

Centrify Declared 2011 Winner for "Best Identity Management Platform"

Reprinted with permission from the print & online editions of *Government Security News*



Photo coverage of GSN's 2011 awards program

Continues on page 15



Special section on mass notification technologies

Begins on page 31



December, 2011 Vol. 9 Issue 12

The News Leader in Physical, IT and Homeland Security

World Business Media, LLC

A new take on securing USB flash drives

Once upon a time, USB flash drives were so cheap and convenient they were passed out free of charge at trade shows and every professional seemed to gather a collection of them in their desk drawers. PAGE 4

Preventing disclosures by 'data-masking' your database

Suppose you're the Chief Information Officer for a major federal department or agency—such as DHS, the FBI or TSA—and your database administration team is planning to make a change in the way your organization accesses data. PAGE 8

Homeland security as an integrative field: Implications for academia

With the emergence of homeland security (HS) as a field of public policy in the immediate post-9/11 period, there arose a commensurate need to educate HS professionals. PAGE 11

DHS offers paid summer internships in science, technology, engineering and math (STEM)

DHS sponsors a 10-week summer internship program for rising college or university juniors and seniors majoring in homeland security-related science, technology, engineering and mathematics (HS-STEM) disciplines. PAGE 13

GSN posts video interviews with winners and sponsors of 2011 awards program

GSN's video production team reports that the first nine of 18 video interviews conducted with winners and sponsors of its 2011 awards program and dinner have been posted on the GSN Website. PAGE 22

This is only a test...Alabama leverages satellite to provide emergency alerts

Until recently, emergency alert tests have been conducted by states and localities alone, and were not integrated at the federal level. PAGE 31



Bastrop County Unified Command won accolades from GSN for its successful battle against Texas wildfires

Mobile devices spawn new B.Y.O.D. security policies

By JACOB GOODWIN

Party goers are often encouraged to B.Y.O.B. (Bring Your Own Bottle) and, increasingly, employees at U.S. companies are being encouraged—or at least allowed—to B.Y.O.D. (Bring Your Own Device.)

That's the catchy phrase being used to describe a recent trend that's now sweeping across the country—the willingness of many American employers to allow some or all of their workers to use their personally-owned smart phones and other hand-held devices, such as iPhones, Blackberries, Android-driven phones, iPads and other portable gizmos, to access company data and perform company work.

The push to B.Y.O.D. comes largely from employees in their 20's and 30's, who have grown up using their smart phones throughout the day to communicate, to surf the Web, to shop, to download music, movies and other entertainment, to check their Facebook pages and to utilize a

hundred other mind-boggling mobile applications. Many of these "Millennials" have begun to insist on using their personal devices at work, so they can keep all of their contacts, email messages, spreadsheets, data and other work-related information

More on Page 29

Increasingly complex narco-tunnels challenge U.S. Border Patrol

By MARK ROCKWELL

A string of recently discovered, highly-developed drug-smuggling tunnels, equipped with electricity, engineered structural support and air-moving systems, has U.S. Border Patrol agents stepping up detection efforts and concerns among U.S. citizens in California and Arizona border towns.

Border agents from federal task forces comprised of local law enforcement, U.S. Border Patrol, Immigration and Customs Enforcement (ICE)

GSN 2011 awards dinner salutes best, brightest and bravest

By ADRIAN COURTENAY

The annual awards dinner hosted by *Government Security News* has traditionally saluted "the best and the brightest" in the homeland security field, and this year was no exception, as 45 awards were presented on Nov. 14 to leading vendors of IT and physical security products for their cutting-edge technologies, and to federal, state and local government agencies for their successful programs, projects and initiatives.

But this year, GSN also focused on "the bravest," as the U.S. Border Patrol's Detroit Sector was honored for a series of arrests on the St. Clair River made under its Remote Video Surveillance Program, as coordinated with the headquarters of the Secure Border Initiative in Washington, DC; and the Bastrop County, TX, Unified Command, a team of elite fire-

fighters from county, state and federal agencies was honored for its teamwork and selfless cooperation in bringing the worst wildfires in the history of Texas under control, following the loss of several lives and about 1,500 homes in the county.

In a related new development

More on Page 15

Definition and motives of 'homegrown' terrorists more fluid than ever

Despite efforts to put a finger on what drives "homegrown" terrorists, the task is almost impossible to do, say experts, as motives among them are as varied as individual human personalities.

