

GSN's Public Security & Safety Profiles

Diebold, Incorporated

Diebold is a leading provider of security and business optimization solutions for your environment - no matter how unique. And, with thousands of Diebold service professionals worldwide, you'll have service support when and where you need it.

Serving the U.S. federal government - as well as state and local agencies and the transportation, critical infrastructure and utility industries - Diebold delivers:

- System design, installation and integration
- Project management
- Facility planning and analysis
- Identity and access management systems
- Logical security solutions
- Intrusion detection systems
- IAS systems
- SCOP implementation and monitoring
- Displacement sensors
- IT break/fix services
- Partnerships with key security vendors
- 24/7 service

GSN's 3rd Annual Public Security & Safety Profiles

Begin on page 12

GSN • Government Security News

Government Technology & Services Coalition's premier newsletter

Page 40

GTSCConnection

Why Small and Mid-Size Quality Innovators and Value

Virtual World Meets Cyber Security Awareness

Future Thought

What do YOU think about the future of IS&C?

PUBLIC SAFETY

Contractors help Park Police secure DC for recent July 4th celebrations

How do you keep track of security for a million spectators, along with dozens of local and federal government agencies, all gathered for a massive display of celebratory mortar fire in the nation's capital? PAGE 4

LAW ENFORCEMENT

New administration strategy aims at big transnational crime groups

The White House embarked on a new strategy the week of July 24 to combat vicious and well-funded criminal organizations that operate across sovereign international borders. PAGE 7

ACCESS CONTROL

Managing visitor access into federal facilities

Lobbies are hectic environments, especially for federal agencies faced with a constant flow of visitors. There's a strong need to quickly process and manage visitor access into federal facilities, while ensuring that all security procedures and policies are followed. PAGE 9

BIOMETRICS

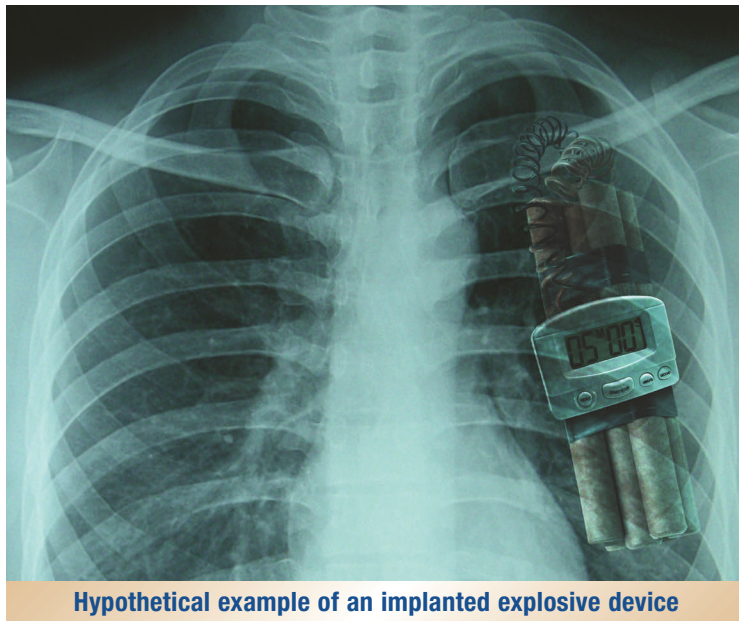
3D 'facial reconstruction' software makes recognition engines more effective

Facial recognition systems have not yet lived up to their potential for security-related applications, say two of the founders of CyberExtruder, an innovative small business based in Newark, NJ. PAGE 27

IT SECURITY

In cloud security, one size does not fit all

Few factors play as decisive a role in federal cloud computing deployments as security. From planning through implementation, federal agencies need to consider how to protect the sensitive data that is central to their missions. PAGE 31



Hypothetical example of an implanted explosive device

Experts worried that implanted explosives could be possible

By MARK ROCKWELL

Suicide attackers boarding airplanes with surgically-implanted bombs sounds like the stuff of overheated spy novels, but medical, explosives and detection experts interviewed by *Government Security News* say the recent concerns about such devices aren't all that far-fetched and are probably warranted.

Medically-speaking, a second-year medical student is very

capable of implanting a device with minimal surgical assistance, other than a simple operating room, basic medical supplies and possibly an anesthesiologist, according to Elliott Haut, associate professor of surgery, anesthesiology and critical care at Johns Hopkins Medical Center in Baltimore. An explosive device, if implanted in the right place on the human body, could be devastating if it explodes in a critical spot in an aircraft, said James Crippin, director of the Western Forensic Law Enforcement Training Center (WFLETC) in Pueblo, CO. WFLETC trains local, state and federal law enforcement and the military in explosives forensics.

