ground.

"We believe that allowing controlled use of cellular handsets and other wireless devices in airborne aircraft will promote homeland security and will benefit consumers by adding to future and existing air-ground communications options that will provide greater access for mobile voice and broadband services during flight," said the FCC in a notice published in the *Federal Register* March 10.



MARK KAPLAN

The FCC envisions the possible use of what are called "pico cells," essentially low-powered cellular base stations installed on the aircraft which can receive transmissions from cell phone users onboard the plane and forward those transmissions via a separate frequency to the ground. "The cellular signal travels from the cellular handset to the pico cell, which then relays the call to the ground via a separate air-to-ground link, e.g., via a satellite band or a 800 MHz Air-Ground band," the FCC explained.

The FCC might allow cell phone owners aboard the aircraft to use their phones providing they operated at the lowest power level – which would not interfere with terrestrial networks on the ground – and remain under the control of the pico cell. The agency is exploring various ways in which such pico cells could be owned and operated; whether by individual cell phone carriers, the airlines themselves, or third parties.

Regardless of any relaxations by the FCC on its cell phone ban, however, the FAA still maintains its own prohibition on cell phones and portable electronic devices (PEDs) while airborne, and those rules are enforced by the airlines.

"Even if the FCC were to remove that ban, which they're considering doing, the FAA is concerned with safety issues and the potential for cell phones to interfere with avionics onboard the aircraft," Alison Duquette, a spokeswoman for the FAA told *GSN*. "We do have an advisory group that's working on the issue long term, but it would have to be proven to us that there is absolutely no potential for interference, so I don't foresee us lifting the ban anytime in the near future."

The two agencies may find themselves at loggerheads, but the FCC currently seems to be following a diplomatic route.

"While our objective is to relax or remove the [Federal Communications] Commission's prohibition on airborne use of cellular telephones, any steps we ultimately take will leave the use of personal electronic devices (including cellular and other wireless handsets) aboard aircraft subject to the rules and policies of the FAA and aircraft operators," said the FCC.

Some cell phone companies, such as **QUALCOMM, Inc.**, of San Diego, CA, have been working on airborne communications systems designed not interfere with either terrestrial cellular networks or an aircraft's navigation and communications gear. About 80 percent of airline passengers currently carry cell phones, according to Qualcomm's Paul Guckian, and many of those passengers would like to be able to talk over their cell phones, but Qualcomm is focusing even more of its energy on the transmission of data so passengers could send and receive e-mail messages while airborne. "Voice doesn't have to be an application offered in the aircraft," Guckian added.

The FCC's possible lifting its prohibition against cell phone use on airplanes not only sets up a tug-o-war between the FCC and the FAA, but also creates an unusual dilemma for the nation's largest cell phone carriers. These companies must determine whether the "upside" of allowing airline passengers to use cell phones, and the extra revenue such increased usage would generate, is worth the possible "downside" from causing so much interference with their terrestrial cellular networks that they antagonized their Earth-bound customers and perhaps decreased their traditional revenues.

The FCC is soliciting comments to its proposed rules by May 9. It indicated that it is particularly open to voluntary initiatives by commercial companies, or organizations such as the Telecommunications Industry Association and the Electronic Industries Alliance, to develop standards for 800 MHz cell phone usage on aircraft that would prevent interference with ground-based cellular networks. ■

# GSN Classified Ads

## SERVICES

### ACCOUNTING

**BUSINESS OWNERS**

WHAT is your business worth?

WHERE is your business going?

WHO reviews your industry and compares it to your company?

WHEN did you last review your buy/sell agreement or your life insurance needs for your business?

HOW do you strategically plan for your business's future growth?

WHY are you in business?

HAVE YOU asked or answered these questions recently?

IT may be time for a BUSINESS APPRAISAL / VALUATION.

A business appraisal is the smart business owner's strategic planning tool.

The appraisal will help you to answer these and other important questions.

**Ringler & Associates P.C.**

CERTIFIED VALUATION ANALYSTS
CERTIFIED PUBLIC ACCOUNTANTS

NOT YOUR EVERYDAY CPAs

**631-859-0100**
**www.ringler-associates.com**



### EXECUTIVE RECRUITMENT

**EXEMPT • POSITION DESCRIPTION**

**JOB TITLE: Business Development Manager, Government Services Group**

**SUMMARY:**

The primary function of this position is to drive the Government business; be the Government / GSA expert as it pertains to Sales & Marketing while working with district offices, and various internal groups. Responsible for key assigned Agencies, internal groups and geographies. Also, responsible for the development and management of specific programs in support of the overall Government Services Group Business Plan.

**RESPONSIBILITIES:**

- Develop & drive market strategies and tactics for Federal, GSA, and State business including identification of market opportunities for assigned geographies / Agencies.
- Develop effective relationships with district offices – become the Government expert for market area.
- Ensure District offices are trained on Government procurement, sales / internal processes, GSA, and State Agreements.
- Bring the correct personnel from district offices into various accounts while assisting with identifying significant sales opportunities and closing.
- Represent SimplexGrinnell in key trade organizations / trade shows.
- Help ensure we are customer focused, by addressing various issues with district management.

**BACKGROUND:**

**Education:** Undergraduate degree or equivalent experience

**Experience:** Minimum of 5 years relevant experience in fire protection sales or service. Ideally, two years experience in business development with Government agencies.

**Special Skills:** Ability to be a strong champion for the government businesses and to drive business within the SimplexGrinnell organization. Ability to present self and SimplexGrinnell effectively in front of customers and large groups. Strategic and analytic thinking skills. Ability to produce, present and defend business plans. Broad knowledge of various services & product portfolio we can provide.