Some of those examining terrorists' psychological drives said homegrown, self-radicalized terrorists have a lot more in common with comparatively run-of-the-mill, mentally unstable murderers and assassins than with principle-driven ideologues bent on a cause. The psychological lines that might divide a "Lone Wolf" terrorist who bombs an army base and a lone assassin targeting the President are blurry, according to Dr. Randy Borum, a board-certified forensic psychologist and professor in the College of Behavioral and

More on Page 37



U.S. Army Major Nidal Hasan



FLIR
Extraordinary Protection

INTRODUCING
IDENTIFINDER 2

See our ad on page 7

Centrify takes Best Identity Management Platform award

Centrify's *Suite 2012* security and compliance solution that allows central control of access to an organization's information systems took home *Government Security News'* award for best identity management platform.

Centrify's *Suite 2011* allows federal, defense, intelligence and civilian agencies to centrally control, secure and audit access to cross-platform systems and applications by leveraging an infrastructure they already own -- Microsoft Active Directory.

"It is a tremendous honor to be named the government industry's Best Identity Management Platform by *Government Security News*, an important source of news and information in all aspects of homeland security," said Frank Cabri, Centrify VP of Marketing. "Centrify's focus on the Federal government sector helps government agencies address compliance and access controls across users and systems. Government agencies continue to consolidate data centers, improve security and embrace cloud infrastructure, and we are pleased to be partnering with them in delivering the identity consolidation and privilege management solutions that are critical to addressing their needs."

Centrify's FIPS-validated solution has broad acceptance throughout federal, defense and civilian agencies for its reliable identity consolidation and privileged access management solutions, said the company.

The Centrify Suite allows these organizations to centrally control, secure and audit access to cross-platform systems and applications by leveraging Microsoft Active Directory infrastructure. Built on an integrated architecture, the Centrify Suite strengthens security, enhances regulatory compliance initiatives, and reduces IT expense and complexity, it said.

The Centrify Suite — consisting of DirectControl, DirectAuthorize, DirectAudit, DirectSecure and DirectManage — delivers secure authentication and single sign-on, role-based authorization, privilege management, user-level auditing, trust-based protection of sensitive systems, and encryption of data in motion for the industry's broadest set of cross-platform systems and applications.



Jacob Goodwin presents award to Greg Cranley of Centrify, for Best Identity Management Solution

Centrify Suite has been awarded the Federal Information Processing Standards (FIPS) 140-2 Level 1 validation, assuring government customers, defense contractors, systems integrators and resellers that Centrify products provide the highest level of protection for sensitive information, and comply with strict government security regulations. ■

Long-term vision earns Port of Long Beach a winner's trophy in 2011 GSN awards program

Back in 2007, when he first became security director of the Port of Long Beach, CA, Cosmo Perrone had a vision of a port security management model controlled by a single security platform on which all the subsystems spoke the same language and all were operated in the same control center.

He felt confident that this vision could be turned into a reality because he had seen the concept work in the aviation field during in his previous career working for McDonnell Douglas and Boeing. He believed that he could create a dynamic port model that could become a template for many other ports.

But when he approached the Department of Homeland Security to request funds for the project, Perrone was told that the system he had in mind was too speculative and had not been sufficiently proven elsewhere to risk a large amount of money.

GSN had a chance to sit down and chat with Perrone at the GSN 2011 awards dinner

in Washington, DC, on Nov. 14 about these rather inauspicious beginnings to the two-phase security integration plan which was recently completed, and which has earned the 2011 winner's trophy for the Port of Long Beach as "Most Notable Program, Project or Initiative in Maritime/Port Security" in 2011.

In the year or two that followed his disappointing initial response from DHS, Perrone told *GSN*, the port's board and executive management were very supportive, enabling him to do some advocacy work for the plan both in Washington and before the Maritime Security Council of California. With the assistance of the executive director of the port, a retired Coast Guard admiral who accompanied him to Washington, Perrone was gradually able to turn around the perception at the DHS.

His efforts in California also met with success when the state's citizens approved a \$100 million bond to upgrade the state's ports -- and a portion of this money was earmarked for the Port of Long Beach.