However, both experts said

Joint Munitions Command completes secure transport and storage of hazardous mercury

By LINDA LOEBACH

10-7-40. Those three digits are not a locker combination, but three important numbers related to the recent move of the National Defense Stockpile's elemental mercury from three disparate locations to Hawthorne Army Depot, Hawthorne, NV, an installation of the Joint

Munitions Command. Ten years ago, the Defense Logistics Agency began seeking a site to store the mercury long-term. Over the course of seven months, semi-trucks transported the mercury to Hawthorne where it will be stored for 40 years or longer.

According to DLA, elemental

mercury is one of three types of mercury that occur naturally in the environment. Also referred to as quicksilver, it is dense, silver-colored and liquid at room temperature. More on Page 36

Rash of cyber attacks on national labs suggest deeper problems

By JOHN P. MELLO JR.

A series of attacks on some of the nation's top government labs in recent months could be a sign that a concerted effort is under way to compromise the network that binds together the U.S. Department of Energy's research infrastructure.

In recent months, cyber attacks have been reported at Oak Ridge National Laboratory in Tennessee, the Pacific Northwest National Laboratory (PNNL) in the State of

Washington and the Y12 National Security Complex, also in Tennessee.

Those attacks have one security strategist wondering if the forays might just be signs of a larger problem within the Energy Sciences Network, or ESnet, which provides high-speed, high-resiliency links to the Department of Energy's (DOE) labs, such as Oak Ridge and PNNL.

"What if ESnet was to get More on Page 35

Coalition general, Comitini, describes program to train Afghan police

By JACOB GOODWIN

When President Obama addressed the nation from the White House on June 22 to talk about the withdrawal of U.S. forces from Afghanistan, he tied the speed of that promised withdrawal, in part, to the success that the U.S. military and its coalition partners can achieve in training "Afghan security forces" to assume responsibility for security in their own country.

Obama promised a reduction of 10,000 U.S. soldiers by the end of 2011, and the with-



Instructing police recruits in riot control at training center in Afghanistan

drawal of a total of 33,000 troops by the summer of 2012.

"After this initial reduction, our troops will continue coming home at a steady pace as Afghan Security forces move into the lead," the president More on Page 37



Anticipate the unexpected



See our ad on page 2

Maintaining security as you enter the cloud



By Rich Thompson

Is cloud computing hype or reality?

The overall benefits and cost savings are a clear sign that cloud computing in various forms is here to stay. For federal agencies, perceived and real security impediments of moving data to the cloud exist. However, acceptable levels of risk are achievable right now for most implementations being considered by government and commercial sectors.

Recently, the U.S. General Services Administration (GSA) established a Blanket Purchase Agreement (BPA) for federal agencies to use in the procurement of cloud computing, along with a shortlist of authorized providers that are currently in the final stages of assessment by GSA.

The Federal Risk and Authorization Management Program (FedRAMP), is essentially like a Certification and Accreditation (C&A) package with an Authority-To-Operate (ATO) in line with implementation guidelines specifically for cloud environments in the government sector. Although it does not relieve agencies of their regulatory responsibilities, it provides an acceptable level of assurance that these providers have at least completed a process and achieved successful results that are both repeatable and auditable.

With the task of migrating your agency's system -- or perhaps entire port-

folio -- into a cloud, how do you maintain an appropriate security posture? There are a number of ways to discuss security during the transition, but here are a few key high-level considerations for agencies entering the new territory.

1. Create a plan of action and cover all of your bases. Make sure the intended cloud implementation will meet all of your requirements, security and otherwise.

2. Stay Informed. Keep abreast of the great cloud security work that is ongoing and pro-actively seek out information on recent mandates or requirements. Also, keep an eye out for best practices that you can potentially incorporate into your plan of action. Follow news from focus groups, like The National Institute of Science and Cloud Security Alliance, which continue to make significant contributions to cloud computing and security.

3. Select knowledgeable and qualified providers. Make sure that your selected providers (i.e. vendors, systems integrators, partners, etc.) have an appropriate level of security domain knowledge, experience, and certifications (i.e. DoD 8570.1M) to meet or exceed your requirements throughout the entire lifecycle. In addition to more traditional security domains of knowledge, qualified providers should be aware of additional requirements, such as the Federal CIO Council -- Information Security and Identity Management Committee's Guidelines for the Secure Use of Cloud Computing

by Federal Departments and Agencies.

4. Consider long-term agency requirements. Strive to plan and implement a security posture that is actually more stringent, or capable of being more stringent, than currently required, in order to accommodate future requirements that may be on the horizon (i.e. FISMA 2.0 -- "continuous monitoring"). Take steps to make sure that your "to-be" implementation has that extensibility, where possible. Cloud providers being considered should have reasonable and demonstrable familiarity and experience with agency-specific requirement sets.

