Interoperability Articles: Weeks of April 1, 2006 – April 14, 2006

Task force rolls DICE to keep lines open

April 3, 2006
GCN
By Mark Tarallo
URL: http://www.gcn.com/print/25_7/40226-1.html

Exercise aims for interoperability with DHS, first responders

The scene of a terrorist attack or a large-scale natural disaster, experts agree, is no place for technology specialists from different response agencies to begin coordinating communication efforts.

"The time of an incident," said Air Force Col. Babette Lenfant, director of communication systems for the Joint Task Force Civil Support, "is not the time we want to be exchanging business cards with the National Guard and saying, 'Here, this is what I do.' "

Various military services, the Department of Homeland Security and first responders such as police and fire departments are getting better acquainted with each other's communications systems during the Defense Department's Interoperability Communications Exercise.

DICE 2006, which started Feb. 6 and continues to April 14, is designed to establish whether systems are interoperable so when an emergency does happen, various agencies and levels of government can communicate effectively and efficiently.

The end goal, Lenfant said, is to take stock of the strengths and weaknesses of existing systems. "It's a great opportunity to see it all," Lenfant said.

DICE has its origins in smaller-scale equipment certification tests started in the late 1980s. Since then, it has evolved into DOD's premier interoperability exercise. In 2002, DICE became an annual event, based at Fort Huachuca, Ariz. This year, DOD held exercises in Okinawa, Japan; Fort Monmouth, N.J.; Camp Pendleton, Calif.; and Fort Monroe, Va., where JTF-CS, and Col. Lenfant, are headquartered.

At the Fort Monroe exercises, DICE participants tested multifunction mobile units designed to establish channels of communication at even the most devastated scenes.

A leading example of this type of system is the Air Force's Hammer Adaptive Communications Element (Hammer ACE), based at Langley Air Force Base, Va.

Run by a three-man rapid deployment team of engineers and technicians outfitted with advanced communications equipment, Hammer ACE (which has its own slogan: "Anytime ... Anyplace ...") is ready to go within three hours of notification. It also can begin operating 15 minutes after arrival on site—with the assistance, if needed, of a car battery or solar blanket to temporarily power the system.

The unit's services include an International Maritime Satellite (INMARSAT), developed by Thrane and Thrane Inc. of Virginia Beach, Va.

A Hammer ACE system includes:

- An Iridium satellite phone, providing worldwide secure access
- A UHF satellite radio with three multiband terminals made by Raytheon Co.
- A land mobile radio with 12 handheld Motorola XTS-5000 radios
- A video teleconferencing unit made by Scotty Tele-Transport Corp. of the Americas Inc. of Norcross, Ga.
- A GPS receiver from Garmin International Ltd. of Olathe, Kan.
- Cell phones from Engenius Technologies of Costa Mesa, Calif.
- Dell notebooks
- A Blackjack TS-21 fax machine.
- At Fort Monroe, Staff Sgt. Travis Queen demonstrated how the unit could connect the cell phones, land mobile radios, land-line phones and satellite radios used by different personnel, then link them all in a "talk group" so the responders could hold phone conferences.

Other agencies reported positive findings at Fort Monroe as well.

Army personnel displayed their expeditionary communications unit—a tent and satellite dish that provides videoconferencing, secure telephone service, laptop computers, Internet connectivity and e-mail.

DICE exercises, Army personnel said, allow for productive mobility testing, so the unit can be relocated quickly.

Specialists from the South Carolina Army National Guard, manning their own mobile communications center called ACE 1000, have been using their unit's ability to "cross-band," or interface different radios, to plug communication gaps between federal agencies and local first responders.

Overall, Lenfant said one of the key lessons of DICE 2006 is that maintaining interoperability is an ongoing job because technologies and capabilities are always evolving. Next year, she said, she hopes the exercise will expand further with the inclusion of system specialists from the Red Cross.

###

NACo Launches Public Safety Communications Project

April 4, 2006
Government Technology
By News Staff
URL: http://www.govtech.net/magazine/channel_story.php/99042

NACo recently received a $1 million grant from the Department of Homeland Security (DHS) and, with the funds, will offer a series of intensive policy academies on public safety communications and interoperability for local officials over the next two years.

The training is made possible through a funding agreement with DHS' SAFECOM Program Office, which works with federal, state and local public safety agencies to improve emergency response through more effective and efficient interoperable wireless communications.

"These resources will help NACo members be informed and effective leaders on such a critically important issue in our communities," said Marilyn Praisner, council member, Montgomery County, Md., who currently chairs the SAFECOM Executive Committee at DHS as well as NACo's Telecommunications and Technology Steering Committee.

The goal of the program is to improve local emergency preparedness by educating county officials and other local policymakers about wireless interoperability, building a better understanding of the complex issues involved and resulting in optimal local decision-making about public safety communications.

Under the grant, NACo will provide information and training to build awareness and knowledge; facilitate peer networking; and design and deliver technical assistance to counties in their efforts to implement interoperability strategies.

The program will aim to assist county officials to:
understand the importance of interoperability
be able to effectively communicate the benefits of interoperability to the public
understand the political and institutional barriers within the public safety community that can impede interoperability
facilitate collaborative planning among local, state and federal government agencies
encourage the development of flexible and open architectures and standards, and
support funding for public safety agencies that work to achieve interoperability within an agreed-upon plan.

Preliminary plans are underway to conduct the first policy academy at a mid-Atlantic disaster preparedness conference in the fall. More information will be available about the training schedule in the early summer.

