



## Department of Homeland Security Daily Open Source Infrastructure Report for 25 January 2008

Current Nationwide



[For info click here](#)

- The Miami Herald is reporting Florida Power & Light (FPL) is facing \$208,000 in federal fines because firing pins were removed from the weapons of Wackenhut guards at its Turkey Point nuclear power plant in Florida. The Nuclear Regulatory Commission's announcement Tuesday listed four violations: two for "willfully failing to properly equip" armed guards, one for failing to promptly report the incident, and the fourth for providing incomplete and inaccurate information about the incident. (See item [6](#))
- According to Computerworld, an Arabic-language Web site, hosted on a server located in Tampa, Florida, is offering a new version of software that was designed to help al-Qaeda supporters encrypt their Internet communications. The tool is being distributed free of charge on a password-protected Web site that belongs to an Islamic forum known as al-Ekhlaas, according to Secure Computing and a blog posting by MEMRI. (See item [26](#))

### **DHS Daily Open Source Infrastructure Report Fast Jump**

Production Industries: [Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams](#)

Service Industries: [Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities](#)

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

Federal and State: [Government Facilities; Emergency Services; National Monuments and Icons](#)

## **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://www.esisac.com>]

1. *January 24, Centre Daily Times* – (New York) **American Superconductor receives Department of Homeland Security contract for project HYDRA.** American Superconductor Corporation (AMSC), a leading energy technologies company,

announced Thursday that it has received a contract from the Department of Homeland Security for Project HYDRA, which focuses on the development and deployment of AMSC's Secure Super Grids technology in the power delivery network in Manhattan operated by Consolidated Edison Company of New York, Inc. Under the terms of the final contract, DHS will provide up to \$25 million in total funding for the \$39 million project. "Utilities worldwide are seeking ways to relieve choke points and instantly suppress power surges in their grids, and Secure Super Grids technology accomplishes both goals simultaneously," said the chief executive officer of AMSC. "[We] look forward to its successful completion in 2010," he said.

Source: <http://www.centredaily.com/business/technology/story/354310.html>

2. *January 24, Associated Press* – (North Dakota) **ND oil pipeline will be stronger near lake, aquifer.** The developer of the Keystone oil pipeline has agreed to lay stronger pipe near a lake and aquifer, and drill a Sheyenne River crossing to save nearby trees and foliage, the state Public Service Commission (PSC) said. TransCanada is pushing for final PSC approval of the pipeline's route to allow the company to begin construction this spring. 2.3 miles of thicker pipe will be installed near the Fordville aquifer in Walsh and Grand Forks counties in North Dakota, and another 1.4 miles of heavier pipe will be installed east of Lake Ashtabula, near Valley City, a PSC Commissioner said. "[Both] of those places represent municipal drinking water supplies," he said. Opponents of the pipeline and some landowners along its suggested route now have ten days to comment on the change. The Keystone project is intended to transport oil from Alberta province in western Canada to locations in Illinois and Oklahoma. The pipeline's proposed route burrows beneath the Sheyenne River in Ransom County in southeastern North Dakota.  
Source: <http://www.bismarcktribune.com/articles/2008/01/24/news/state/147250.txt>

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

## **Chemical Industry Sector**

3. *January 23, Infrastruct Security* – (National) **Infrastruct Security, Inc. creates task force dedicated to protecting critical infrastructure and providing non-lethal defense solutions.** Infrastruct Security, Inc. formed the Homeland Defense Division to assist chemical facilities with Chemical Facility Anti-Terrorism Standards compliance. The team is armed with emerging defensive security technology, specifically designed to counter the sophisticated terrorist threats facing our nation's critical infrastructure.  
Source: <http://prweb.com/releases/2008/1/prweb647151.htm>

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

## **Nuclear Reactors, Materials, and Waste Sector**

4. *January 24, Cape Cod Times* – (Northeast) **NRC staff opposes license renewal delay.** The Nuclear Regulatory Commission staff is balking at a petition from Duxbury-based Pilgrim Watch and three other citizens groups that seek to halt license renewal proceedings at nuclear power plants until safety inspections are conducted again. In its recommendation to the commission, the NRC staff argues that the petition is not timely,

lacks the necessary legal basis, and does not satisfy requirements to stop the process. “The requested stay will harm the license renewal applicants by denying them determinations on their applications for an indefinite period,” wrote the NRC staff. The Pilgrim Nuclear Power Station in Plymouth, Massachusetts, and three other plants in the Northeast region are in the process of having their licenses renewed. A safety report released last year found few problems at Pilgrim.

