

TR2 Terror Response Technology Report

Business Opportunities for Critical Infrastructure Protection

September 6, 2006

www.defensedaily.com

Vol. 2, No. 18

Briefing

► The Transportation Security Administration has slowed the deployment of General Electric [GE]-produced EntryScan walk through explosives trace detection portals used at some U.S. airports, citing maintenance issues. TSA and GE are working on enhancements to improve the already deployed and next generation units. TSA originally purchased walk through trace detection portals from GE and Smiths Detection for airport pilot programs but earlier this year decided to award GE a sole-source contract to continue producing the machines. So far 94 of the portals have been installed against TSA's goal of over 300 by the end of 2006.

► American Science & Engineering [ASEI] received a potential \$46.2 million contract from the Marine Corps for service and maintenance support for 67 Z Backscatter Vans fielded in Iraq and Afghanistan. The initial value of the award is \$11 million and contains options that would extend the contract to May 2009. The award is one of two major contracts the company says it is expecting in the near-term.

► TSA plans to award a sole-source contract with Infoglide Software Corp. to provide system design, testing, and support for the Secure Flight program. TSA is developing and maintaining threat-based vetting systems and analytical processes that can detect terrorist threats from known and potential terrorists in near real-time.

L-3, SAIC Selected for ACSD Phase Two

The Department of Homeland Security (DHS) has selected **L-3 Communications [LLL]** and **Science Applications International Corp. (SAIC)** to further develop and provide prototypes of security devices that can quickly detect threats to cargo containers.

Managed by the Science and Technology Directorate of DHS, one of the goals of the Advanced Container Security Device (ACSD) program is to "jumpstart" development of a sophisticated security system within the electronics industry that can detect unauthorized breaches of a standard cargo container while also monitoring its internal conditions, Bob Knetl, the ACSD program manager at DHS S&T, tells **TR2**. "So we chose two solutions with the least risk and greatest chance of success while still achieving our goals."

SAIC actually was selected in February and L-3 in June to move into Phase Two, which lasts 18 months for both contractors. Phase One, which began in FY '04 and ended last year, also included the engineering and construction firm **Black and Veatch**, **General Electric [GE]**, and Georgia Tech Research Institute.

Knetl says that Phase One of the program showed there are various approaches to the challenge of developing an ACSD. "We also learned that some technologies were not far enough along or integratable enough yet to move forward." The technical challenge of developing an ACSD appears daunting, Knetl and industry officials agree.

Under the original Broad Agency Announcement issued by the Homeland Security Advanced Research Projects Agency, the ACSD performance require-

► *continued on p.3*

Inside

Aquatic Bio-Monitor	2
Earnings News	5
Business Opps	8

DHS Lab to Review Guardian Technologies PinPoint Software

The Department of Homeland Security's (DHS) Transportation Security Lab (TSL) has agreed to assess software developed by **Guardian Technologies International, Inc. [GDTI]**, that analyzes images taken by airport checkpoint X-Ray machines and alerts screeners to the presence of explosives.

TSL's review of the image analysis software, which begins this week, is obviously a critical step for Guardian Technologies if it is going to sell its PinPoint threat detection technology to U.S. civilian agencies for homeland security purposes. There is no timeline to complete the TSL assessment.

Guardian's first target customer is the U.S. is Transportation Security Administration (TSA), Steve Lancaster, the company's vice president, tells **TR2**. But a potentially larger market exists through the Federal Protective Services which maintain security at U.S. federal buildings, thousands of which require a certain level of security screening, he says.

The Federal Protective Service

► *continued on p.6*



► DHS [cont'd from page 1]

“looks at what TSA is doing and follows their validation process” for security technologies, Lancaster says.

The PinPoint image analysis software is a standalone package that runs on a standard Pentium IV computer processor and essentially just analyzes the image provided by an X-Ray machine.

“We’re saying we’re like a second set of eyes,” Lancaster says.

The images provided to TSA screeners from X-Ray machines show organic materials in the orange color range. While explosives are organic, so are many other things that are packed into carry on bags, and plastic explosives can be formed into different shapes, thereby making it nearly impossible for screeners to tell the difference between innocuous and threat objects.