The partnership with DHS is one of several new funding agreements recently awarded to NACo that will enable the association to expand its education, training and assistance programs for county officials. Other new programs coming online in 2006 include:

the Coastal Counties Restoration Initiative, to assist counties in protecting and restoring coastal wetlands and watersheds
a partnership with the Department of Defense on cooperative land-use planning around military installations
best practices for revitalizing previously used properties, such as brownfields
jail-to-community transition planning for inmates exiting county jails with substance abuse, addiction and mental illness diagnoses
strategies to increase access to health care for vulnerable populations, especially in rural counties and counties designated as persistently poor, and
enhanced research, education and training regarding methamphetamine and its impact on counties.

###

Lockheed Martin / Northrop Grumman TSAT Team Achieves High-Data-Rate Communications Processor Milestone

April 4, 2006
Northrup Grumman Corp.
By Bob Bishop
URL: http://www.primezone.com/newsroom/news.html?d=96703

A team led by Lockheed Martin (NYSE:LMT) and Northrop Grumman Corporation (NYSE:NOC) became the first to successfully demonstrate the interoperability of a new high-data-rate protected waveform in the initial test of the Next Generation Processor/Router (NGPR), the brain of future Internet protocol-based military satellite communications for the Transformational Satellite Communications System (TSAT).

The test of the NGPR, built by Northrop Grumman's Space Technology sector, was conducted against the TSAT RF Universal System Test Terminal at Massachusetts Institute of Technology's Lincoln Laboratory from Jan. 23 to Feb. 2. This initial compatibility test, NGPR-1, verified compliance with key aspects of the U.S. government's compatibility standards for the XDR+ waveform, a secure, protected, anti-jamming waveform developed for TSAT ground-to-satellite uplinks and downlinks.

The tests measured the compatibility of XDR+ as well as increased bandwidth efficiency to transfer more information in the same transmitted signal bandwidth. Northrop Grumman's NGPR operated at full-flight data rates established for TSAT.

XDR+ waveforms represent an advancement of the XDR waveform used on the Advanced Extremely High Frequency (EHF) satellite system. It meets the higher throughput requirements of TSAT, which uses both radio frequency and optical communications to provide secure, efficient, global communications for warfighters. The NGPR takes the information transmitted through military user terminals, determines where the information needs to go and selects the most efficient route based on standard commercial network design principles.

"The success of the NGPR-1 test is yet another important milestone in risk reduction for the TSAT program," noted Stuart Linsky, Northrop Grumman's vice president, Satellite Communications. "Our ability to successfully complete this test reflects our continuing track record of success in developing generations of sophisticated processors for MILSATCOM systems, including Milstar and Advanced EHF."

In addition to meeting planned objectives for NGPR-1, Northrop Grumman performed additional risk reduction tests on features for the next test, NGPR-2, which will include both waveform and networking capabilities. The NGPR is a critical component of TSAT, an Internet protocol-based system that is designed to provide military users with protected high-bandwidth communications whenever and wherever needed, as well as new communications-on-the-move capabilities. TSAT will network mobile warfighters, sensors, weapons and piloted aircraft in the air, on the ground, at sea and in space.

"The successful test represents an important step in our effort to advance breakthrough technologies needed for TSAT," said Rick Skinner, vice president, Transformational Communications for Lockheed Martin. "We look forward to continuing our work to provide the Air Force with a revolutionary system that will deliver extraordinary communications capabilities for our men and women in uniform."

The Lockheed Martin / Northrop Grumman TSAT space segment team, which includes ViaSat, Rockwell Collins, General Dynamics Advanced Information Systems, L-3 Communications, Stratogis and Caspian Networks, is currently working under a $514 million contract for the Risk Reduction and System Definition phase. This effort will culminate with a multi-billion dollar development contract to be awarded to a single contractor in 2008.

Lockheed Martin Space Systems, Sunnyvale, Calif., serves as the prime contractor. Northrop Grumman Space Technology has responsibility for the communications payload, including laser and radio-frequency communications and on-board processing. The U.S. Air Force is managing the program at the MILSATCOM Joint Program Office, located at the Space and Missile Systems Center, Los Angeles Air Force Base, Calif.

Northrop Grumman Corporation is a global defense company headquartered in Los Angeles, Calif. Northrop Grumman provides technologically advanced, innovative products, services and solutions in systems integration, defense electronics, information technology, advanced aircraft, shipbuilding and space technology. With approximately 125,000 employees and operations in all 50 states and 25 countries, Northrop Grumman serves U.S. and international military, government and commercial customers.

###

Crisis mandate remains unmet

April 9, 2006
2theadvocate.com
By Penny Brown Roberts
URL: http://www.2theadvocate.com/news/2602596.html

Infighting hinders 'interoperability'

A committee of Louisiana law-enforcement agencies charged with coordinating what has been deemed top priority in hurricane season preparations — making sure they can talk to one another — has yet to hold a single meeting.

Efforts have been stymied for months by behind-the-scenes fighting over who will control a radio and data system that allows emergency agencies to communicate in a crisis — and the millions of federal dollars that come with it.

In January, Gov. Kathleen Blanco appointed a Statewide Interoperable Communication System Executive Committee stacked with state officials and light on local first-responders.

After the Louisiana Sheriffs Association and other local law-enforcement entities balked at their lack of representation and threatened not to cooperate, the governor agreed to expand the committee — but still hasn't appointed all of its members.
Hurricane season arrives June 1.

"Much to our dismay — despite what we thought was a loud message demanding that we be in on the ground floor — the commission basically did not include first-responders in a real way. It was all about the state agencies," said Ascension Parish Sheriff Jeff Wiley, president of the Louisiana Sheriff's Association.