Source:

<http://www.capecodonline.com/apps/pbcs.dll/article?AID=/20080124/NEWS/801240324>

5. *January 23, Associated Press* – (Mississippi) **Entergy to submit final application for nuclear reactor.** Entergy Nuclear officials plan to submit an application next month for permits that would clear the way for construction of a second nuclear reactor at the Grand Gulf Nuclear Station near Port Gibson in southwest Mississippi. Approval by the Nuclear Regulatory Commission of the Combined License Application would be one of the final steps before construction could begin. However, Entergy has not decided if the company plans to build the reactor yet, and the final application process will take years. The NRC and Entergy officials will hold a public meeting in Port Gibson on February 21, so concerned residents can ask questions about the application. Officials said security concerns would be addressed at the appropriate time during the application process.

Source: <http://www.dailycomet.com/article/20080123/APN/801231041>

6. *January 23, Miami Herald* – (Florida) **FPL blasted for security gaffe at Turkey Point.** Florida Power & Light (FPL) is facing \$208,000 in federal fines because firing pins were removed from the weapons of Wackenhut guards at its Turkey Point nuclear power plant in Florida. The Nuclear Regulatory Commission’s announcement Tuesday listed four violations: two for “willfully failing to properly equip” armed guards, one for failing to promptly report the incident, and the fourth for providing incomplete and inaccurate information about the incident. Neither FPL nor Wackenhut -- a security firm -- offered explanations on Tuesday for why the firing pins were removed. An FPL spokeswoman said FPL had taken corrective actions in the security organization. While the mistakes were made by Wackenhut employees, “we believe in strong oversight and we’re ultimately responsible,” she said. “The NRC has concluded FPL retained the ability to successfully implement the plant’s protective strategy. The plant was not at risk, because of the security redundancy we require,” said a regional NRC administrator.

Source: <http://www.miamiherald.com/business/story/389742.html>

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

## **Defense Industrial Base Sector**

7. *January 23, Defense News* – (National) **U.S. Navy could upgrade all Aegis ships with BMD.** The U.S. Navy is considering equipping all of its cruisers and destroyers with the capability to shoot down an enemy missile from sea, the director of surface warfare at the Pentagon said recently. By the end of 2009, the Navy plans to have 18 ships -- 15 destroyers and three cruisers -- fitted with the Aegis Ballistic Missile Defense (BMD)

system.

Source: <http://www.defensenews.com/story.php?F=3326889&C=america>

8. *January 23, Defense News* – (National) **DoD seeks 3 JLTV prototypes.** The U.S. Army-led Joint Light Tactical Vehicle program should give three industry teams 27-month contracts to develop prototypes as the effort moves to the technology development phase, according to a December 22 acquisition decision memorandum from the defense acquisition undersecretary. The program office will issue a request for proposal by month's end, said a Marine Corps spokesman January 23. The Army will lay out its 2010-15 spending plan in the Program Objective Memorandum that arrives next month. Low-rate initial production is slated for 2012, but could be moved up if prototyping suggests a way to do so, said a DoD pre-solicitation notice posted January 16. Interested companies and teams include Oshkosh and Northrop, BAE and Navistar International, General Dynamics and AM General, and Lockheed Martin.  
Source: <http://www.defensenews.com/story.php?F=3327915&C=america>

