

November 1 ,
2007

ASDWire

*'If your news
needs to reach
the world'*

Deliver your
news to
5000+
important
Aerospace
and Defence
Media around
the world.



Articles

- Security Alert: Do Not Open "FTC" Email
- Fortify Software Sets the Industry Standard for Secure Code Development
- Announcing Fortify SCA 5.0: Application Security Without Borders
- Phase One Awarded GSA USA.gov Support
- Phase One Receives Service Oriented Architecture Award
- U.S. Air Force Bolsters Itself for Cyber War
- With BlackBerry in Crosshairs, Microsoft Debuts Mobile Server
- IG: DHS Falls Short on Security
- Tighter Security Over Power Plant Computer Systems Urged
- IG: DHS Has Yet to Properly Secure Networks
- Changes to Air Force IT Contract Could Benefit New Vendors
- City of Bowling Green Uses Mobile Wireless Technology for Public Safety
- IT Standards Cited as Key to Meeting Intelligence Sharing Goals
- Industry Embraces Health IT Bill
- Law Firm Fears Government is Tapping Phones
- Fed IT Security Spending Set to Soar
- IT Security Group Honors Three Feds
- Port Security Card System Will Work, Officials Tell Senators
- Former Homeland Security Secretary Ridge Launches Security Consultancy
- GAO: Departments Lag on FISMA Controls
- DHS Under More Scrutiny After Attacks
- Gap Contractor Loses Laptop With Personal Job Information
- Survey Finds Gap Between Perceived and Actual IT Security
- DISA Setting Up New Network Monitoring Center
- Private-sector Info-sharing Network in Works
- Cyber Security Chiefs Keep a Low Profile
- VA: IT, Security Progress to Accelerate in 2008
- Privacy, IT Officers Come Together to Create Policy
- Avaya Honors Verizon Business as 2007 Alliance Partner of the Year
- Microsoft-backed Enterprise Mobile Launches
- eBay: Phishers Getting Better Organized, Using Linux
- Small Business Administration Awards \$30M Contract to SRA
- Stanley Announces Additional \$17 Million Prime Contract Award
- DHS Awards \$74.1M Professional Support Contract
- USDA First to Award SmartBuy Encryption Contract

Announcements

Security Alert: Do Not Open "FTC" Email

Don't Open Bogus Email that Claims to Come From the FTC
Email That States It's From the FTC's 'Fraud Department' Has Virus Attached

A bogus email is circulating that says it is from the Federal Trade Commission, referencing a 'complaint' filed with the FTC against the e-mail's recipient. The email includes links and an attachment that download a virus. As with any suspicious email, the FTC warns recipients not to click on links within the email and not to open any attachments.

The spoof email includes a phony sender's address, making it appear the email is from '**frauddep@ftc.gov**' and also spoofs the return-path and reply-to fields to hide the e-mail's true origin. While the email includes the FTC seal, it has grammatical errors, misspellings, and incorrect syntax. Recipients should forward the email to **spam@uce.gov** and then delete it. Emails sent to that address are kept in the FTC's spam database to assist with investigations.

Simply opening the email does not appear to cause harm. However, it is likely that anyone who has opened the e-mail's attachment or clicked on the links has downloaded the virus on their computer, and should run an anti-virus program. The virus appears to install a 'key logger' that could potentially grab passwords and account numbers. More information about bogus emails, phishing, and virus protection is available at www.OnGuardOnline.gov.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to more than 1,600 civil and criminal law enforcement agencies in the U.S. and abroad. For free information on a variety of consumer topics, click <http://ftc.gov/bcp/consumer.shtm>.

Fortify Software Sets the Industry Standard for Secure Code Development with Introduction of Fortify SCA 5.0

Application security leader delivers a customizable, collaborative and comprehensive solution based on feedback from the world's largest software developers.

