



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 02 September 2004

Current Nationwide  
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- First Coast News reports that after Hurricane Charley, there is a potential for identity theft stemming from financial records and documents strewn about in storm debris. (See item [5](#))
- The Department of Homeland Security has announced September as National Preparedness Month, with hundreds of activities planned to highlight the importance of individual emergency preparedness. (See item [18](#))
- The US-CERT has released "Technical Cyber Security Alert TA04-245A: Multiple Vulnerabilities in Oracle Products." (See item [24](#))

### DHS/IAIP Update *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Web Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *September 01, CBS.MarketWatch* — **Dip in natural gas prices seen.** Natural gas prices are forecast to drop as much as 10 percent in 2005, Merrill Lynch said in a new report Wednesday, September 1. "Over the last month or so, natural gas prices have been moderating since there has been little cooling demand, more liquefied natural gas imports at the front half of the summer, and no real Gulf of Mexico hurricane downtime or infrastructure loss of consequence," analyst John Herrlin wrote in the report. **Herrlin said he expects full natural gas supply levels of 3.1 trillion to 3.2 trillion cubic feet by the start of the season when storage is opened for withdrawals. However, prices aren't likely to fall much below \$5 per**

**thousand cubic feet due to high crude prices, he said.** "But 2005 natural gas prices could be down 10 percent vs. 2004 realizations without strong winter weather demand, and given our current assumptions on the U.S. economy," Herrlin wrote.

Source: <http://cbs.marketwatch.com/news/story.asp?guid=%7B405A4EA6%2DCB8B%2D45B9%2DBC65%2D60AF5B00C629%7D&dist=rss&siteid=mktw>

- 2. August 31, Reuters — U.S. drivers can expect highest Labor Day gasoline prices.** A record number of Americans planning one last summer road trip this weekend will shell out the highest Labor Day gasoline prices ever seen, and there's little relief in sight, experts said on Tuesday, August 31. **A shortage of domestic refineries and ever-growing demand in the United States is likely to turn this summer's sticker-shock at the pumps into a routine of higher fuel costs for years to come,** analysts said. In the near-term, September will likely show average U.S. gasoline prices falling to \$1.80 a gallon or less, from the current \$1.86, said Doug MacIntyre, analyst for the U.S. Energy Information Administration (EIA). This is normal. Once Labor Day passes, driving demand diminishes and gasoline prices fall, MacIntyre said. Last year, after Labor Day, prices dropped 15.5 cents by the end of September, but this year's drop is not expected to be as big, said MacIntyre. **The EIA said that gasoline demand is expected to continue to rise about 100,000 barrels per day annually, far outpacing increases in domestic production. This will mean a growing reliance on imports and a higher likelihood of price spikes,** said Dan Gilligan, president of the Petroleum Marketers Association of America (PMAA).

Source: [http://news.yahoo.com/news/?tmpl=story&u=/nm/20040831/us\\_nm/energy\\_gasoline\\_labor\\_dc\\_1](http://news.yahoo.com/news/?tmpl=story&u=/nm/20040831/us_nm/energy_gasoline_labor_dc_1)

- 3. August 31, The News Journal (DE) — Conectiv ordered to alter outage response.** Delaware state regulators on Tuesday, August 31, ordered power utility Conectiv to change the way it responds to massive power outages, including restarting a program that warns customers with medical conditions about approaching storms that could cause a blackout. In ordering improvements to how Conectiv prepares for and responds to widespread blackouts, the Delaware Public Service Commission ended a nine-month investigation into the company's performance during last year's Hurricane Isabel, which knocked out power to 109,000 customers for up to one week. The commission also ordered the company to speed up its plans to improve the restoration process, and its ability to give customers an estimate of when their power would return. One of the biggest complaints during the blackouts was that customers who had been waiting for days had no idea when to expect their power to be restored. Conectiv also must train more employees to perform "second jobs," such as customer-service work, during a major storm.