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

## **Banking and Finance Sector**

9. *January 24, New York Times* – (International) **\$7.1 Billion fraud uncovered at Société Générale.** The French bank Société Générale said Thursday that it had uncovered “an exceptional fraud” by a trader that would cost it about \$7.1 billion, and that it would seek new capital of about \$8 billion. The company, the second-largest listed bank in France, said in a statement that the fraud had been committed by a trader in charge of “plain vanilla” hedging on European index futures. The company also said it would write off \$3 billion from its exposure to derivatives linked to the U.S. mortgage market, including \$1.6 billion related to risks in residential housing and \$800 million related to U.S. bond insurance companies. It said it was also setting aside \$580 million in provisions against the risk that losses in those two areas would grow. There was some skepticism in the market about the trading fraud disclosure.  
Source:  
<http://www.nytimes.com/2008/01/24/business/worldbusiness/25socgen.html?em&ex=1201323600&en=1774c9bb72b09856&ei=5087%0A>
10. *January 23, WCPO 9 Cincinnati* – (Kentucky) **Old phone scam ringing once again in Northern Kentucky.** Police in Northern Kentucky want to warn residents about a phone scam. Scammers are posing as police officers calling with an emergency. The caller poses as an out of state police officer advising the recipient of a car accident. Then, the recipients are told to dial \*72 followed by another number for more information. What people do not realize is that \*72, forwards the call and allows the scammers to charge calls to the recipient's phone. Police believe they know where some of the scammers are located. Police have been in contact with officials in Cook County to track down the suspects. A spokesperson said people can easily deactivate call forwarding by dialing \*73. People should also double-check their phone bill to see if there are any collect calls or added charges due to the scam.  
Source: [http://www.kypost.com/content/wcposhared/story.aspx?content\\_id=7a05ebe1-](http://www.kypost.com/content/wcposhared/story.aspx?content_id=7a05ebe1-)

## **Transportation Sector**

11. *January 24, Post-Standard* – (National) **Educators fear that school buses could be targets.** In North Carolina, school bus drivers are being trained to spot suspicious activity and, in some districts, drivers peek under their buses every morning in search of anything odd. The president of a national group of school transportation directors and the transportation chief for the North Carolina Department of Public Instruction other school transportation leaders fear that the federal government is not taking their concerns about terrorism seriously. “The nation’s school bus system is the largest system of public transportation. It’s just very vulnerable. We’ve been concerned about that for quite some time.” The federal Transportation Security Administration has yet to begin a safety assessment that Congress ordered in August. Though the agency has poured billions of dollars into shoring up security for ports, railways, motor coaches, and the air industry in the past six years, it has done little for the millions of children who ride school buses, school leaders said. In August, legislation signed by President Bush gave the TSA a year to develop a national assessment of school bus security. The chairman of the House Homeland Security Committee and a committee member learned last week that the TSA has yet to develop a plan for how to go about the assessment. A spokesman for the TSA said the study would be completed on time.

Source: [http://blog.syracuse.com/news/2008/01/educators\\_fear\\_that\\_school\\_bus.html](http://blog.syracuse.com/news/2008/01/educators_fear_that_school_bus.html)

12. *January 23, Computerworld* – (National) **Southwest, American test in-flight Wi-Fi.** This week, Southwest Airlines Co. and American Airlines Inc. separately announced that they will test systems that offer passengers in-flight Wi-Fi data access. Both airlines would need Federal Aviation Administration approval before launching their Web services. Southwest announced today that it will test satellite-delivered broadband Internet access on four aircraft this summer. If the tests are successful and Southwest receives the FAA’s approval, passengers of the airline who have Wi-Fi-enabled devices would be able to access the Internet to check e-mail and surf the Web. However, “Southwest has not embraced voice calling” because of passengers’ concerns about cell phone calls made during flights, a spokeswoman said in an interview. “Voice is not a direction we’re taking.” Yesterday, American Airlines said that it had installed a broadband Internet connection on a Boeing 767-200 plane and that it will install and test the technology on 15 such aircraft throughout the year. American uses 767-200s primarily for transcontinental flights. Like Southwest, American plans to offer its passengers full data service but not cell phone or VoIP service. In September, Aircell announced plans to equip Virgin America planes with Wi-Fi access systems this year. JetBlue Airways Corp., Deutsche Lufthansa AG, and Qantas Airways Ltd. have also announced in-flight Wi-Fi in various forms.