PALO ALTO, Calif., October 22, 2007 - Fortify® Software Inc., the market-leading provider of enterprise application security solutions, today introduced Fortify SCA 5.0, the fifth generation of its award-winning source code analysis software. Fortify SCA is the industry's most powerful static analysis solution, designed to enable enterprises to eliminate security vulnerabilities in the applications they develop. Fortify's latest version, Fortify SCA 5.0, incorporates new capabilities that set a new industry standard for application security including several industry firsts:

- Wizard-driven creation of customized security rules by those who aren't software developers
- Enablement of global collaboration between software development teams
- Protection against new classes of vulnerabilities specific to application security
- Support for programming languages, including PHP, JavaScript (Ajax), Classic ASP/VB Script (VB 6) and a limited release of COBOL

According to Gartner, "Enterprises must adopt source code scanning technologies and processes, because the need is strategic." (Market Definition and Vendor Selection Criteria for Source Code Security Testing Tools, May 2007, Neil MacDonald and Joseph Feiman). As application security establishes itself as a 'must have' for organizations developing their own applications, a secure development process must be more closely integrated into their day-to-day activities. Fortify, already the market leader in application security, has incorporated



Make your
hiring
decision
easier.

Find out
how.



Information Resources
Management College
National Defense University

"Educating
CIO, IA, and
eGov
Leaders"



www.ndu.edu/irmc

feedback from its worldwide customer base to bring collaboration, customization and more comprehensive protection to the enterprise secure development lifecycle.

"The breadth and depth of our customer base gives us unique insight into the largest application security deployments in the world, as well as detailed knowledge of how organizations are using this technology," said John M. Jack, Fortify's CEO. "These businesses are faced with constant security threats and customers who evaluate their products and services based on the level of security they assure. As a result, they have spent a lot of time evaluating their secure development practices and have very specific requirements for any solution they may deploy. With the release of Fortify SCA 5.0, we have implemented feedback from these market leaders to deliver the first solution meeting these requirements and the most effective application security solution in the industry."

Announcing Fortify SCA 5.0: Application Security Without Borders



Join our informative webinar to learn why Fortify SCA is the standard solution protecting applications for the largest and most demanding companies globally. Be the first to view in detail what's new in this latest product release. Also click here for more information: <http://www.fortifysoftware.com/landing/scawebinar1.jsp>

Phase One Awarded GSA USA.gov Support

Phase One Consulting Group is proud to announce that it has been awarded a blanket purchase agreement (BPA) with the U.S. General Services Administration (GSA) to support the Office of Citizen Services and Communications (OCSC), USA.gov Technologies Division. The BPA period of performance will be a 12-month base year with four (4) option-year periods.

Phase One Receives Service Oriented Architecture Award

Phase One Consulting Group is proud to announce that they have received an award on behalf of the National Park Service for developing the Best Agency Service Oriented Architecture (SOA) Application at the 4th Annual SOA for E-Government Conference, held in McLean, VA on October 1-2, 2007.

U.S. Air Force Bolsters Itself for Cyber War by Selecting Fortify's Application Security Suite for Worldwide Development Teams

Palo Alto, California – October 1, 2007

Fortify® Software Inc., the market-leading provider of enterprise application security solutions, today announced that its suite of products—covering both static analysis and runtime approaches—has been selected by the U.S. Air Force as part of a comprehensive \$10.2 million security protection plan to protect its applications from malicious hackers.



The U.S. Air Force—a leader in the Department of Defense's strategy for cyber security—will use Fortify's complete product portfolio to develop secure code, as well as identify, protect and monitor these applications from attacks, including SQL injection, cross-site scripting, buffer overflows, and a full range of additional malicious activities.

[Back to top](#)

Industry News

With BlackBerry in Crosshairs, Microsoft Debuts Mobile Server

Taking direct aim at BlackBerry's commanding lead in the enterprise smartphone business, Microsoft (NSDQ: MSFT) will announce its first server-based tool for managing and securing Windows Mobile devices today. The debut will occur during CEO Steve Ballmer's keynote address this morning at the CTIA wireless conference in San Francisco. Called System Center Mobile Device Manager, the new product is Microsoft's first dedicated mobile device server, bringing it into direct competition with the BlackBerry Enterprise Server from Research in Motion.

IG: DHS falls short on security

Despite improvements, the Homeland Security Department still falls short in protecting its critical IT systems and data, according to a new report from the department's Inspector General Richard L. Skinner.