"No sheriff fancies or fathoms being the overseer of this major entity; we're comfortable with and understand the logic of State Police being the quarterback," Wiley added. "But what we do want is to be first-string players. Because when it hits the fan, we're the first ones on the scene."

Turf tussles continue even as communication has been fingered repeatedly as the single largest barrier to emergency response after Hurricane Katrina devastated the Gulf Coast on Aug. 29.

"A Failure of Initiative," the final report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, concludes that despite millions of dollars in federal funding for technology and communications, "the absence of true communication interoperability within and between affected jurisdictions severely hindered rescue and response efforts at all levels of government."

The terrorist attacks of Sept. 11, 2001, initially exposed the dramatic need for a uniform system nationwide through which emergency responders can talk to one another and exchange data — known as interoperability.

Since then, the federal government has given $8.6 billion to states for equipment, first-responder training and disaster exercises. Last year alone, the U.S. Department of Homeland Security gave states $2.1 billion — $935 million of which was allocated for communications upgrades.

Louisiana has gotten $135 million for preparedness since 1999 — $108 million of which went to parish and municipal governments; the rest to the state. Of that, nearly $107 million was dedicated to equipment purchases, but only $16 million actually was spent on interoperability.

On top of that, the city of New Orleans got a $5.5 million Community Oriented Policing Services grant for interoperability, but by September 2005 had spent only $275,428 of it, said Gilbert Moore of the COPS Program External Affairs Office.

Nevertheless, police officers, deputies and other emergency workers responding to the disaster had to resort to using CB radios and dispatching messengers with handwritten notes to communicate, according to testimony before Congress earlier this year. Commanders in the New Orleans Police Department went for days after the storm without talking to any supervisors.

Water and wind knocked out land telephone lines and electricity to government and commercial communications towers, limiting — and eliminating — radio, cell phone and Internet availability. The New Orleans Police Department dispatch center flooded, disabling what little connectivity existed between the department and other agencies. And portable satellite phones were hampered by heavy cloud cover.

FEMA officials claimed, for example, that because of hampered communications, they didn't know for days about thousands of people camped out without food or water at the Ernest L. Morial Convention Center. And New Orleanians with working cell phones resorted to Lafayette emergency agencies because calls for help to their own authorities went unanswered.

System outdated

Even before the hurricane did its damage, however, emergency communications in Louisiana were languishing.

Louisiana State Police currently use a decades-old statewide 800 MHz analog wireless communication system. It's used by 70 Louisiana agencies and 10,000 fee-paying users.

The manufacturer — Motorola — no longer manufactures parts or upgrades the technology, and by the end of the year plans to discontinue technical support. It has a capacity of only 46 towers and there's no space for new users.

At the same time, the Federal Communications Commission — trying to address growing interference on public safety radio transmissions by Nextel and other cellular operations — is encouraging law-enforcement to move to 700 MHz.

The new frequency — once the purview of public television — has a greater bandwidth to support not only voice interoperability, but data and imagery as well, which would allow agencies to transmit fingerprints, suspect photos, rap sheets, warrants, building blueprints and other critical information into the field.

The downside of switching to a new communication system is the cost.

In a December 2005 letter to the House Select Committee to Investigate the Preparation for and Response to Hurricane Katrina, Louisiana State Police Superintendent Col. Henry Whitehorn estimates Louisiana must spend $553 million for infrastructure and equipment "to achieve true interoperability" — plus more than $10 million annually to keep it going.

A 2004 U.S. Conference of Mayors Interoperability Survey found that two-thirds of the 192 cities surveyed are using 800 MHz to communicate with other public safety organizations. Just 2 percent were using 700 MHz.

The study also found Louisiana isn't alone in its predicament. It concluded that in 77 percent of the 192 cities surveyed, police and fire departments could not talk to one another, and in 66 percent of them, police, fire and EMS agencies weren't interoperable.

"We have what I've been calling the intersection of opportunity and necessity," said Lt. Col. Joey Booth, deputy superintendent of crisis response and special operations for Louisiana State Police.

"We're got to do something with our system because the vendor won't support it anymore, and they're already to the point where some of our gear they won't repair," he said. "And we have the opportunity to move into a bandwidth with all our state and local partners to run all of the applications that we need to run."

State vs. local

But money hasn't been the only impediment to interoperability. There's also politics.

A Government Accountability Office report to Congress last month cited a lack of "effective, collaborative, interdisciplinary and intergovernmental planning" as the single greatest barrier to decades-old problems of interoperable communications.

U.S. Comptroller General David M. Walker emphasized in his testimony that "no one first-responder group or governmental agency can 'fix' the interoperability problems."

Cash-strapped local law-enforcement agencies vying for their slice of the anti-terrorism funding pie have been suspicious of any state government efforts to control it. As Wiley expressed it, “if we’re not at the table of input, we can’t be surprised later on if the end result doesn’t meet our needs.”

But state authorities have argued true interoperability can develop in Louisiana only if it is coordinated at the state level.

In his December 2005 letter to the House Select Committee, Whitehorn suggests federal authorities give all funding designated for interoperability to the state, provided parishes and cities with 100,000 or more residents are included in the system.

“Compounding the issue of inadequate funding is the grant requirement that local governments receive a minimum of 80 percent of the funds — coupled with the inability of the state to direct those expenditures,” Whitehorn writes. “By virtue of the grant guidelines, the state cannot control how the local governments spend the grant funds.”

At stake is more than $135 million in Department of Homeland Security funding — $106 million of which is allocated for equipment purchases. Louisiana State Police currently get 20 percent of that money, with local law-enforcement agencies splitting the rest. That figure could climb even higher post-Hurricane Katrina.