Source:

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9058598&source=rss\\_topic15](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9058598&source=rss_topic15)

13. *January 23, Government Executive* – (National) **TSA reports progress in port identification card program.** According to the Transportation Security Administration's latest estimates, about 1.5 million workers at the nation's ports will have to carry a Transportation Worker Identification Credential (TWIC) card, double the initial estimate of 750,000. The program was established in December 2001 to tighten security at ports by requiring individuals to carry high-tech ID cards with biometric data to gain access to facilities and vessels. TSA has not issued regulations for when ports' shore-based facilities will be required to use TWIC cards, nor has the agency provided specifics for which sea vessels will require them for access. Also, while TSA recently published the technical specifications for the TWIC card readers, which it is now testing, no timeline has been provided for when approved readers will be installed at facilities. In the meantime, port attendants must check cards manually.  
Source: <http://www.govexec.com/dailyfed/0108/012308j3.htm>

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

## **Postal and Shipping Sector**

Nothing to report.

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

## **Agriculture and Food Sector**

14. *January 24, USAgNet* – (National) **New Era recall expanded for canned green beans and garbanzo beans.** The U.S. Food and Drug Administration (FDA) announced that New Era Canning Company, New Era, Michigan, is expanding its product recall because of potential *Clostridium botulinum* (*C. botulinum*) contamination to all canned green beans and garbanzo beans in #10 cans distributed by the company nationwide over the last five years. The affected cans are large institutional-sized containers, weighing approximately six and a half pounds. For specific brands and codes of green beans and garbanzo beans that are subject to this recall, consumers and retailers can access this information at the following link:  
<http://www.fda.gov/oc/opacom/hottopics/newera.html>. Please note that New Era produces canned products under other brand names and labels. Therefore, the recalled products may not necessarily be labeled with New Era's name. Also, the cans may bear a variety of product codes or no codes at all. Regardless of brand name or label, or the presence or absence of a code, the recalled cans should not be opened or used, and should be disposed of.  
Source: <http://www.usagnet.com/story-national.php?Id=196&yr=2008>

15. *January 23, USAgNet* – (Minnesota) **Bovine TB detected in ninth beef herd in Minnesota.** The Minnesota Board of Animal Health said Tuesday that a beef cattle herd in Roseau County has tested positive for bovine tuberculosis. The herd is the ninth in Minnesota where the disease has been confirmed. All cases have been in northwestern Minnesota. According to the Associated Press, the board said the U.S. Department of Agriculture is appraising the herd so it can be purchased and the animals killed.

Source: <http://www.usagnet.com/story-national.php?Id=176&yr=2008>

16. *January 23, Luminex Corporation* – (National) **Luminex, Tyson Foods to collaborate on new food safety, animal health tests.** Luminex Corporation and Tyson Foods, Inc. have reached a collaboration agreement to create faster, more accurate, and cost-effective food safety and animal health tests, the two companies announced Wednesday. Tyson is the world's leading producer and marketer of chicken, beef, and pork, while Luminex is the worldwide leader in multiplex solutions. "We believe it (the technology) will give us the flexibility to gather more testing data faster and develop and validate rapid testing options not currently available commercially." Tyson and Luminex's first collaboration is the development of an avian flock health monitoring panel.

Source: [http://www.agprofessional.com/show\\_story.php?id=50499](http://www.agprofessional.com/show_story.php?id=50499)

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

## **Water Sector**

17. *January 24, Oklahoman* – (Oklahoma) **Herbicide spill closes Lone Grove water supply.** City officials in Long Grove, Oklahoma, have completely shut down the municipal water supply after a handheld canister of a concentrated weed-killer cocktail was sucked into the system Wednesday afternoon. While officials with the water department say they believe the herbicides drained out of the system before making it to any customers, the Oklahoma Department of Environmental Quality is running tests and make sure the water system is safe. Until the Department of Environmental Quality renders the water supply safe; however, city residents are urged to not even turn their faucets on. Lone Grove schools canceled classes today because of the lack of water. The liquid herbicide mix entered the water system when a city worker was preparing to add water to an herbicide concentrate in a handheld sprayer. A water main broke somewhere south of the where the worker was getting ready to spray for weeds, she explained. Instead of releasing water, the line break caused a reverse in pressure that essentially sucked in the herbicide mix. The chemicals released in the system range from slightly toxic to possibly carcinogenic.