Tighter security over power plant computer systems urged

Current regulations to protect the control systems that support power plants nationwide fall short of federal recommendations, posing a serious threat to the electric infrastructure and national security, witnesses testified at a hearing Wednesday. One lawmaker threatened legislation if standards don't improve.

IG: DHS has yet to properly secure networks

The Homeland Security Department, chastised by Congress and security experts for having some of the worst information security practices in government, has improved its security plan and policies but now must begin deploying its plan, according to a report recently released by the department's inspector general.

Enterprise Architects Driving Government SOA

[Click Here For Case Study](#)



Changes to Air Force IT contract could benefit new vendors

Proposed changes to the Air Force's marquee contract vehicle could prove to be a financial boon for a handful of product and solutions providers, according to a pair of industry reports. The Air Force plans to split the second version of its \$9-billion Network Centric Solutions contract into three parts: services, products and services-small businesses. The original NETCENTS contract, awarded to eight prime contractors in 2004, wrapped all three pieces into one.

City of Bowling Green Uses Mobile Wireless Technology for Public Safety

The Cisco Mobile Government solution encompasses a set of products and partners that enable more efficient and effective decision-making for public safety and mobile workers, through the use of collaborative wireless mobility technologies. The city of Bowling Green, Kentucky, is capitalizing on the benefits of wireless and mobile technologies at a time when their value and investment are growing within public sector circles, due to increasing citizen



demands.

IT standards cited as key to meeting intelligence sharing goals

Information technology standards are needed to help intelligence agencies meet the objectives of a new plan to enhance collaboration and information sharing, according to a federal executive and an analyst. The 500 Day Plan for Integration and Collaboration, released by the Office of the Director of National Intelligence last week, will require intelligence agencies to develop standardized systems that enable collaboration and information sharing and modernize business practices.

Industry embraces health IT bill

A new health information technology bill has quickly won support from the IT industry. The measure, which aims to accelerate the adoption of e-health records that can be seen across systems, was one of several technology-related bills introduced this week in the House.

The legislation, H.R. 3800, would establish a national coordinator within the Health and Human Services Department and create a public-private advisory body to ensure interoperability standards in health IT.



[PC on a Stick: A Portable Endpoint Security Nightmare](#)

[Click here for this whitepaper and to find out how Sanctuary® is your best, first line of defense against data leakage and malware.](#)

Law firm fears government is tapping phones

A law firm that represents clients at Guantanamo Bay, Cuba, and in Afghanistan is warning its Vermont clients that it believes the federal government has been monitoring its phones and computer system. In a letter sent to clients of the St. Johnsbury firm of Gensburg, Atwell & Broderick, the three attorneys said they can't guarantee their communications were confidential.

Fed IT security spending set to soar

Federal government spending on IT security is expected to rise sharply over the next five years, according to forecasts recently released by both government and private sector analysts. The Office of Management and Budget, the executive department which oversees federal spending, now forecasts FY 2008 IT spending at \$66.4 billion. Security spending within government IT budgets will total \$5.4 billion.

IT security group honors three feds

Three federal officials were recognized for their contributions to government information technology security by (ISC)² at its fourth annual Government Information Security Leadership Awards given Oct. 3. There were three categories of awards: senior IT security manager, senior non-IT security manager and non-managerial IT security professional.



Port security card system will work, officials tell senators

Homeland Security Department officials on Thursday attempted to assure lawmakers they are ready to begin a massive program to issue port workers security cards, despite years of delays and concerns that individuals might be mistakenly denied the credentials.

Members of the Senate Commerce Committee peppered Homeland Security officials with questions during a hearing about how they will handle vetting up to a million port workers for the so-called transportation worker identification credentials. They also asked whether the department is ready to correct mistakes that could cost innocent workers their livelihoods.

Former Homeland Security Secretary Ridge launches security consultancy

Former U.S. Secretary of Homeland Security Tom Ridge has formed his own private security consulting firm. The company, Ridge Global LLC, will offer a variety of consulting services, including what it calls "strategic business generation, global trade security, risk assessment and

contingency planning, crisis management and communications, leadership guidance and change management, special event security and technology innovation and integration," according to a news release.