With the necessary funds secured, Perrone



Members of the Centrify Federal Sales Team (Right to left - Steve Barry, Dan Jamison, Greg Cranley) celebrate GSN's award of Best Identity Management Solution for Centrify Suite

proceeded to select Sunnyvale, CA-based Proximex and its *Surveillint* software command and control center solution to implement his strategy. With the *Surveillint* platform, every new and existing security system is now connected through the secure, high speed fiber optic network to the software located in the command center. Orion Network Monitoring Software tools provide real-time data regarding the health of all security systems. Any device that fails to perform is automatically detected and operators are alerted for investigation.

To secure the port at below-water level, sonar technologies were remotely located at crucial underwater locations. The

Kongsberg Sonar Solution provides military grade sonar detection and analytics to enhance underwater surveillance and provide visibility while meeting the State of California's strict environmental regulations for sea mammals.

More systems were installed or expanded to enhance port security at water level. The SSR/Radar Ves-



Leaders of Port of Long Beach, CA, and supporting contractors were hailed for port's new consolidated security platform

sel Acquisition System was added to the port's radar system to give better visibility and definition within the port's security area, and, because it is a public port, track personal and watercraft.

A Blue Force tracking solution provides real-time domain awareness of all port security assets below, at or above water, so operators can map assets in real-time, then confirm availability with personnel and dispatch instructions as necessary. Information is automatically included in incident reports for upper management.

The port also enhanced its above-water level security. Avigilon 16-megapixel cameras were added for critical infrastructure security. These cameras deliver multiple smaller views from one larger camera and offer a 360-degree view for better video coverage with fewer cameras. More than 100 CCTV cameras owned and operated by port tenants were integrated to expand the port-wide video surveillance system and leverage existing assets.

A new visitor management system lets visitors obtain their own badges and receive approval before entering the secured area. ITrack, a new CAD system, was installed to manage port security assets and respond to incidents.

The port-owned AM radio station is now integrated with *Surveillint*, so operators at the command center can deliver important messages to the whole community. The AM radio station is now connected to the port's new mass notification system to notify and instruct everyone within its 18-square-mile radius of important events, such as warning of a tsunami. This system will be integrated with *Surveillint* within the next six months.

True to Perrone's original vision, almost all subsystems are integrated onto the same Proximex *Surveillint* software platform, and they're all talking the same language.

New identification kiosk will also look for trace explosives on documents

The next time you present your passport, driver's license or credit card to a user-friendly kiosk installed in some public place by DHS – in an effort to authenticate your identity -- be advised that DHS might also be examining the document to see if it contains any traces of dangerous explosives.

The Science & Technology Directorate of DHS has just released a broad agency announcement in search of one or more companies that can work cooperatively to design a kiosk the size of a convenience store ATM that has two missions – screening documents to validate a person's identity against a pre-programmed list of names, and detecting trace explosives, such as TNT, RDX, PETN or other explosive materials.



"Kiosk appearance will be such that it is not apparent that trace analysis is being conducted," says S&T's broad agency announcement, which was made public on Nov. 2.

"Kiosk should be welcoming to the person checking in, and instruct the person to insert their government issued identification through both text and graphics/video displayed on the touch screen," says the announcement.

The proposed kiosk would have the ability to perform a "trace chemical analysis of the documents for explosive analytes of interest," which might include commercial military or homemade explosives.

The weight of the new kiosk should

not exceed 150 pounds, and ideally weigh less than 75 pounds, says S&T. It should be able to "reliably detect and identify trace levels of explosives upon the surface of the credentials," it adds.

The new kiosk should also be fast. "The sampling of the document for explosives will take place at some point during the document scanning procedure that is used for authentication," explains DHS, "and it will not add substantially to the amount of time required to perform authentication, so as to provide a smooth user interface." The explosive trace detection and the authentication procedure should both be completed in less than 15 seconds per document, says the directorate.

In case the new kiosk detects some worrisome explosives, it will try not to tip off the person who presented the document. In fact, it will seek that person's further cooperation. "In the event of a trace alarm or credential alert, the person being screened should be notified innocuously that there was a problem with check-in, that an officer has been notified, and directed to the security officer's station to wait for assistance," says the announcement.

DHS expects that the design and development of such a new kiosk will take about 12 months, and that the delivery of two prototypes to the DHS Transportation Security Laboratory, and their testing, will consume another six months.

FBI's Washington area buildings need security boost, says GAO

The security of the FBI's headquarters building in Washington DC, as well as the dozens of annex buildings in the surrounding area, are inadequate and alternatives have to be determined soon, said a study by the Government Accountability Office (GAO).