Source: <http://www.delawareonline.com/updates/Conectivordered.html>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## Defense Industrial Base Sector

4. *September 01, Federal Computer Week* — **Improving NIPRNET. Department of Defense (DoD) information technology officials recently installed new hardware to better protect military networks. However, the new equipment cannot achieve its full capability unless DoD's IT workers install products correctly and patches more quickly, according to a Defense Information Systems Agency (DISA) official.** DISA officials put in large routers at the base borders of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET), said Joe Boyd, chief of DISA's Center for Network Services. The new hardware should increase NIPRNET's security, letting DoD workers do their day-to-day activities, Boyd said. However, he added that improving information assurance department-wide also requires IT workers to work more diligently. About 62 percent of military networks' intrusions result from poor configuration practices, Boyd said. Another 24 percent comes from not installing software fixes and updates in a timely fashion -- a negligence that DoD technology officials describe as unresponsiveness to information assurance vulnerability alerts, said Boyd, who oversees combat support of the Global Information Grid, the military's network of voice, video and data systems.

Source: <http://www.fcw.com/fcw/articles/2004/0830/web-niprnet-09-01-04.asp>

[[Return to top](#)]

## Banking and Finance Sector

5. *September 01, First Coast News (FL)* — **Disaster creates potential for identity theft.** As victims of Hurricane Charley try to recover, there's another kind of disaster waiting to happen, identity theft. **When Hurricane Charley left fields of debris in Port Charlotte, FL, it also left some very personal information belonging to residents in the area. A reporter found boxes of property appraisals containing social security numbers and other personal information.** All of it was out in the open, and available for would be thieves. The documents were found outside of the American Eagle Appraisals, an office Charley destroyed. Mixed in the debris was the file of financial planner Francis Long. Long said with that little bit of information, fraud, terrorist activities, or even run of the mill identity theft could have happened. He says businesses have a responsibility to keep confidential client information safe and secured in case a storm hits. Local police were called and are now investigating the case. The department of financial services says it will put out a notice to businesses damaged by Hurricane Charley, reminding them not to dispose of confidential information without shredding it first.

Source: <http://www.firstcoastnews.com/news/florida/news-article.aspx?storyid=23615>

6. *August 31, United Press International* — **Banks announce Web finance data repository. The U.S. Federal Reserve Board said Tuesday, August 31, federal banking agencies would implement a Web-based Central Data Repository (CDR) for bank data in 2005.** The CDR is an Internet-based system created to modernize and streamline how the agencies collect, validate and distribute financial data, or "Call Reports," submitted by banks. Originally scheduled for implementation in October 2004, the system's start date was postponed last month to address industry feedback and to allow more time for testing and enrollment. The

agencies are currently considering Call Report changes that may also be introduced in 2005.

Source: [http://washingtontimes.com/upi-breaking/20040831-025428-4732\\_r.htm](http://washingtontimes.com/upi-breaking/20040831-025428-4732_r.htm)

[\[Return to top\]](#)

## **Transportation Sector**

7. *September 01, KLTV 7 (TX)* — **American Airlines flight lands at Pittsburgh after bomb threat.** An American Airlines flight was grounded at Pittsburgh International Airport overnight. That's where the pilot of the Chicago-to-New York flight made an unscheduled landing last night after a threat was found written on a passenger's tray table. Crews at the Pittsburgh airport searched the M-D-80 jet. There was no immediate word that anything suspicious was found — other than the tray table message. Authorities say they don't have any suspects in the incident aboard American Flight 346. Authorities say the jet's 130 passengers were put on another plane to New York. None of them nor the five crew members were reported injured. American Airlines is headquartered in Fort Worth, Texas.  
Source: <http://www.kltv.com/Global/story.asp?S=2244752>
  
8. *September 01, Department of Transportation* — **Emergency grant to restore Florida airport.** Department of Transportation Secretary Norman Y. Mineta and Florida Governor Jeb Bush on Wednesday, September 1, announced an emergency federal grant of \$5.4 million to help Charlotte County airport in Punta Gorda rebuild in the wake of damage caused by Hurricane Charley. **The grant will provide immediate funding to restore the airport runway's lighting, fencing, drainage and electrical systems.** The grants come from the Airport Improvement Program of the U.S. Department of Transportation's Federal Aviation Administration. In addition to the \$5.4 million announced for Charlotte County, the Department has also made available \$10.7 million for Orlando International, \$1.5 million for Orlando Sanford, \$600,000 for Daytona Beach, and \$2 million for general aviation airports throughout the state.  
Source: <http://www.dot.gov/affairs/dot15904.htm>
  