**Contact John Harding, Government Services Group, 978 731 7179**
**Send resumes to: joharding@tycoint.com**

**Senstar-Stellar, Inc.**, a thirty-year-old electronic security equipment manufacturer is seeking a highly motivated Federal Market Sales Manager. The successful candidate must have proven experience selling technical security systems to the Federal Government, DoD, Homeland Security marketplaces. A minimum of 5 to 7 years experience in these areas in necessary and have the ability to work with both end users and system integration companies. Must be familiar with government agencies, and be able to follow current and emerging trends relating to security technology.

Candidate must be a self-starter, and demonstrate proven executive level presentation, communication, forecasting, sales and marketing skills. This position will require location in the Washington/Baltimore area, with travel to other parts of the U. S.

**Interested candidates please send resume to: usinfo@senstarstellar.com.**

## PRODUCTS - PHYSICAL SECURITY

### INTEGRATED SECURITY SYSTEMS



## AD CATEGORIES

**PRODUCTS**
- **IT SECURITY**
  - Hardware
    - Data storage
    - Desktop computer
    - Laptop computer
    - Firewall appliance
  - Software
    - Anti-virus / anti-spam
    - Authentication
    - Compliance
    - Database management
    - Document security
    - E-mail
    - Encryption
    - Firewall network monitoring
    - Patch management
    - Vulnerability management
    - Wireless intrusion
- **PHYSICAL SECURITY**
  - Access control
  - Asset tracking
  - Armored vehicles
  - Biometrics
    - Face recognition
    - Fingerprint
    - Iris
  - Bio-terrorism
  - Blast resistant
  - Communications
  - Detection
    - Chem / bio / nuclear
    - Chemical trace
    - Video
    - X-ray
  - Emergency alert notification
  - Identification
  - Integrated security systems
  - Intrusion detection
  - Locking mechanisms
  - Night vision
  - Object detection
  - Perimeter protection
  - Port security
  - Signage
  - Telecommunications
  - Video surveillance
    - Abandoned bag detection
    - Analytic software
    - Camera
    - Digital video recorder
    - Monitor
  - Wireless

**SERVICES**
- Accounting
- Airport screening
- Consulting
  - Background investigation
  - Forensics
  - Management
  - Vulnerability assessments
- Disaster recovery
- Document destruction
- Education
- Executive protection
- Executive recruiting
- Financial
- Guard services
- Internet services
- Investigative
- Legal
- Marketing
  - Advertising
  - GSA contracts
  - Market research
  - Public relations
  - Trade shows
- Publications
- Systems integration
- Threat assessments
- Training

**HELP WANTED**

Personality Profile

# Richard Falkenrath

## "On Duty"

**Current jobs:** Visiting Fellow, Foreign Policy Studies, The Brookings Institution; Senior Director, Civitas Group LLC; National security analyst, Cable News Network

**Career steppingstones:** Deputy Assistant to the President and Deputy Homeland Security Advisor, The White House (2003 – 2004); Special Assistant to the President and Senior Director for Policy and Plans, Office of Homeland Security, The White House (2001–2003); Director of proliferation strategy, National Security Council, the White House (2001); Assistant professor of public policy, John F. Kennedy School of Government, Harvard University (1999–2000)

**Education:** Ph.D., Department of War Studies, King's College, London (1993); B.A., Occidental College, Los Angeles (1991)

**Homeland security mission:** Analyst, consultant, commentator and "former"

**Top job priority:** To prepare the next generation of national & homeland security officials

**Biggest obstacle:** The need to earn a living

**Proudest career moment:** Passage of the Homeland Security Act of 2002

**Your role model:** Andrew H. Card, Jr., current White House chief of staff

**Career ambition:** The Cabinet

**Birth year:** 1969

**Hometown:** Mendocino, CA

**Childhood nickname:** Ricky

**Current residence:** Washington, DC

**Family:** Wife, Penelope Wilson; children: Olivia, 3-years-old and Reed, 1-year-old

**Last book read:** "The Blind Assassin," by Margaret Atwood

**Favorite films:** "Mystic River," directed by Clint Eastwood (2003)

**Ideal vacation:** Remote, desolate mangrove flat frequented by bonefish, permit, tarpon and other assorted game fish

**Hobby / sport:** Playing with my children; fly fishing; smoking, grilling, baking, and cooking; traveling; reading; watching NFL football

## "At Ease"

Richard Falkenrath lands a whopper in Mexico

**Favorite meal:** Medium rare USDA Prime bone-in strip; iceberg wedge with blue cheese and bacon bits; onion rings; pecan pie a la mode

**Clubs / groups:** Member, Aspen Strategy Group; member, International Institution for Strategic Studies; life member, Trout Unlimited

**Major regret:** Never to have served in the military

**Proudest achievement:** Marrying Penny and bringing two beautiful children into the world.

**Inspiring quotation:** "Do or do not; there is no try." Yoda

>THIS IS **THE WAY**

# THE U.S. DEPARTMENT OF DEFENSE STAYS ON THE OFFENSIVE.

You'll find Nortel™ embedded in the communications network of the U.S. Department of Defense. And wherever secure, reliable voice, video and data communications are critical.

>THIS IS NORTEL™

nortel.com

# Works well with others.


## Introducing FIPS 201 compliant readers.

HID's new family of FIPS readers meet the latest U.S. Government Smart Card Interoperability Specifications. They read FIPS 201 compliant cards in either low or medium assurance profiles, output the Federal Agency Smart Card Credential Number (FASCN), support multiple Wiegand output configurations, and are field upgradable. Make HID your card and reader bridge to interoperability between new and existing access control systems.

HID

**ACCESS** interoperability.

*iCLASS*