PinPoint basically “extracts” the image generated by the X-Ray machine and brings “it into our box,” Lancaster says. PinPoint then analyzes that image and puts it on a second monitor that displays whether a threat has been found and if so, “it will put a big red box around where we think that explosive is and at the bottom it will say check bag, or whatever they want it to say,” he says.

“It’s still up to the screener to determine what they want to do, regardless of what we say,” Lancaster says.

The second monitor could be right beside the one used by screeners using X-Ray machines or it could be in a remote location.

Based on the colorization provided by the X-Ray machine produced images, PinPoint can begin to distinguish the densities of the various organic materials to pick out “areas of interest” for more analysis, Lancaster says. However, the software can’t determine the presence of a threat just based on the densities, he says. That’s because if a bunch of organic materials are stacked on top of each other it will impact the colorization and possibly end up displaying as brown or black in the image, making it impossible to tell what the items are.

Through an “iterative process,” PinPoint automatically selects areas of interest for further investigation “where we begin to get different responses from those items, whether they’re stacked up or not stacked up,” Lancaster says. “And we do that until we’ve received the response or a unique signal that tells us either that an explosive or inert object is present. Through the development of the product we know the unique signals that we’re looking for an explosive. We do a lot of contextual imagery where we map down to the pixel level the relationship of the pixels around it. Remember, you can’t go by shape and you can’t go by density alone, so we apply some higher mathematics to the contextual imagery and orientation to ensure that we are finding that unique signal that we’ve established that each explosive has through

► L-3 [cont'd from page 4]

tics service providers may eventually adopt the ACSD technology in order to help drive the government’s requirements. Still, whether shippers want an ACSD or CSD may depend

the development process.”

The TSL testing will also be beneficial to Guardian Technologies because the company will gain from the “thousands of explosives images packed in various carry on bags” during the independent assessment, Lancaster says. “So we can see if we need to fine tune the product for those various explosives that the labs can provide.”

Liquid Explosives

The ongoing development of the image analysis software could also yield the ability to alert to liquid explosives threats. Lancaster says that after the news broke about the breakup of the alleged plot in Britain to bring down several or more aircraft on trans-Atlantic flights to the U.S. using electronic devices to trigger liquid explosives, he had his development team find the “signature” of one liquid versus a bunch of others. It only took them two to three hours to obtain the signature and “from various cluttered bags we could pick out that one liquid,” he says. It would work the same with liquid explosives, he adds.

Eventually PinPoint could be integrated into X-Ray machines but they don’t have enough processing power to use the software now, Lancaster says. Guardian Technologies is talking with all the X-Ray machine manufacturers and wants to avoid being exclusive with any of them, he says.

Integrating PinPoint into the computed tomography (CT)-based Explosives Detection Systems used to screen checked bags for explosives would be easier since those machines are equipped with plenty of processing power to search for bomb threats, Lancaster says.

Lancaster says that the CT machines provide three-dimensional imaging, giving a better view of the contents inside a bag, which would enable PinPoint to conduct better analysis to “enhance the detection capability and drastically reduce the false alarm rate, which then requires secondary screening.”

However, Guardian Technologies hasn’t worked in the CT area yet because there’s “enough to keep us busy on the X-Ray side” since those machines don’t provide any explosives detection capability, Lancaster says.

The software behind PinPoint is the basic platform Guardian Technologies is using in other products as well. In May the company unveiled PinPoint nSight, which would provide image analysis for portable X-Ray detectors used by bomb squads. PinPoint nSight offers better image clarity, colorization of grayscale images and a visual representation of the texture of scanned materials. The product has been field tested with the Miami, Fla., police bomb squad and is being used by the FBI at its school in Alabama.

The image analysis software is also being used in clinical trials for medical radiology imaging and the company is also getting into analysis of hyper-spectral imaging for the Defense Department, Lancaster says.

on the value of the product being shipped, he says.

For now it appears to be anybody’s guess on what the market wants in the way of secure containers. “There’s no paradigm we can call upon today for container security,” Young says.