9. *September 01, USA TODAY* — **United plans 6,000 job cuts. United Airlines, currently in Chapter 11 reorganization under bankruptcy law, plans an extra 6,000 job cuts as part of a cost-cutting plan, the Financial Times newspaper reported on Wednesday, September 1.** The cuts amount to a 10% reduction in the current workforce. Before the attacks in the United States on September 11, 2001, the airline had employed 104,000 people. It now employs 62,000. The report, quoting sources close to the matter, said the airline planned to reduce annual operating costs by \$655 million. The report of extra cuts comes amid growing anger from the airline's flight attendants. Reuters reports the attendant's union is calling for new company management. The reported cuts come just a day after the airline said it would recall 375 flight attendants due to fuller planes and more international flights.  
Source: [http://www.usatoday.com/travel/news/2004-09-01-united-cuts\\_x.htm](http://www.usatoday.com/travel/news/2004-09-01-united-cuts_x.htm)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

10. *August 30, Associated Press* — **Radiation leak shuts post office. Health officials declared a New York City postal facility free of radiation Monday, August 30, a day after a low-level leak from an X-ray camera forced the closing of the building and surrounding streets.** After conducting tests, authorities found no elevated radiation levels in the Franklin D. Roosevelt Station or adjacent streets. The facility was closed Sunday "out of abundance of caution," health officials said, although there was no evidence of a significant health risk. Twenty postal employees, but no customers, were inside the closed station when the leak occurred. The leak occurred as a contractor was using the X-ray camera to make an assessment of piping within the building's loading bays and ramps. A mechanical problem with the camera occurred, and elevated radiation levels were detected, health officials said. The contractor was doing work for another building tenant, post office spokesperson Pat McGovern said.  
Source: [http://abcnews.go.com/wire/US/ap20040830\\_2135.html](http://abcnews.go.com/wire/US/ap20040830_2135.html)

[\[Return to top\]](#)

## **Agriculture Sector**

11. *September 01, Reuters* — **Vietnam expects bird flu to linger. Vietnam has warned that bird flu is a "local epidemic" that could erupt anywhere, and says it expects the virus to linger for at least five more years.** The warning from the agriculture ministry follows criticism that Vietnam was too quick to declare an outbreak over earlier this year. "It is very difficult to eradicate the bird flu virus. Our hope is in five years we could get rid of this virus entirely," Bui Quang Anh, director of the agriculture ministry's animal health department, told a news conference on Wednesday, September 1. Vietnam was criticized for declaring at the end of March that it had vanquished the virus, which re-emerged in July, confirming experts' warnings it was almost certain to reappear. The agriculture ministry said poultry farms were especially at risk of fresh outbreaks. Anh also said two more provinces, Hai Duong in the north and Quang Tri in the centre, have reported H5N1 bird flu infections in poultry but that the outbreak had been contained. The new cases took the total number of provinces that reported bird flu infection this time to 13.  
Source: <http://www.reuters.co.uk/newsPackageArticle.jhtml?type=world&News&storyID=574968&section=news>

12. *September 01, San Diego Union-Tribune (CA)* — **Scientists scramble to understand disease ravaging a California icon.** For nearly a decade, scientists have been watching oaks die in Northern California's coastal forests. In some years, the blight that is killing them spreads slowly, giving scientists hope that they might figure out ways to control it before it spirals totally out of control. But in other years, it has spread much more quickly. By now, its impact is readily apparent even to the casual observer. **The cause is a disease called sudden oak death, which started cropping up in 1995 and has since killed tens of thousands of trees. And that's just the beginning: More trees are dying each month. Most are in the coastal mountains between Big Sur and northern Sonoma County, but the disease has crept as far north as Oregon, and nearly as far south as San Luis Obispo.** In places, the blight is so extensive that entire hillsides have been devastated, says David Rizzo, a plant pathologist at the University of California Davis. **Ecologically, the death of that many oaks is an immense change to California's coastal woodlands. To start with, all of that dead wood will provide**

**fuel for potentially intense fires. In addition, sick, dead and dying trees open the door for the spread of other diseases.** That's beginning to happen in some areas, where Rizzo says that a native pathogen, oak root fungus, is already taking hold.