Leonard Kleinpeter, Blanco’s special assistant, said authorities had been working steadily on addressing interoperability, “but it’s been on and off in terms of what was practical, whether there was proper input and where the money’s going to come from and who it’s going to go to. Every one of those things would cause a glitch in the system.”

When the governor appointed the first executive committee in January, however, the tension reached a breaking point. Kleinpeter said the District Attorney’s Association, Louisiana Supreme Court Justice Catherine “Kitty” Kimball and the Louisiana Sheriff’s Association contacted the Governor’s Office to complain.

He scheduled a meeting of federal, state and local authorities to hash it out, and the result was a revamped executive committee with greater local representation.

“It’s not that there were any problems; it’s what I described earlier,” he said. “If you have people on parallel tracks and the communication’s not there, and after all we’re trying to do interoperability and we don’t have everyone involved, by definition that’s not going to work.”

Booth insists Louisiana State Police aren’t making a power play in the interoperability game.

“We want a statewide network. I emphasize statewide because we’re not looking for it to be a state project,” he said. “The state is trying to get the ball rolling and present a table or platform for everyone to come and provide their input.

“The state wants to help with the initiative and make it statewide because we want to make sure there’s connectivity between all the users,” Booth added. “If a firefighter in Shreveport goes to New Orleans to assist in a response, his communication gear will work when he gets to New Orleans and he can talk not only back home to Shreveport but to other responders in New Orleans.”

Booth said key players from the state as well as local first responders already have begun meeting several times a week independently of the pending executive committee to work on interoperability issues.

Louisiana Commission on Law Enforcement Executive Director Mike Renatza said he believes the expanded committee — once it starts meeting — will alleviate worries on both sides.

“Regardless of what you have heard, I really think this can and will happen,” he said. “It is in all of our collective best interest to accomplish this task. I think the funding barrier can be overcome if we can assemble everyone on this common goal.”

Ready or not

So where does that leave Louisiana’s communications capabilities for the impending storm season?

Kleinpeter said the executive committee’s first task will be to develop a “hybrid interoperability plan” for the southeast Louisiana parishes most affected by the storm.

“If we can’t communicate there,” he said, “we’re in trouble.”

Louisiana State Police persuaded FEMA to issue a $15.9 million no-bid purchase order for a 700 MHz Motorola system — including upgrading 19 communication tower sites in that region. But the system reportedly was in limbo after the federal agency balked at spending $150 million for the handheld radios needed to communicate through the system.

State Police also bought eight ACU-1000 devices which will allow it to bridge — or patch together — otherwise incompatible radios, both 700 MHz and 800 MHz.

Blanco’s proposed budget includes $2.8 million of an unexpected windfall of sales tax and gambling revenue to upgrade emergency communications in southwest Louisiana to the 700 MHz system.

As for other regions, Booth said, the agency is urging their first-responder and other entities to purchase communications systems that meet national compatibility standards.

“Are we ready with the grand plan? Absolutely not,” Wiley said. “But the immediate needs are being worked on, and we’re on the right track. The week after Katrina, it was smoke signals. I’m confident it will be better this time.”

###

Globe Talk: Tech No Panacea To Preparedness

April 10, 2006
The Post Chronicle
By Shihoko Goto
URL: http://www.postchronicle.com/news/technology/article_21213851.shtml

Be prepared for the next big one to strike. That's been the rallying cry of the government ever since the Sept. 11, 2001, terrorist attacks, and yet public confidence in the public sector to deliver on those calls has been badly shaken since Hurricane Katrina. So high has public criticism been of the government in handling the natural disaster last autumn that the position of heading the Federal Emergency Management Agency is regarded very much as drawing the short straw -- a post anyone with political ambitions would not care to pursue.

For businesses, though, fears about another large-scale crisis shaking the nation -- be it in the form of terrorism or a natural disaster -- is an opportunity to win big public-sector contracts, too.

Certainly, there were plenty of bureaucrats from federal agencies that attended a half-day conference on emergency preparedness this week sponsored by mobile group Sprint Nextel. Still, the Washington hotel ballroom was packed not just with federal government officials, but also with firefighters, emergency medical providers and other first-responders from the nearby communities as well as representatives from non-profits involved with providing disaster relief on the ground, all who were eager to hear about what they could and should do in the event of a worst-case scenario.

But while Sprint was eager to promote its various products and networks, much of the actual presentations by public-sector officials and academics focused less on technology and more about trying to improve coordination among agencies and various groups that were all working for a common objective and yet often finding themselves in each others' ways when disaster struck.

"Technology is important, but it's not the core" of what emergency responders need, Undersecretary for the Preparedness Directorate at the U.S. Department of Homeland Security George Foresman told the audience. "The core is governance," he argued, pointing out that communications networks to ensure that all parties involved already exist. Yet a clear action plan on how to talk to which group and when was not let clearly defined, that would ultimately lead to confusion and even panic in the event of a disaster.

Indeed, the former coordinator for the fire department that handled the Columbine High School shootout in 1999 detailed in his speech how fire department officials were at one end of the school while the police force were on the other, and they were unable to talk to each other to coordinate activities initially as both groups used different frequencies.

Meanwhile, using cell phones to communicate was not an option as "too many people were trying to talk at the same time ... and they were all clogging up the lines," said William Pessemier, formerly of the Colorado Fire Department and incident commander at Columbine High School Littleton, who is now executive communications systems adviser for the International Association of Fire Chiefs.