Source: <http://newsok.com/article/3196521/1201195366>

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

## **Public Health and Healthcare Sector**

18. *January 24, Reuters* – (International) **Experts probe high bird flu mortality rate in Indonesia.** Medical experts are worried about how death rates for H5N1 bird flu have shot up in places like Indonesia, and studies are being carried out to see if victims require higher dosages of drugs. "It could be they are treated later, or the virus is different, more virulent. There are many maybes, including differences in susceptibility of the virus," a doctor, who has treated bird flu victims in Vietnam, told Reuters on the sidelines of a bird flu conference in Bangkok. He said a major concern was the H5N1 variant in Indonesia appeared to be less susceptible to oseltamivir, the antiviral used to combat the disease. Studies are being conducted in Thailand, Vietnam, and Indonesia to

see if H5N1 patients need to be given higher dosages of oseltamivir. Details emerged on Thursday on how the virus had been passed from mother to foetus in the case of a pregnant 24-year-old Chinese woman who died of the disease in 2005. A leading scientist at Beijing University said the virus was detected in most organs of the foetus, including the brain.

Source: <http://www.reuters.com/article/europeCrisis/idUSB610075>

19. *January 23, Reuters* – (International) **Don't blame wild birds for H5N1 spread – expert.** There is no solid evidence that wild birds are to blame for the apparent spread of the H5N1 virus from Asia to parts of Europe, Africa, and the Middle East, an animal disease expert said on Wednesday. There was also no proof that wild birds were a reservoir for the H5N1 virus, said an international wildlife coordinator for avian influenza at the U.N.'s Food and Agriculture Organization at a bird flu conference in Bangkok. He stressed the need to focus attention on the poultry trade, and particularly smuggling, adding that these factors may instead be spreading and sustaining the deadly disease.

Source: <http://www.reuters.com/article/latestCrisis/idUSBKK319659>

20. *January 23, ABC News* – (National) **The great MRSA epidemic: Is it time to worry?** Flesh-eating bacteria, a drug-resistant menace, spreading silently through hospital hallways. But even as new research suggests that the disease may be spreading through the homosexual community -- and could even be developing into a full-blown epidemic -- health experts studying MRSA say panic over the disease may be premature. The director of clinical research in the department of emergency medicine at Brigham and Women's Hospital in Boston and his colleagues discovered that visits to emergency departments due to MRSA rose from 1.2 million in 1993 to 3.4 million in 2005. Community-acquired MRSA infections have become the number one cause of abscesses in otherwise healthy emergency room patients. But the official, whose study will appear in the upcoming issue of the journal *Annals of Emergency Medicine*, says that despite the confirmation that a MRSA epidemic is in full swing, the disease does not pose the level of disaster that the use of the term might suggest.

Source: <http://abcnews.go.com/Health/Germs/story?id=4172257&page=1>

---

## **Government Facilities Sector**

21. *January 24, Telegraph* – (Georgia) **Suspicious package at Robins closes two gates.** A suspicious package that led to the closure of two gates at Robins Air Force Base in Georgia on Wednesday afternoon turned out to be nothing, a base spokesman said. "Whenever we find something out of place, we label it as a suspicious package, and security measures are implemented," he said. People were evacuated from within the safety cordon established around the building where the package was found, he said. Base officials would not say what was in this package. "We don't want to divulge anything," the spokesman said. "It was an unsubstantial item."