Source: [http://www.signonsandiego.com/news/science/20040901-9999-1c1\\_oak.html](http://www.signonsandiego.com/news/science/20040901-9999-1c1_oak.html)

[\[Return to top\]](#)

## **Food Sector**

### **13. *August 31, Government Computer News* — Report urges faster mad cow tracking system.**

**The U.S. Department of Agriculture should expedite development of a new disease surveillance system for tracking cattle samples from collection to testing to reporting results and integration with diagnostic testing labs, a recent report from the department's Office of Inspector General said.** The new system will support the department's expanded program to test cattle for bovine spongiform encephalopathy (BSE). Under the program, the Animal and Plant Health Inspection Service (APHIS) and the Food Safety and Inspection Service plan to increase testing to 200,000 cattle annually from 12,500. APHIS, the agency responsible for the new system, should also implement performance measures and a continuous risk assessment to enhance management of the program and better assess its effectiveness, the report said.

Source: [http://gcn.com/vol1\\_no1/daily-updates/27121-1.html](http://gcn.com/vol1_no1/daily-updates/27121-1.html)

### **14. *August 31, American Forces Press Service* — Test program protects food, water supplies.**

The Defense Department's Veterinary Food Analysis and Diagnostic Laboratory analyzes food bound for troops in Iraq, Afghanistan, and elsewhere around the world, as well as military dining facilities, commissaries, exchanges, clubs, and other outlets, to ensure it's free of pathogens, heavy metals, and chemical contamination. **Colonel Les Huck, the lab's director, said the current system still isn't responsive enough. New equipment under development will make it easier for specially trained troops on the ground to do their own testing, with far faster results.** A wide range of test equipment and procedures is being developed, he said, and some are already being delivered to forward-based troops. The ultimate goal, Huck said, is to get enough "rapid screening process" capability into the field so troops can rapidly screen for pathogens and pull any suspect items from the inventory.

Source: [http://www.defenselink.mil/news/Aug2004/n08312004\\_2004083101.html](http://www.defenselink.mil/news/Aug2004/n08312004_2004083101.html)

[\[Return to top\]](#)

## **Water Sector**

### **15. *August 30, Kentucky Lake Times* — Lake contaminated with toxic chemical.** A Tennessee Emergency Management Agency spokesperson says that chemical cleanup is now nearly finished where polyurethane was found in a creek in Robertson County. **Kurt Pickering said that almost a hundred gallons of a polyurethane leaked into a retention pond on the property of the Collins and Aikman plant.** But the pond then leaked and Pickering says some of the chemical went down a sinkhole. **Then environmental and emergency crews found themselves pumping out water from the Wartrace Creek and Wartrace Lake after finding**

**the same chemical in both places.** Safety agencies have placed booms in the various areas throughout water in an attempt to contain the hazardous spill. They said it would take several more days to completely clean up the spill. Investigators said that they are trying to figure out exactly how the spill occurred. Polyurethane contains toluene di-isocyanate which is toxic. In addition, polyurethane products also contain additives, such as insecticides and fungicides.  
Source: <http://www.kentuckylaketimes.com/localnews/august04/lakecontam/08300406.php>

[[Return to top](#)]

## **Public Health Sector**

**16. *September 01, Agence France Presse* — Death from bubonic plague in China. At least one person has died from an outbreak of bubonic plague in northeastern China but the disease has now been brought under control, the health ministry said on Wednesday, September 1.** Two cases were found, one in Gansu province's Sunan county and the other in Qinghai province's Qilian county, a ministry Website notice said. It gave no further details about the cases. The World Health Organization (WHO) was seeking more information after being told about the cases, said spokesperson Roy Wadia who added bubonic plague was not uncommon and occurred across the world from time to time. The health ministry urged local authorities to take measures to prevent the disease and to raise health staff awareness about symptoms in case it spread.

Source: [http://www.channelnewsasia.com/stories/afp\\_asiapacific/view/104311/1.html](http://www.channelnewsasia.com/stories/afp_asiapacific/view/104311/1.html)

**17. *September 01, The Oregonian* — Hospitals stock up for terrorism.** Ten Oregon hospitals have purchased biosafety cabinets at a cost of several thousand dollars each. The cabinets use high-tech air filters to protect hospital workers from anthrax, smallpox and other biological agents. The cabinets represent the first purchases made from millions of dollars in federal funds aimed at making Oregon's medical care facilities better prepared for bioterrorism catastrophes that could cause large numbers of casualties. Similar steps are being taken at facilities nationwide as the Department of Homeland Security and other federal agencies push hospitals to become better prepared to handle future terrorist attacks. But according to Dr. John Jui, medical director for several municipalities and government agencies, including the city of Portland, Multnomah County and the Oregon State Police, Oregon hospitals, by almost anyone's measure, still have a long way to go. **During a bioterrorist attack, people who may not need acute care will probably bypass first responders and head for a hospital anyway. The result: a deluge of patients, making it all the more difficult to assess the infected.**

Source: <http://www.oregonlive.com/business/oregonian/index.ssf?/base/business/1094039961318270.xml>

[[Return to top](#)]

## **Government Sector**

Nothing to report.