Pessemier pointed out that the worst-case scenario actually did happen at Columbine, as the police and fire officials got in each others' way as "interoperability broke down," and the police actually mistook one fire official for someone siding with the students wrecking havoc within the school.

Of course, that's not to say emergency relief workers and governments on the local, state and federal level should settle for ancient technology and networks. In fact, the need for secure and fail-proof communications networks with mobile broadband and encrypted e-mail systems are prerequisites to preparing the nation for a large-scale emergency situation.

Yet simply investing in those state-of-the-art technologies is not enough. Presenters at the conference all agreed that organizations must not only come with plans for internal action, but they must also communicate more among themselves at all levels to ensure that they do not replicate efforts, or worse, prevent each other from doing their respective jobs. When it comes to preparing in advance, though, there is only so much that can be learned from past mistakes, cautioned Leonard Marcus, co-director of the National Preparedness Leadership Initiative at Harvard University.

"The past is not a reliable predictor of what might occur, especially if it is unprecedented," Marcus said. Rather, it was more important for leaders to conquer their fear of the unknown and fear of personal failure so that they will not hesitate to take decisive steps under a situation when time is of the essence.

Whether or not that is the case, one thing is clear: Public awareness of the need for emergency preparedness is higher than ever before, and expectations for the government to handle the next disaster, be it man-made or natural, are high as well.

"We need to capture this moment in time" to meet those expectations "or we will lose it," Foresman said.

###

Penalties proposed for poor radio communications

April 12, 2006
9news.com
By Marissa Pasquet
URL:
http://www.9news.com/acm_news.aspx?OSGNAME=KUSA&IKOBJECTID=864fdc10-0abe-421a-0050-69e0bf3bb76a&TEMPLATEID=0c76dce6-ac1f-02d8-0047-c589c01ca7bf

DENVER - Nearly seven years after the Columbine tragedy, hundreds of first responder agencies throughout Colorado still cannot communicate with each other over radio frequencies and some state lawmakers are tired of waiting for the process to evolve naturally.

Senator Dan Grossman (D-Denver) said he will introduce a measure within the week to withhold homeland security money from any city or first responder agency which does not adopt a technology plan which works with the statewide Digital Trunk Radio System.

"It doesn't mean you have to buy a particular radio if you can show us a technology that's going to work (with our system)," said Grossman, who also chairs the Senate's Select Committee on Homeland Security.

"Show us how you're going to become interoperable not just with your neighbors, but with the state system, so we can all rely on our first responders to talk to one another if, God forbid, another Columbine happens or another tragedy of that scale happens in Colorado."

The process is called radio interoperability and currently, Grossman says 400 of the state's 1,400 first responder agencies use the same technology as the state.

Public safety organizations throughout the U.S. continue to face the difficult challenge of achieving true radio interoperability which will enable them to communicate across agency, jurisdiction, and geographic boundaries while using dissimilar equipment and frequencies.

Supporters for radio interoperability do not see the issue as a convenience. They believe it is a matter of life and death. Supporters say if police, fire and EMS crews cannot talk to each other, the margin for error - and loss of life - can be profound.

That's why supporters say they will hold back homeland security money to force fixes.

"There has to be an enforcement mechanism," said Grossman. "Just saying you have to do it, there's no reason for people to comply. We need to send a message the state is serious about this issue and that we're willing to put our money where our mouth is or

take the money away where the mouth isn't and that is where people are not willing to come up with interoperability plans."

State lawmakers finish their annual session one month from Monday.

9 News contacted the County Sheriff's of Colorado in response to the legislative proposal, but we haven't heard back at this time.

###

Tech firms tackle border security challenges

April 12, 2006
FederalTimes.com
By Adam Stone
URL: http://federaltimes.com/index.php?S=1673638

Holding down the fort on the home front takes brains and muscle, brawn and ingenuity. Plus it takes some really cool toys, stuff like fiber-optic perimeter sensors and portable satellite communications centers.

When it comes to homeland security, “the technology aspect is clearly a key enabler,” said Alan Balutis, president and chief executive officer of government strategies at research firm INPUT.

Those on the front lines say smarter solutions are indeed a key ingredient in the security recipe. “Technology is a critical and important piece of what we are trying to accomplish,” said Jim Williams, director of US-VISIT, a program to screen foreigners as they enter and leave the country.

The numbers tell the tale. The Homeland Security Department’s fiscal 2006 budget contained $3.6 billion for information technology spending, Balutis said. The proposed budget for 2007 includes $4.4 billion for IT, a 22 percent increase.

Clearly, technology is intended to be a big part of the homeland security solution. Take, for example, the realm of border protection and security. With Homeland Security bidding out its Secure Border Initiative, big brains nationwide are out to show how their machines can keep the borders secure.

At Annapolis, Md.-based CompuDyne, chairman and CEO Martin Roenigk describes a fiber-optic detection system that cover distances too vast to be managed by traditional cable, while pinpointing intrusions to within a couple of feet.

“The technology out there is old and expensive, and there is a lot of new stuff out there that could make controlling that border a lot more effective,” Roenigk said.

While some baddies may be trying to get across the borders in the flesh, others may think U.S. seaports offer a route to smuggle in foul materials, be they of the biological, chemical or even radioactive varieties.

Robert Ledoux has considered the problem and is looking for new applications to stop such traffic in its tracks. As president of Acton, Mass.-based Passport Systems, he is looking to develop nonintrusive cargo inspection technology.