GAO: Departments lag on FISMA controls

Some of the agencies most critically involved with the country's security still have not fully implemented key provisions of the Federal Information Security Management Act five years after the act was passed. The Defense, Homeland Security, Justice and State departments especially face challenges in establishing information security control activities that FISMA and the Office of Management and Budget require, the Government Accountability Office said.

DHS under more scrutiny after attacks

The Homeland Security Department's networks are vulnerable to cyber-attacks, and several lawmakers said last week that sends a poor message and highlights the challenges agencies face in securing networks that contractors manage.

Gap contractor loses laptop with personal information of 800,000 job applicants

Clothing retailer Gap revealed on Friday that a laptop containing the personal information of approximately 800,000 of its job applicants was stolen from a third-party contractor that manages the company's data.

Included in the information were applicants' Social Security numbers, according to Gap. The stolen laptop contained personal information for those who applied for jobs with the company's Old Navy, Banana Republic, Gap and Outlet stores in the United States, Puerto Rico and Canada between July 2006 and June 2007, the company said.

Survey finds gap between perceived and actual IT security

A survey released Monday to mark cyber-security awareness month in October shows that consumers are aware of security risks online, but there is a big gap in what they have done versus what they think they have done to protect themselves.

DISA setting up new network monitoring center

Defense Information Systems Agency officials will soon kick off an experimental program that could help defense officials pinpoint service outages and security breaches across the military's networks.

The pilot effort, slated to begin next month, is a step toward setting up an Information Sharing Operations Center early next year, according to Anthony Montemarano, DISA's program executive officer for information assurance and NetOps.

Private-sector info-sharing network in works

A group led by former Homeland Security Department Undersecretary Asa Hutchinson that aims to organize private-sector crisis response has set up a new network to share information during disaster rescue and recovery.

Cyber security chiefs keep a low profile

It's a job with little authority and no budget of its own. Few people are aware of the post, or its role in safeguarding millions of Americans' personal information and ensuring the continuity of government. Not every federal agency even has one. When chief information security officers do get attention, it's usually because someone lost or swiped a laptop. In a government populated with countless thankless jobs, the challenges facing cyber security managers seem especially daunting.

VA: IT, security progress to accelerate in 2008

The Veterans Affairs Department expects the technical applications that are the foundation of its information security will be in place during the next fiscal year, said Robert Howard, VA's chief information officer. Improving policies and procedures are a continuous process.

Privacy, IT officers come together to create policy

The Bush administration's effort to improve how agencies protect personally identifiable information and report breaches has pushed federal privacy and information technology officers to work together, according to federal privacy and data security executives.

Solution Provider News

Avaya Honors Verizon Business as 2007 Alliance Partner of the Year

Avaya Inc. (NYSE:AV), a leading global provider of business communications applications, systems and services, today announced that Verizon Business has been named the company's 2007 Alliance Partner of the Year based on revenue growth, performance and commitment to the sale of Avaya products and services.

Microsoft-backed Enterprise Mobile launches

Enterprise Mobile, a Microsoft-funded startup, made its debut yesterday. The firm, led by software distribution veteran Mort Rosenthal, will help deliver and manage Windows Mobile devices for enterprises.

EBay: Phishers getting better organized, using Linux

When it comes to launching online attacks, criminals are getting more organized and branching out from the Windows operating system, eBay's security chief said Tuesday. EBay recently did an in-depth analysis of its threat situation, and while the company is not releasing the results of this analysis, it did uncover a huge number of hacked, botnet computers, said Dave Cullinane, eBay's chief information and security officer, speaking at a Microsoft-sponsored security symposium at Santa Clara University.



Awarded Contracts

Small Business Administration Awards \$30M Contract to SRA

SRA International, Inc., a leading provider of technology and strategic consulting services and solutions to federal government organizations, has been awarded a task order to provide a managed hosting solution for major information systems at the Small Business Administration (SBA). The task order, awarded in September under the Chief Information Officer Solutions and Partners 2 Innovations (CIO-SP2i) contract, has an estimated value of \$30 million over four years if all options are exercised.

Stanley Announces Additional \$17 Million Prime Contract Award to Support U.S. Marine Corps Recruiting Command Headquarters

Stanley, Inc., a leading provider of systems integration and professional services to the U.S. federal government, today announced the award of an additional \$17 million, five-year contract by the U.S. Marine Corps (USMC) to provide sustainment, support and enhancement for the Marine Corps Recruiting Command (MCRC) Recruiting Information Support System (MCRIS).