Source: <http://www.macon.com/197/story/246740.html>

22. *January 23, KNBC 4 Los Angeles* – (California) **Portion of City Hall East evacuated after suspicious package found.** A bomb squad determined a package found in City Hall East in Los Angeles on Wednesday was not a threat, and employees evacuated from several floors of the 18-story building were allowed to go back to work, police said. A police bomb squad was sent to the building about 12:30 p.m. to check out the package, a Los Angeles police lieutenant said. Several floors were evacuated as a precaution. It was unclear what made the package suspicious or what was in it. Police said they had not received any threats regarding City Hall East.  
Source: <http://www.knbc.com/news/15121508/detail.html>

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

## **Emergency Services Sector**

23. *January 24, Huntington News* – (West Virginia) **Equipment stolen from Charleston could jam emergency communications.** The FBI has joined an investigation into the theft of electronic equipment after break-ins at several transmitting towers in Charleston, West Virginia. According to a Huntington TV station, ten break-ins at three separate sites resulted in the loss of a radio receiver/transmitter (repeater) and frequency counter. Charleston police asked the FBI to enter the investigation after they learned the stolen equipment could possibly be used to jam emergency frequencies. Thieves took only the specified equipment leaving other items untouched. Anyone with information about the break-ins should call (304) 348-6480.  
Source: <http://www.huntingtonnews.net/local/080124-rutherford-localequipmentstolen.html>
24. *January 23, Associated Press* – (New York) **FDNY unveils high-rise fire simulator.** Officials broke ground Wednesday on a simulator that will help firefighter trainees prepare to face a high-rise fire. The four-story, 4,000-square-foot space will be constructed atop an existing building and will include a dry standpipe system, mock elevators and stairways, and a mock fire command station. It will include layouts of residential, office, and commercial space. The training area will be able to simulate a fire and “flashover,” the moment when everything combustible in a space goes up in flames. There will be video hookups on each floor for teaching purposes. It is scheduled to be completed next year. At the groundbreaking ceremony, New York City’s mayor said the \$4.5 million simulator “will help train our members for one of the most notoriously complex parts of the job.” The city said that since 2004, more than \$60 million has been dedicated to improving the Fire Academy facilities. Last year, two firefighters died in an August blaze at the former Deutsche Bank building, a condemned 41-story skyscraper. In the 2001 terrorist attacks, 343 firefighters were killed in the collapse of the World Trade Center, whose twin towers stood at 110 stories. At the former Deutsche Bank building, a new fire suppression system will be able to detect a breach in the standpipe, officials said Wednesday. The standpipe, which supplies water to fire hoses, was broken when the fire occurred.  
Source:  
[http://news.yahoo.com/s/ap/20080123/ap\\_on\\_re\\_us/fdny\\_simulator;\\_ylt=AoZkg1pQJWtdZ\\_bgLQK3FEhG2ocA](http://news.yahoo.com/s/ap/20080123/ap_on_re_us/fdny_simulator;_ylt=AoZkg1pQJWtdZ_bgLQK3FEhG2ocA)

## **Information Technology**

25. *January 24, IDG News Service* – (National) **Windows Small Business Server at risk from critical flaw.** Microsoft said Wednesday that another one of its operating system products is susceptible to a critical vulnerability, first patched two weeks ago. In an update to its MS08-001 security bulletin, Microsoft said that the latest release of Windows Small Business Server was also critically at risk from a bug in Windows' networking software. The flaw is also considered critical for Windows XP and Vista users. Microsoft did not say why it had initially omitted Small Business Server from its list of critically affected operating systems, but it said that the product's users were being offered patches via Microsoft's various automatic update services. "Customers with Windows Small Business Server 2003 Service Pack 2 should apply the update to remain secure," Microsoft said in its updated bulletin. The bug lies in the way Windows processes networking traffic that uses IGMP (Internet Group Management Protocol) and MLD (Multicast Listener Discovery) protocols, which are used to send data to many systems at the same time. Microsoft said that an attacker could send specially crafted packets to a victim's machine, which could then allow the attacker to run unauthorized code on a system. Microsoft rates the flaw as "important" for Windows Server 2003, meaning that it would be more difficult for attackers to exploit the flaw on this operating system.