[[Return to top](#)]

## Emergency Services Sector

18. *September 01, Department of Homeland Security* — **National Preparedness Month.** The Department of Homeland Security has announced September as National Preparedness Month. **Throughout the month, hundreds of activities are planned to highlight the importance of individual emergency preparedness.** The National Preparedness Month coalition, which includes the U.S. Department of Homeland Security, more than 80 organizations and all 56 states and territories, will encourage Americans to take simple steps now to prepare themselves and their families for any possible emergencies. For a listing of the National Preparedness Month coalition members, their planned activities and points of contact, see this site:  
Source: <http://www.dhs.gov/dhspublic/display?content=3963>
19. *September 01, Associated Press* — **Florida calls for hurricane evacuations.** Hundreds of thousands of people were told Wednesday, September 1, to get ready to evacuate as Hurricane Frances crept closer to Florida just weeks after Hurricane Charley's rampage. It would be the worst double hurricane strike on one state in at least a century. **Forecasters warned the core of the Category 4 storm with 140–mph top sustained winds was due along Florida's Atlantic coast late Friday, September 3, or early Saturday.** About 300,000 residents in coastal areas of Palm Beach County were told to evacuate starting 2 p.m. Thursday, September 2. In Rockledge, about 45 miles southeast of Orlando, Brevard County told at least 50,000 residents to start evacuating mobile homes and barrier islands Thursday afternoon. In Stuart about 85 miles south, Martin County planned to urge up to 7,500 residents to evacuate low-lying areas starting at noon Thursday. **Craig Fugate, director of the state Division of Emergency Management, said steps were being taken for to prepare for large-scale evacuations, including possibly reversing lanes of some highways to accommodate fleeing coastal residents.**  
Source: <http://apnews.myway.com/article/20040901/D84R1MC80.html>
20. *September 01, Government Technology* — **South Carolina's hurricane evacuation Web-based system performed successfully.** The South Carolina Hurricane Evacuation Decision Support Solution, managed by the South Carolina Department of Transportation (SCDOT), provides government officials, the Emergency Preparedness Office and transportation executives with near real-time information on rapidly changing traffic and evacuation route information. With information provided by the Web-based system, officials successfully managed the mandatory evacuation of residents along the state's East coast during Hurricane Charley. **The system's intelligent maps incorporate live traffic volume and speed information from SCDOT's GIS; automated traffic recorders; evacuation route and detour maps; traffic cameras; and real-time weather data.** The Web application integrates interactive maps with dynamic traffic volume and traffic speed charts and graphs. Using a combination of maps, charts and graphs, SCDOT personnel can analyze and estimate evacuation traffic. The system enables SCDOT to compare current traffic trends with normal loads, look for traffic slow-downs and determine if alternative routes should be opened and/or lane directions should be reversed on selected routes.  
Source: <http://www.govtech.net/news/news.php?id=91321>
21. *August 31, National Journal* — **EPA scout plane on lookout for toxic chemicals at GOP convention.** The massive effort to protect the Republican convention has meant bringing in

special units including a scout plane belonging to the Environmental Protection Agency (EPA). With the Army providing the technology, Gary Brown, emergency management coordinator for Woodbury County, IA, contributing the local users' perspective, and the EPA footing the bill — about \$500,000 a year — EPA official Mark Thomas put together a program called ASPECT (Airborne Spectral Photometric Environmental Collection Technology). **ASPECT's array of sensors and analysis software are mounted on a twin-propeller Aero Commander 680; the equipment allows the three-person crew to map the location of a toxic cloud and to determine its composition. The system can download data to a wide range of wireless networks but, if necessary, it can also parachute a special terminal to first responders on the ground.** Since ASPECT became operational in April 2001, it has been deployed 36 times, on missions ranging from a chlorine-spilling train derailment near San Antonio, TX, to the 2002 Olympic Games, to the crash of the space shuttle Columbia (with its release of toxic fuel).