Passport Systems already has a contract with the Domestic Nuclear Detection Office to help produce a detection system that would scan a cargo container and identify every element bigger than helium. Do that, and you are apt to spot potentially harmful radioactive components. Ledoux said he can have the system ready in less than two years.
Others are considering technologies such as radio frequency identification as a way to quickly scan and process incoming cargo. Coast Guard Rear Adm. Patrick Stillman said that using RFID at seaports could cut backlogs and help the U.S. economy. “The more that queue is lengthened, the more you pay at Wal-Mart,” Stillman said April 4 at a panel discussion hosted by the American Council for Technology’s Information Advisory Council in Vienna, Va.
Like many on the cutting edge of the defensive sciences, Ledoux gives high marks to Homeland Security and other government agencies for seeking out new and better tools for patrolling the perimeter. “I am encouraged to see that they are putting in place a plan that is addressing threats in a prioritized order,” he said.
Even more important, he said, decision-makers are being methodical about what they choose to pursue. Before going to full deployment phase, “they are trying to decide which new technologies need to be brought to the point where they can be tested in the field.”
An example is with Homeland Security’s SAFECOM project, which aims to connect wireless communication systems used by federal, state and local first-responders.
Commercial ventures are working on this problem too. Take for instance British Columbia-based satellite technology company Norsat, which has developed a compact satellite-communications system that can be set up and used under virtually any circumstance. “If there is a catastrophe like [hurricanes] Katrina or Rita, one of the first things that will be unavailable is the communications systems that people use,” said CEO Bill Coyne.
In September, Norsat supplied such systems to the Army’s 1st Cavalry Division to transmit high-fidelity data and video as part of Joint Task Force Katrina.
Billions of dollars have been allotted, initiatives have been launched, the private sector has stoked the furnace. There’s lot of smoke at the intersection of technology and homeland security. But is there fire? The answer is a qualified yes. “A lot of it depends on who you talk to,” INPUT’s Balutis said.
“The technology aspect is clearly a key enabler,” he said, but there still is some energy in the direction of more brute-force solutions. “You can say: ‘We’re just going to hire more inspectors, we are going to hire more border and custom agents, just hire more people.’ And to a considerable extent, that has happened.”
Overall, though, the vast scope of the problem at hand is pushing government inexorably toward the adoption of cutting-edge technology as a front-line solution.
As time goes by, “a lot of people are going to say that at some point we really need to look at the technology types of solutions that are going to provide real-time information faster for protection and detection,” Balutis said. “Ultimately that technology is going to be the real enabler for DHS to be able to find a solution and protect the homeland.”

###

First Responder Radio

April 12, 2006
Military Information Technology
By Mickey McCarter
URL: http://www.military-information-technology.com/article.cfm?DocID=1398

Responding to a communications problem that has continued to vex first responders during major disasters, the federal government is pushing ahead with development of a nationwide radio system linking some 80,000 federal, state and local law enforcement and emergency management personnel.

The departments of Justice, Homeland Security and Treasury have been teaming up to establish the Integrated Wireless Network (IWN), which targets the interoperability woes that have plagued public safety workers during times of crisis.

Although the Department of Defense is not directly involved in the procurement, companies competing to become the prime contractor for IWN say that their experiences putting together systems for DoD has convinced them that achieving the goals of IWN are feasible.

Four contractor teams—led by Lockheed Martin, General Dynamics, Motorola and Raytheon—are competing to become the lead systems integrator for IWN. These teams survived a first-phase competition last year—along with the Boeing, which has since dropped out of the competition—after the Justice Department certified their initial proposals as satisfactory for IWN requirements.

The remaining teams face another possible down-selection this spring, when Justice may drop one or two of them and then let the remaining companies compete until the final award at the end of the year. Experts predict that the government will select one systems integrator to run the final network of integrated voice and data communications.

IWN has a $10-billion ceiling over a possible lifespan of 15 years, according to the IWN Joint Program Office, although the estimated total value of the program tops out at $2.5 billion. The IWN competition is designed to result in an indefinite-delivery, indefinite-quantity contract with a base period of five years and two additional five-year option periods. The IWN Joint Program Office estimates that IWN will serve more than 80,000 law enforcement officials across the departments of Justice, Homeland Security and Treasury as well as at the state and local levels, while reaching up to 2,500 sites across the United States.

The IWN network is also required to integrate legacy systems with new equipment while using strict security and encryption measures. The joint program office also requires that the system support new technologies such as Voice over Internet Protocol.

“The scope of this effort, while currently focused on voice and data communications, includes wireless information transmission, such as data, files, streaming video, images, and applications yet to emerge,” according to the IWN request for proposals for phase two of the program.

Management Enabler

Given the size and complexity of the proposed program, observers suggest, it’s not surprising that key competitors in the IWN project point to their DoD experience as evidence that they and the government are on the right path with IWN plans and strategies.

The depth of Lockheed Martin’s experience with integrating complex military communications systems has positioned the company as a successful competitor in the IWN race, according to Gordon McElroy, vice president of intelligence and homeland security at Lockheed Martin.

“With most complex DoD systems, technology is not the key enabler,” McElroy said. “The key enabler is the management of products, technologies, subsystems, requirements and people to produce a system of systems that meets its requirements in a reliable manner. This is system integration, and system integration is an essential element of any complex program.”

Lockheed Martin manages bigger and more complex systems than IWN for DoD on a daily basis, providing the company with the seasoning to tackle complex communications programs that involve different users in separate agencies with different missions and needs, McElroy explained.

“We learned long ago from the military that the problem is so much more than picking an equipment manufacturer and buying radios, but rather it’s all about the approach to ensure a high-performance network is focused on satisfying multiple missions with a solid infrastructure,” he added.