Source:

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9058759&taxonomyId=17&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9058759&taxonomyId=17&intsrc=kc_top)

26. *January 23, Computerworld* – (International) **U.S. Web site said to offer strengthened encryption tool for al-Qaeda backers.** An Arabic-language Web site hosted on a server located in Tampa, Florida, is apparently offering a new version of software that was designed to help al-Qaeda supporters encrypt their Internet communications. The new encryption tool is called Mujahideen Secrets 2 and appears to be an updated version of easier-to-crack software that was released early last year, said the vice president of technology evangelism at Secure Computing Corp. The tool is being distributed free of charge on a password-protected Web site that belongs to an Islamic forum known as al-Ekhlaas, according to Secure Computing and a blog posting by the Middle East Media Research Institute. MEMRI is a Washington-based organization that monitors what it describes as jihadist Web sites and publishes translations of online content originally posted in Arabic, Persian, or Turkish. The vice president said that he contacted the FBI about the al-Ekhlaas site and its contents last weekend. But as of Wednesday afternoon, the site was still up and running. A Reuters story posted January 18 and datelined Dubai, quoted the al-Ekhlaas Web site as saying that the new release was a "special edition" of the encryption tool created "in order to support the mujahideen in general and the Islamic State in Iraq in particular." That organization was described by Reuters as being linked to al-Qaeda. Efforts by groups that support al-Qaeda to develop their own encryption tools appear to be driven by concerns about possible back doors being built into publicly available encryption software, the Secure Computing representative said.

He added that the upgraded Mujahideen Secrets tool could cause problems for law enforcement and antiterrorism agencies that are tracking the activities of such groups.

Source:

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=17&articleId=9058619&intsrc=hm\\_topic](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=17&articleId=9058619&intsrc=hm_topic)

### Internet Alert Dashboard

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/>.

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

## Communications Sector

27. *January 24, Burlington Free Press* – (Vermont) **Rural towns bundling a blueprint for broadband.** Using Burlington Telecom’s municipal broadband network as a model, 22 rural Vermont towns are poised to pool their resources and launch a fiber-optic project that could go online by the end of 2009. Members of the East Central Vermont Community Fiber Network announced Wednesday that formal agreements are in the works from Windsor to Montpelier that would bring the strength of numbers -- and attractive financing -- to universal broadband Internet coverage. The group’s leadership presented the project at a board meeting of the Vermont Telecommunications Authority held Wednesday. The presenters made no funding requests, but asked the state board for support with credit and regulatory hurdles. The chairman of the Strafford Selectboard said commercial broadband providers could not meet the needs of rural Vermonters. “These fiber-optic connections are absolute necessities; not luxuries,” he said. “We need them for our economical and cultural development.” More than 1,000 residents in his area have registered for service, he said. About half of the population targeted by the East Central Vermont Community Fiber Network has no broadband service. Earlier attempts to serve rural areas with broadband, including state-funded pilot wireless systems, have fallen short of fiber-optic’s technical advantages. The East Central Vermont Community Fiber Network, said one participant, would permit an “overlay” of wireless coverage that could accommodate data or voice transmissions.

Source:

<http://www.burlingtonfreepress.com/apps/pbcs.dll/article?AID=/20080124/NEWS02/801240322/1007>

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

## Commercial Facilities Sector

28. *January 23, Associated Press* – (Maryland) **Rocket in Maryland museum 2 years was no dud.** A rocket on display at a veterans’ museum in Maryland for two years was discovered Wednesday to be live. After Allegany County authorities were notified that

the Mark 1 rocket on display in Cumberland might be live, the state fire marshal's office and the FBI confirmed it was. Bomb experts removed the ordnance and rendered it safe. The 48-inch-by-2.75-inch rocket was similar to those used on helicopter gun ships during the Vietnam War, said the Deputy State Fire Marshal. A local veteran donated it to the museum. Authorities are investigating how the man came to possess the live ordnance.