The GAO was directed to examine the agency's headquarters facilities' security, space and building conditions in 2009. In its examination, the GAO interviewed FBI officials, as well as personnel at the buildings' property steward agency, the Government Services Administration (GSA), about the continued suitability of the facilities. The government watchdog agency said it found that since the Sept. 11 attacks in 2001, the FBI had outgrown its Hoover Building headquarters building in downtown Washington and many of the over 40 annex buildings in the region.

"The FBI's headquarters facilities -- the Hoover Building and the headquarters annexes -- do not fully support the FBI's

long-term security, space, and building condition requirements," said the report.

"FBI security officials told us on our site visits that they have some security concerns -- to varying degrees -- about some of the headquarters annexes," it said. Those officials, according to the GAO, said the concerns included the proximity of FBI agents performing sensitive operations to non-FBI tenants, lack of control over common areas and that security at the agency's many annexes is handled by an uneven mix of contract guards, local police, the FBI's internal police force, depending on a given facility's location and circumstance.

The GAO said the agency's workforce, widely distributed across the D.C. region housed in aging and inefficient facilities,

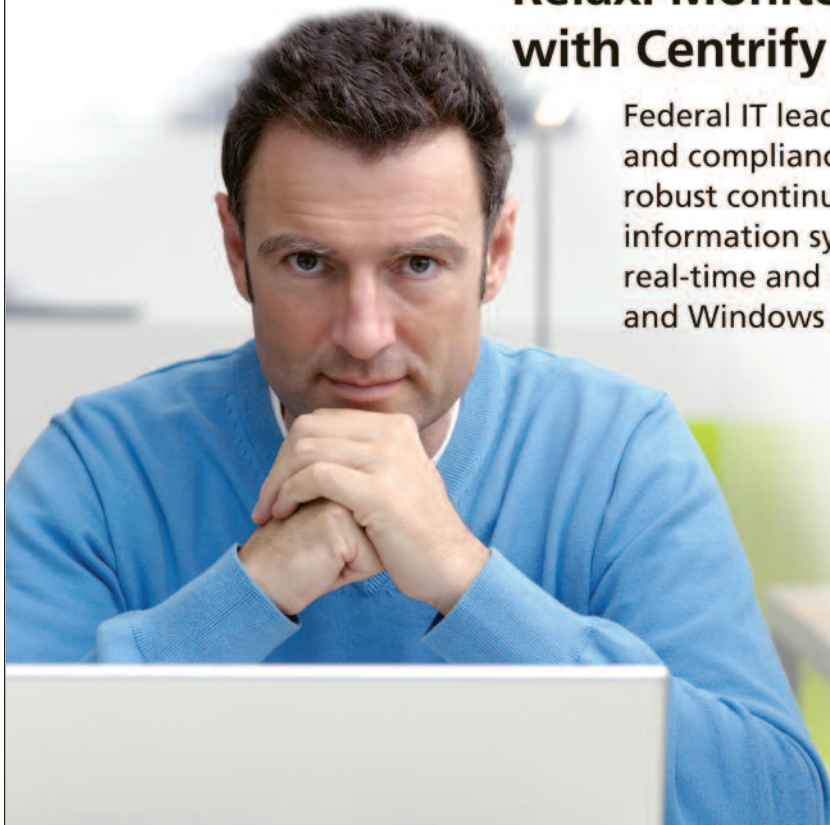
requires an alternative. The FBI, said GAO, is "under pressure to find an alternative that will meet its security, space and building condition requirements." GAO added that given the size and scope of the alternative the FBI is looking for, that search could take years and cost over a billion dollars.

In the meantime, the GAO said the FBI should keep a close tab on its search requirements and base its decisions on "up-to-date assessments" of its security, space and building condition needs." While the FBI searches, the GAO said GSA should take a closer look at how it will spend money to maintain the Hoover Building, since the FBI is likely to be there for "several more years, while its long-term facility needs are being planned." ■



FBI headquarters in Washington, DC

Stressed out about Compliance deadlines? Relax. Monitor systems continuously with Centrifly DirectAudit.



Federal IT leaders know that security best practice and compliance guidance like FISMA require a robust continuous monitoring strategy for information systems. Centrifly DirectAudit makes real-time and ongoing visibility of UNIX, Linux and Windows systems easy.



Centrifly DirectAudit is part of Centrifly Suite, winner of Government Security News Homeland Security Award for Best Identity Management Solution.

Get started now at www.centrifly.com/getda