While acknowledging that the challenges in IWN are unique to that project and its contracting agencies, McElroy argued that his company has gained the tools, experience and people required to run a robust and challenging program on the scale represented by IWN.

“You are not going to see an analogous communications program per se at DoD that is similar to IWN, but what you will see is analogous integration of technologies or subsystems and requirements to produce a systems-integrated architecture that is essentially a system of systems,” McElroy said. “There are numerous platforms out there for communication. There are numerous data transport layers. There are numerous formats and all that kind of stuff that we have architected in a number of networks for DoD.”

But technology developed under the auspices of military programs also would have direct application to IWN, McElroy noted. Specifically, Lockheed Martin is very interested in the ability of the Internet Protocol to interconnect systems both old and new.

"We have applied IP to numerous communication programs such as WIN-T, MUOS, net-centric warfare and our recent TMOS win," McElroy said, referring to the Transformational Satellite (TSAT) Communications program's ground-based Mission Operations System (TMOS). "IP has the ability to enable the secure interconnection of both new and legacy communication systems providing the IWN user access not only to his/her fellow agents or officers, but also access a wide variety of network application and databases."

The use of IP applications would enable law enforcement personnel using an IWN network to enjoy the same interoperability that many military warfighters share under net-centric warfare concepts, McElroy said. Such an approach will enable FBI agents to talk to Customs agents without using extra radios and juggling several of them, depending on who needs to talk to whom.

In the future, IWN also may enable users to talk to military personnel.

"DoD has different kinds of security requirements, different kinds of protocols for getting on that system. But once a need is identified or once a mission is identified, having DoD or IWN users be able to integrate together or network for a specific task force or whatever is not outside the realm of possibility," McElroy said.

Rescue 21

General Dynamics C4 Systems, meanwhile, has capitalized on its experiences with the departments of Defense and Homeland Security in its development of an IWN solution, according to Lee Wright, director of national communications and homeland security.

"Our experience in developing, deploying and supporting the nationwide wireless communication system for the Coast Guard points to the fact that larger-scale system-integration projects must be architected as a total system and dynamically managed in order to meet the most pressing interoperability objectives," Wright said. "As the prime integrator and logistics provider for the Common Ground Station [GCS], we enabled the DoD's communications and situational awareness with a global real-time data, video and voice network."

General Dynamics is leading a team to overhaul the Coast Guard's national distress-communications system with a new project called Rescue 21. Rescue 21 would serve more than 78 million boaters and 13 million vessels navigating coastal and intra-coastal waters as the primary U.S. maritime emergency system, according to Coast Guard estimates.

In the case of the CGS, the Army sought tactical communications to provide real-time C4ISR capabilities from multiple sensors. According to General Dynamics, the company has implemented a solution that provides the Army with the ability to "acquire, process, display and disseminate" data from a variety of sources on the ground, in the air and in space.

The challenge of providing interoperable communications for more than 80,000 law-enforcement officers and federal agents presents large-scale and critical needs similar to those in the individual Coast Guard and Army projects, Wright said.

"The technology solution is all about interoperability and the ability for users on the network to have access to all relevant information," Wright explained. "IWN is the first communications system to be procured by multiple departments—versus having every agency buy its own small system—so it can really solve the interoperability problem."

For example, such interoperability would enable customs and border-protection officials at the Department of Homeland Security to access intelligence databases owned by the FBI, Wright noted. The ability to network such information also provides everyone involved with access to a common operating picture at a central location, such as a joint command center.

Systems Integration

In making their case, Raytheon executives point to their company's work as the prime mission systems integrator for the Navy DD(X), the fleet's next-generation destroyer, as well as a provider of military tactical communications across a range of programs.

The company also recently finished a program for Brazil for monitoring the Amazonian rain forest with a network of communications, sensors, radars and other technologies. That has strengthened the company's experience in establishing a network of networks across a large geographic area, according to Jerry Powlen, Raytheon vice president of integrated communications systems.

"Raytheon offers a unique capability in that not only do we have the large systems integration capabilities, we also have a lot of deep roots in wireless technology itself," Powlen said. "Raytheon is one of the leaders in wireless technology for the military from a tactical communications point of view. So while it's great and it's important for a system to have the capability to manage suppliers, people, processes and requirements, if you don't really have an underlying knowledge of the base technology domain itself, sometimes these programs get away from you."

The Raytheon IWN team consists of AT&T, Bechtel, Hewlett-Packard and Cap Gemini. AT&T originally led the team during phase one of the IWN program, but quickly concluded that Raytheon's capabilities were best suited for leading the team into the second and third phases of the competition phase.

The IWN Joint Program Office has never set goals for interoperability with DoD, Powlen noted. But the military's assistance to the Gulf Coast after Hurricane Katrina has underscored the need for wireless interoperability between first responders and DoD.

"So while the customer clearly hasn't defined the requirement to achieve interoperability between IWN and DoD, I think anybody who can sit here and see what we have lived through for the past nine months, can clearly see the value in the bridging of these networks between DoD so you can achieve interoperability. Currently, that is not the path IWN is on," Powlen said.

But the departments of Justice, Homeland Security and Treasury have made it clear that they recognize IWN is an evolving program, Powlen emphasized, and they learned some of the lessons that have been incorporated into it from challenges faced by DoD.

"Technologies will continue to evolve, and one of the issues that DoD continually faces is that they launch a program that takes three to five years of development, and by the time they are ready to field the technology, the technology is obsolete. It certainly is not state-of-the-art," Powlen said. "Homeland Security and Justice are painfully aware of how the world works. While they set up this IWN capability, they are looking for some of the same things that DoD is looking for, which is open architecture, non-proprietary systems and open standards."