DHS awards \$74.1M professional support contract

The Homeland Security Department's Office of Intelligence and Analysis will get professional support services from General Dynamics under a five-year contract worth as much as \$74.1 million.

USDA first to award SmartBuy encryption contract

Aspect Security is a leading provider of application security services.



Assurance Services



Acceleration Services



Education and Training

Our security services enable organizations to eliminate flaws in their custom applications through rigorous security analysis, code review and application testing.

The Agriculture Department awarded SafeBoot through its partnership with Spectrum Systems the first enterprise encryption task order off SmartBuy's Data at Rest government-wide procurement vehicle.

The \$1.8 million contract provides for 180,000 licenses across USDA's 29 agencies for SafeBoot's device encryption, full-disk encryption and port monitoring controls, hardware, and the first year of maintenance and support.

[Back to top](#)

Ask the Dr.



Dr. Lenny Superville, Ph.D.
Chief Information Officer
North Carolina's Office of the State Auditor

Question: "How much should CIOs worry about the 'Insider-Threat' and what can be done to safeguard an organization against this threat?"

Answer:

CIO's have to worry about headlines in the mainstream media about their company losing control of its data. Sometimes, the cost for a breach cleanup may be in excess of hundreds of millions of dollars. This of course will get the attention of Board members who want to know what the CIO's are doing to prevent this from happening at their company.

There is plenty that CIO's can be doing. The technology has finally caught up with our security needs in watching and protecting our "intellectual" property.

Security is an ever moving target that must be continually managed and refined to ensure appropriate confidentiality, integrity, and availability of the services and systems that are critical to your business, as well as the valuable information that is often at the heart of the organizations CIO's defend.

To ask the Dr. and get your questions posted with his answers, please email: parhame@convurge.org. Your question can be anonymous and asked by ConVurge or we can post your name, title, organization - please specify preference.

[Back to top](#)

ConVurge News

Government Council Meetings 2008



SecureGOV March 9 - 11, 2008

SecureGOV Scope:

**Application Security
Authentication
Biometrics**

Cyber Security
Encryption
Identity Management
(HSPD-12:P/V, FIPS201)
Information Assurance
IPv6
Network Security
Physical Security
Risk Management & Compliance
SCAP
Secure Infrastructure
SOA Security
Wireless Security

Donna Dodson, Senior Computer Scientist and Deputy Director, Information Technology Laboratory, Computer Science Division, **NIST**

Mike Butler, Director, Access Card Office, Defense Manpower Data Center - OSD, **Department of Defense**

Rick Estberg, Chief of Staff, **Interagency OPSEC Support Staff**

Scott Bernard, Deputy CIO, Office of Railroad Administration, **Department of Transportation**

Ron S. Ross, Ph.D., Project Leader, FISMA Implementation Project, Computer Information Technology Laboratory, Computer Science Division, **NIST**

Daniel Schmidt, Technical Director, Engineering and Integration, Vulnerability Analysis and Operations Group, **NSA**

Paul Batrock, Technical Director for Operational Network Vulnerabilities, **NSA**

www.SecureGOVCouncil.org



MobileGOV March 9 - 11, 2008

MobileGOV Scope:

Authentication
Compliance
Convergence
COOP
Emergency Preparedness
Enterprise Mobility
Implementation
Information Assurance
Infrastructure
Inter-Agency Information Sharing
Interoperability
IPv6
Mobile/Remote Computing
Risk Management
Satellites
Scalability
Security
Spectrum Management
Surveillance

**Telework
WiFi/WiMax**

Mischel Kwon, Director, Information Assurance, Wireless Management Office, **Department of Justice**

John McManus, Deputy CIO and CTO, Office of the CIO, **Department of Commerce**

Peter Tseronis, Director of Network Service, Office of the CIO; Co-Chair, **Federal IPv6 Working Group-Department of Education**

Susan Moore, Director, Telecommunications Management Division, **US Department of Agriculture**