Source: <http://ap.google.com/article/ALeqM5iUFCIPE-aEbw5edJ1hJDMxd1JekwD8UBUQPO3>

29. *January 23, KTBC 7 Austin* – (Texas) **Georgetown Wal-Mart evacuated after suspicious device found.** The Super Wal-Mart in Georgetown, Texas, is back to normal after it was evacuated when a suspicious device was found in the portrait studio of the store Tuesday afternoon. After investigation by the Austin Police Bomb Squad, the device was found to be an aerosol can with wires coming out of it. Georgetown Police said Wednesday that an employee reported the device to the store manager. Dozens of customers and employees were evacuated into the parking lot during the investigation. An Austin Bomb Squad robot X-rayed the device and found it to not be explosive.

Source:

<http://www.myfoxaustin.com/myfox/pages/News/Detail?contentId=5570139&version=6&locale=EN-US&layoutCode=TSTY&pageId=3.2.1>

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

## **National Monuments & Icons Sector**

30. *January 24, USA Today* – (National) **National parks robbed of heritage.** Looting of fossils and archaeological artifacts from national parks is increasing as demand for such items rises on the Internet and the world market, U.S. National Park Service officials say. Over the past decade, an average of 340 “significant” looting incidents have been reported annually at the 391 national parks, monuments, historic sites, and battlefields — probably less than 25 percent of the actual number of thefts, says a park service staff ranger. “The trends are up,” he says. The park service has 1,500 law enforcement rangers and 400 seasonal law enforcement rangers — one for about every 56,000 acres. “We really don’t have enough manpower,” he says. That can make it difficult to catch criminals such as the three men who dug 460 holes at the Fredericksburg-Spotsylvania military park in search of artifacts and the man who pleaded guilty to taking 252 relics last year from Colorado’s Mesa Verde National Park.

Source: [http://www.usatoday.com/news/nation/2008-01-23-looting\\_N.htm](http://www.usatoday.com/news/nation/2008-01-23-looting_N.htm)

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

## **Dams Sector**

31. *January 24, Associated Press* – (Florida) **Work crews try to shore up levee around Lake Okeechobee.** Work crews are cutting into the dike around Lake Okeechobee in a renewed push to protect South Florida from catastrophic flooding. The crews will build a wall through the middle of the earthen levee surrounding the lake. The wall is meant to

stop erosion that could lead to a breach in the levee that holds back the 730-square-mile lake. The U.S. Army Corps of Engineers has identified Lake Okeechobee's Herbert Hoover Dike as one of the country's most at-risk dams. Concerns about the levee have forced South Florida water management officials to keep the lake lower than normal. That is not helping a water shortage due to two years of drought. Work on the first section of the levee wall, from Port Mayaca to Belle Glade, is expected to continue until 2013. It is considered the dike's most vulnerable section.

Source: <http://www.wwsb.com/Global/story.asp?S=7766396>

32. *January 23, KLTV 7 Tyler* – (Texas) **Inspection results in on what caused East Texas dam to break.** The Texas Commission on Environmental Quality's inspection of the dam at Rhines Lake, which failed earlier this month, shows the failure was apparently caused by piping in the dam: seepage and leaks had been occurring for a while, small trees and brush were found along the slope of the dam and in the joints, and there were also erosions in the concrete. Similar findings were noted the last time the dam was inspected, and the dam was found to be in "fair to good" condition back in 1984. "When an inspection is done, they assess risk, and the higher the risk, the more frequent an inspection would occur," said a representative with the regional TCEQ office in Tyler. "In their previous inspection, they considered it low risk." TCEQ reports there are more than 400 public and private dams in East Texas, most of which are rated as "low risk."  
Source: <http://www.kltv.com/Global/story.asp?S=7764721>

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

## DHS Daily Open Source Infrastructure Report Contact Information

**DHS Daily Open Source Infrastructure Reports** – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

## DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to <a href="mailto:NICCReports@dhs.gov">NICCReports@dhs.gov</a> or contact the DHS Daily Report Team at (202) 312-5389
Distribution Information:	Send mail to <a href="mailto:NICCReports@dhs.gov">NICCReports@dhs.gov</a> or contact the DHS Daily Report Team at (202) 312-5389 for more information.

## Contact DHS

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).

## **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.