Source: [http://www.govexec.com/story\\_page.cfm?articleid=29353&dcn=to\\_daysnews](http://www.govexec.com/story_page.cfm?articleid=29353&dcn=to_daysnews)

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

22. *September 01, Secunia* — **Kerberos V5 multiple vulnerabilities.** Multiple vulnerabilities have been reported in Kerberos V5, where the most serious can potentially be exploited by malicious people to gain access to protected corporate networks and execute arbitrary code. Patches are available (see patch matrix in the original advisories). Update to version 1.3.5, when it becomes available: <http://web.mit.edu/kerberos/dist/index.html> Original Advisories: <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-02-dblfree.txt> and <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-03-asn1.txt>  
Source: <http://secunia.com/advisories/12408/>
  
23. *September 01, PC World* — **Al Qaeda's tech traps.** Al Qaeda and other terrorist groups are becoming more technically adept at using the Web and computers. The arrest of alleged Pakistani terrorist Mohammad Naeem Noor Khan, captured this summer with 51 optical discs and three computers full of terror intelligence, is the most recent indicator. For the past ten years, dissidents from the Middle East, Chechnya, and Latin America have used the Internet to further their cause, says Josh Devon, a senior analyst at the SITE Institute, a terrorism research group that monitors the Web. **But the proliferation of the Web and the availability of more powerful and affordable graphics and multimedia processing tools have dramatically increased al Qaeda's and other terrorist groups ability to communicate, to broadcast their message, to create public lists of who and what to target, and to train others much more than was possible even five years ago.** While technology can make it easier to conceal information and communicate covertly using digital tools such as encryption, it also leaves digital trails of evidence. Computer intelligence found on Khan's computers was instrumental in the arrests of Pakistani and UK terror suspects.  
Source: <http://www.pcworld.com/news/article/0,aid,117658,00.asp>
  
24. *September 01, US-CERT* — **Technical Cyber Security Alert TA04-245A: Multiple Vulnerabilities in Oracle Products.** Several vulnerabilities exist in the Oracle Database Server, Application Server, and Enterprise Manager software. The most serious vulnerabilities

could allow a remote attacker to execute arbitrary code on an affected system. Oracle's Collaboration Suite and E-Business Suite 11i contain the vulnerable software and are affected as well. **The impacts of these vulnerabilities range from the remote unauthenticated execution arbitrary code to data corruption or leakage.** Vendor patches and updates are available: <http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf>  
Source: <http://www.uscert.gov/cas/techalerts/TA04-245A.html>

25. *September 01, Government Computer News* — **The human factor trumps IT in the war on terror.** Computer scientists at the University of Maryland are pushing the technology envelope to assist in intelligence gathering and analysis, but the people using the data may be the limiting factor in its effectiveness. “While there is a lot of good information out there, it isn’t getting to the right people at the right time,” said William J. Lahneman, coordinator of the Center for International and Security Studies in the School of Public Policy. Implementing recent presidential directives on moving data across agency lines will require not only changing IT architectures, but will “challenge the very culture” of those agencies, said James Hendler of the university’s Institute for Advanced Computer Studies. **Hendler is focusing on the intelligence needed to use the Web effectively in gathering information and answering questions.** The university’s Computational Linguistics and Information Processing Lab is developing more-fluent automated translation systems for languages such as Arabic. Co-director Amy Weinberg said the lab also is working on how to rapidly ramp up systems to handle new languages as new threats develop. **Some terrorist groups already are ahead of the government in their use of existing Web technology to win the hearts and minds of people, said Lee Strickland, director of the university’s Center for Information Policy.**  
Source: [http://www.gcn.com/vol1\\_no1/daily-updates/27131-1.html](http://www.gcn.com/vol1_no1/daily-updates/27131-1.html)

26. *August 31, SecurityTracker* — **Input validation flaw in 'register.php' lets remote users conduct cross-site scripting attacks.** According to SecurityTracker, 'register.php' does not filter HTML code from user-supplied input in the username or blog name fields. A remote user can submit specially crafted input so that when a target user views the names of the blogs, arbitrary scripting code will be executed by the target user's browser. **As a result, a remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the pLog software, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user.** No vendor solution is available at this time.  
Source: <http://www.securitytracker.com/alerts/2004/Aug/1011117.html>