5. Avoid "one-size-fits-all" provider services. When you consider the broader portfolio of systems that agencies are looking to place into a cloud, more than one type is often necessary to accommodate all of the operational and security requirements. Beyond the sensationalistic hype and the myriad of different views about the current state of cloud security, the fact remains that public (provider-owned and managed) and private (customer-owned and managed) implementations of clouds -- consisting of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) -- can meet regulatory requirements, if they are architected and implemented to do so. Realistically, however, multiple types of clouds in conjunction with more traditional co-location scenarios may be necessary when more stringent requirements come into play.

6. Clearly define in-house and partner roles and responsibilities. Consider that with "as-a-Service" cloud

types, responsibilities change and move up a notionally layered "stack." The implication being that management responsibility shifts to:

a. With IaaS, the provider is responsible for managing everything up to the server;

b. With PaaS, the provider is responsible up through the platform; and

c. With SaaS, the provider is responsible up through the software (or application).

Depending on the need, it is quite possible that there could be a requirement for a combination of the three, plus a determination of what will be in a public or private cloud. Possibly, a decision as to which will require some combination of all-of-the-above or a more traditional co-location approach (i.e. to meet more stringent requirements).

Remember that in most government cloud implementations, the government customer will still have the overall responsibility for ensuring that the system deployed to a cloud meets all security and regulatory requirements, and for reporting on the state of that compliance periodically.

Early adopters of cloud computing have taken advantage of cloud computing's overall nimbleness of deployments and key benefits. By keeping your head in the cloud, you'll help lead your agency into the next generation of government efficiency and overall cost savings. ■

Rich Thompson, CISSP ITIL, is Cybersecurity Practice Lead for Carpathia Hosting. He can be reached at: rthompson@carpathia.com

Security can make a cloud smarter

The list of benefits cloud computing can bestow on an organization is a long one, but for many IT professionals it can't override their qualms about security in the nimbus. Those fears can be allayed, though, with something called a "smart cloud."

"A smart cloud can be any IT-enabled capability that is delivered via the Internet as a service," Satwant Kaur, a management consultant and author, told *Government Security News*. They also have all the benefits usually associated with the cloud, she added, such as the ability to:

- Dynamically right-size and increase agility;
- Give businesses ways to connect to customers and other businesses;
- Break down boundaries to IT systems and processes, and simplify access to information needed to achieve business results;
- Support community-driven innovation, within and outside the boundaries of a business;

• Ensure interoperability, resiliency, security and development of new services with the consistent user experiences through a standard cloud infrastructure; and

• Easily migrate, design, build and deploy around enterprise business models.

What makes smart clouds "smart," however, is that they can use their smartness to make themselves more secure, maintained Kaur, a former platform architect at Intel and a strategist for the chief technology officers of EMC Corp., of Hopkinton, MA, and TIBCO software, of Palo Alto, CA.

She explained that smart clouds provide security through threat protection, privacy, compliance and protection of data and intellectual property. She cited HP Cloud Assure as an example of the kind of solution that makes smart clouds secure.

"It offers an end-to-end solution for performing security risk assessments to detect and correct security vulnerabili-

ties," Kaur explained, "and it provides common security policy definitions, automated security tests, centralized permissions control and Web access to security information."

In addition, it can scan networks, operating systems, middleware layers and Web applications, as well as perform automated penetration testing to identify potential vulnerabilities -- giving an organization an accurate security-risk picture of its cloud services.

She also noted that smart clouds make themselves more secure through policy-based automation and management. A product such as IBM's *Tivoli Live* can monitor and manage the performance of IT infrastructure, as well as IT incidents and problems, she observed, and HP Enterprise Security Management can intelligently identify and mitigate cyber threats and risks through complete visibility and insight into IT infrastructure and application events.

Security governance, risk management and compliance are all hallmarks of the smart cloud, Kaur said. HP Enterprise Cloud Services, for instance, includes

robust vulnerability scanning features that can proactively find and fix security threats. It can validate the effectiveness of current security safeguards for network devices and resources, as well as quantify the risk to internal systems and confidential information.

The HP offering can proactively address security issues before they are exploited, she added, and support compliance with industry and government regulations, especially those elements requiring regular scans.

She noted that it has a Web application scanning service, too, that looks for vulnerabilities like cross-site scripting and SQL injections -- two common types of flaws exploited by Internet vandals and hackers.

"The mainframe and PC world is behind us," Kaur declared. "The virtual enterprise enabled by the smart cloud offers a perfect mix of solutions -- unified communications, thin client computing and desktop virtualization -- for transitioning from the traditional static computing model to the dynamic cloud environment." ■