Jenny Hansen, Project Manager NG9-1-1, **Department of Transportation**

Pamela Kruzic, Nuclear Specialist and Incident Response, **Nuclear Regulatory Commission**

Kathy James, Office of training and Knowledge Management, **Department of Commerce**

www.MobileGOV.org



ArchitectureGOV June 2008

ArchitectureGOV Scope:

Managing Data as a National Asset
The Socialization of Information through
Data Architecture
Governance of SOA
Information Visibility and Reliability
Internal Controls, Compliance,
and Risk Management
What Effect is Architecture Having
on Your Mission?
E-Discovery
Infrastructure Lines of Business
EA: Measuring Values, Outcomes, and ROI
Practical guide to SOA
The Architecture of Privacy
Long-term EA trends and its impact
on EA today
How will a new administration
change policies that will affect EA
Identity and Access Management
Intergovernmental view of EA
Inter-agency collaboration
Records Management
Geospatial Capabilities
CPIC and EA
National Information Exchange

Richard "Dick" Burk, (*former*) Federal Enterprise Architecture Program, Chief Architect, Office of E-Government and Information Technology, **OMB, Executive Office of the President - Council Member**

John McManus, Deputy Chief Information Officer, and Chief Technology Officer, **US**

Department of Commerce

Ira Grossman, Chair, **Chief Architects Forum**

George Thomas, Chief Enterprise Architect, **General Services Administration**

Kshemendra Paul, Chief Enterprise Architect, **US Department of Justice**

Suzanne Acar, Senior Information Architect, **US Department of the Interior**

Mary E. McCaffrey, Senior Advisor to the Assistant Administrator, Office of Environmental Information, **US EPA**

John Sullivan, Chief Architect, **US EPA**

COL. James Kirby, Deputy Director, Army Architecture Integration Center & Chief, LandWarNet Architecture Integration and Battle Command Division, **Office of the CIO/G-6**

Richard Klemmer, Chief Enterprise Architect, National Telecommunications and Information Administration, **US Department of Commerce**

Donna K. Seymour, Chief Information Officer, **Special Assistant to the Associate Administrator for Administration Maritime Administration**

Neela Lakhmani, Assistant Director, Information Technology Architecture and Systems Issues, **US Government Accountability Office**

Dr. W. Stan Boddie, PMP, CISSP, Professor of Systems Management, Information Resource Management College, **US National Defense University**

Scott Bernard, Deputy Chief Information Officer, Office of Railroad Administration, **US Department of Transportation**

www.ArchitectureGOV.org



HrGOV September 2008

HrGOV Scope:

COOP
Human Capital Management
Leadership
Learning
Performance
Project Management
Recruiting
Talent
Telework
Training
Workforce Management

Norman Enger, (*former*) Director, Human Resources Line of Business Program Management Office, **Office of Personnel Management - Council Member**

Arleas Upton Kea, Director, Division of Administration, **Federal Deposit Insurance Corporation**

Mary Lacey, Program Executive Officer, **National Security Personnel Service, Department of Defense**

Marco Santini, Director, Federal Learning Technology Program, **General Services Administration**

Joe Chang, Director of Acquisition Workforce and Career Management, **Defense Acquisition University**

Chris Hardy, Deputy Director, **Defense Acquisition University**

Dr. Kathleen James, Office of Training and Knowledge Management, **Department of Commerce**

Dr. Ronald Sanders, Associate Director of National Intelligence for Human Capital and Chief Human Capital Officer, **Office of the Director of National Intelligence**

www.HrGOV.info

The content of each GOVmeeting is steered by a Strategic Intelligence Council comprised of public and private sector executives, who are recognized for their knowledge and expertise in their respective profession.

Join round table discussions and interactive strategy sessions with other senior level executives to discuss initiatives, challenges, and strategies for common goals. Be involved and share your insight and knowledge in your area of expertise with the group.

You have the opportunity to revolutionize the way government does business.

"There *is* a solution, find it."
--Thomas Edison

For more information on how you can participate, please contact us:

Kelly Yocum
CEO
ConVurge
1701 Pennsylvania Avenue, NW
Suite 300
Washington, DC 20006
202.248.5411

ConVurge ... Where government and technology intersect.

[Back to top](#)