27. *August 31, Federal Computer Week* — **DoD reveals viral infection. Two computers in the Army Space and Missile Defense command connected to the Defense Department’s classified Secret Internet Protocol Router Network (SIPRNET) were infected because they did not have any virus protection.** William Congo, a spokesperson for the Huntsville, AL-based Space and Missile Defense Command said the two computers were located at a facility in Colorado Springs, CO. **The viruses were detected quickly and the two computers were then isolated from the SIPRNET, Congo added.** The incident occurred "within the past month" and officials are still investigating the matter to determine how the infection occurred and prevent future occurrences, he said.  
Source: <http://www.fcw.com/fcw/articles/2004/0830/web-siprnet-08-31-04.asp>

## Internet Alert Dashboard

### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** The US-CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See <http://www.us-cert.gov/cas/alerts/SA04-243A.html> for more information.

### Current Port Attacks

<b>Top 10 Target Ports</b>	445 (microsoft-ds), 135 (epmap), 137 (netbios-ns), 9898 (dabber), 5554 (sasser-ftp), 1023 (Reserved), 1434 (ms-sql-m), 139 (netbios-ssn), 1433 (ms-sql-s), 3127 (mydoom) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## Commercial Facilities/Real Estate, Monument & Icons Sector

### 28. *September 01, New York Times* — **Suit seeks tighter security at the Empire State Building.**

Two partners in a law firm in the Empire State Building in New York City have sued the building's operators, claiming that security is too lax at the 102-story Midtown landmark and that tenants are exposed to the "clear and present danger" of a terrorist attack. According to the lawsuit, filed Tuesday, August 31, by the firm Broder & Reiter, the building's operators recently reduced the level of security they had instituted after the September 11, 2001, terrorist attacks by removing scanners, screening devices and security personnel from the building's lobby. **In the suit, filed in State Supreme Court, the plaintiffs cite reports that terrorist groups like al Qaeda have conducted surveillance in the city and desire to attack symbolic buildings. The Empire State Building, the suit states, would be a prime target.** A spokesperson for the Empire State Building, Howard J. Rubenstein, issued a statement denying the charge of recklessness and saying the building's security practices were based upon industry standards.

Source: <http://www.nytimes.com/2004/09/01/nyregion/01empire.html>

[\[Return to top\]](#)

## General Sector

29. *September 01, Associated Press* — **Hundreds held hostage in Russian school. Attackers wearing suicide–bomb belts seized a school in a Russian region bordering Chechnya on Wednesday, September 1, and were holding hundreds of hostages, including 200 children. The assault came a day after a suicide bomber killed 10 people in Moscow.** The attackers warned they would blow up the school if police tried to storm it and forced children to stand at the windows, said Alexei Polyansky, a police spokesperson for southern Russia. Both the school attack and the Moscow bombing appeared to be the work of Chechen rebels or their sympathizers, but there was no evidence of any direct link. The two strikes came just a week after two Russian planes carrying 90 people crashed almost simultaneously in what officials also say were terrorist bombings. "In essence, war has been declared on us, where the enemy is unseen and there is no front," Russian Defense Minister Sergei Ivanov said, according to the Interfax–Military News Agency. He spoke before the seizure. **The hostage–takers demanded the release of fighters detained over a series of attacks on police facilities in neighboring Ingushetia in June, the ITAR–Tass news agency reported.** The well–coordinated raids killed more than 90 people.

Source: [http://abcnews.go.com/wire/World/ap20040901\\_399.html](http://abcnews.go.com/wire/World/ap20040901_399.html)

30. *September 01, Reuters* — **Russia sends troops to guard nuclear sites. Russia deployed extra troops to guard dozens of nuclear facilities across the country on Wednesday, September 1, after militants seized a school in the south, and a suicide bomb attack in Moscow,** the nuclear authority said. Russia, the world's number two atomic power after the United States, has come under international pressure to do more to protect its Soviet–era nuclear facilities against attack. Russia runs dozens of atomic reactors, uranium enrichment facilities and nuclear research reactors — some in the far–flung corners of Siberia and which are poorly guarded. **Reactors are also attractive to militants because atomic fuel stored at many sites can be used in nuclear bombs.**

Source: <http://www.reuters.com/newsArticle.jhtml?type=worldNews&storyID=6123907>

[[Return to top](#)]

### DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 883-3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.