###

Bills Reforming FEMA, Upgrading Communications Being Drafted in House

April 12, 2006
Congressional Quarterly
By Patrick Yoest
URL: www.cq.com

Proposals to reform the Federal Emergency Management Agency (FEMA) and improve emergency communications will likely emerge next month, according to Rep. Dave Reichert, R-Wash.

Reichert announced the bills at a hearing Wednesday morning in Orting, Wash. Reichert, who chairs the House Homeland Security Subcommittee on Emergency Preparedness, Science and Technology, said he would introduce the legislation "within the next month or so," adding to a legislative calendar for the House Homeland Security Committee that already includes comprehensive port security legislation.

The FEMA proposal will not make the emergency response agency independent, but will "better integrate" it into the Department of Homeland Security, according to Reichert. The proposal would reunite FEMA with the DHS Preparedness directorate.

Preparedness and response functions had been formally separated in the DHS's 2005 Second Stage Review, a comprehensive reorganization of the department.

The announcement comes after a bipartisan group of House members released a statement Wednesday calling on Congress to leave FEMA within DHS. The group included Reichert, House Homeland Security Committee Chairman Peter T. King, R-N.Y., House Homeland Security Committee ranking member Bennie Thompson, D-Miss. and Rep. Bill Pascrell Jr., D-N.J.

"Removing FEMA from DHS would only exacerbate the agency's problems," the statement said. "It would reduce FEMA's access to the vast resources available within the Department, create duplicative response efforts for natural and man-made disasters and significantly delay our ability to prepare for future emergencies."

That sentiment is reflected in Reichert's FEMA legislation, which is now only in draft form. According to a subcommittee staffer, the legislation would also codify many of recommendations included in the White House's "Lessons Learned" report on the Hurricane Katrina response.

The FEMA legislation appears to be an alternative to FEMA's removal from DHS, which has been proposed by Rep. Bill Shuster, R-Pa., the chairman of the Transportation and Infrastructure Subcommittee on Economic Development, Public Buildings and Emergency Management.

Reichert's bill would keep FEMA a coordination agency, managing assistance to localities, rather than a cabinet-level response agency, according to sources.

"FEMA has never been a response agency," a senior committee staffer describing the draft legislation said. "It is and should remain a coordination agency, designed to support state and local governments when a catastrophe overwhelms them."

The emergency communications bill, which takes aim at persistent problems with establishing radio interoperability in response to catastrophic incidents, could eventually be combined with the FEMA reform legislation. The emergency communications bill is also in draft form right now.

Under the bill's provisions, a $1 billion interoperability grant program, created by the sale of the federal radio spectrum, would be moved from the Department of Commerce to the Department of Homeland Security. DHS has already begun to manage much of the program, but Commerce maintains official control.

The Emergency Preparedness, Science and Technology subcommittee will hold a hearing April 25 with key federal players to discuss grant programs, according to the staffer.

A number of different interoperability programs currently residing in the DHS Science and Technology directorate, including the National Communication System, SAFECOM

program and the Integrated Wireless Network would be transferred to a new Office of Emergency Communications. That office would be headed by an assistant secretary who would be confirmed by the Senate and would be directly responsible for all interoperability efforts within DHS — an interoperability “czar,” in the words of one staffer.

Technical portions of DHS’s interoperability operations would remain in the Science and Technology directorate.

###

Va. emergency systems to get aid

April 13, 2006
Times Dispatch
By Michael Martz

$2 million distributed to 25 areas to improve response in disasters

Firefighters and rescue workers in Hanover County will be able to radio their counterparts in Richmond and other neighbors in a regional emergency.

Police in Petersburg will be able to monitor video feeds from a safe distance and retrieve medical data from hospitals. Fire and rescue crews will be able to find out about potential hazards in buildings they're about to enter.

Hanover and Petersburg are two of the 25 localities that learned yesterday that they will receive federal grants in the next two weeks to improve the ability of emergency communications systems to talk to one another in a disaster. Virginia is distributing $2 million through its homeland security grant program.

The purpose of the grants is to improve the "interoperability" of emergency communications systems in a terrorist attack or natural disaster. The issue has been high on the country's security agenda since the chaos that followed the attacks on the Pentagon and World Trade Center in 2001.

In Hanover, for example, county fire and rescue workers use a radio system made by M/a-Com Inc., while emergency workers in neighboring jurisdictions rely on systems made by Motorola. "They will not naturally talk to each other," said Cecil V. "Buddy" Martinette Jr., assistant county administrator in charge of emergency communications. "You can do some patching and things, but that does not really work well in an emergency situation."

The county's sheriff's department received grant money last year to buy portable radios so it could communicate directly with law-enforcement agencies in Richmond, and

Chesterfield and Henrico counties. The $75,000 grant announced yesterday will allow Hanover to buy portable radios for fire and rescue services, as well.

Petersburg also received a $75,000 grant through the state. The city plans to use the money to create a wireless, high-bandwidth network capable of transmitting data -- from building plans to medical information and video feeds -- according to a spokeswoman for the Petersburg Police Department.

The city already is improving its ability to share voice communications by erecting an 800-megahertz communications tower, financed by a grant from a nonprofit foundation, the department said. The new grant will expand the ability of city police, fire and rescue workers to share critical data in an emergency.

The grants were awarded by the State Interoperability Executive Committee, which Gov. Timothy M. Kaine said is the only such coordinating committee in the country. The committee is primarily composed of representatives from police, fire and rescue organizations, which are the "first responders" in an emergency.

###