



Department of Homeland Security Daily Open Source Infrastructure Report for 16 May 2008

Current Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](#)

- New Scientist reports Core Security has discovered a serious vulnerability in a software package called Suitelink that is widely used to automate the operation of power stations, oil refineries, and production lines. (See item [3](#))
- According to SkyNews, Swiss police say Al Qaeda is planning to attack the Euro 2008 football championships in Switzerland and Austria in June. (See item [36](#))

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. *May 15, Reliable Plant* – (Massachusetts) **OSHA cites Dominion Energy following explosion.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has cited Dominion Energy New England for alleged serious violations of safety standards following a November 2007 steam explosion at the Salem Harbor Power Station that killed three employees. OSHA's investigation found that the company failed to take effective steps to protect employees against the hazards of burns and other bodily injuries from hot ash and steam as a result of ruptured or leaking boiler tubes and piping. Specifically, the boiler's lower vestibule/dead air space area, where the rupture occurred, had not been entered or inspected in more than nine years, and entry had been prevented by the accumulation of ash and debris over that period of time.

OSHA's inspection also identified several other hazards not directly related to the explosion. Dominion Energy New England was issued a total of ten serious citations carrying a total of \$46,800 in proposed fines, and has 15 business days from receipt of its citations to meet with OSHA or to contest its citations and fines.

Source:

<http://www.reliableplant.com/article.asp?pagetitle=OSHA%20cites%20Dominion%20Energy%20following%20explosion&articleid=11920>

2. *May 14, Reuters* – (California) **Southern California faces summer power challenge: NERC.** Southern California's electricity system will be challenged this summer, and power emergencies may result if an extended drought leads to massive wildfires, the main U.S. electricity reliability watchdog said on Wednesday. Southern California is the area that most concerns analysts at the North American Electric Reliability Corp. (NERC), which on Wednesday issued its summer 2008 outlook. Of southern California, NERC said, "capacity margins will remain tight. Significant amounts of imported power are required to fortify capacity margins and preserve reliability, resulting in heavily loaded transmission lines into this area during peak conditions." "As a result, unplanned major transmission or generation outages, or extreme temperatures/demand may lead to resource constraints." NERC said voluntary conservation and on-call interruptible loads will likely be necessary more often than usual this summer.

Source: <http://www.reuters.com/article/domesticNews/idUSN1451329920080514>

3. *May 14, New Scientist* – (National) **Power plants open to hacker attack.** Power plants could be sabotaged by a simple internet attack that shuts down their control systems. Core Security has discovered a serious vulnerability in a software package called Suitelink that is widely used to automate the operation of power stations, oil refineries, and production lines. This could allow attackers to crash Suitelink by sending an outsize data packet to a certain port on the computer running the program. Suitelink's maker, Wonderware, has since issued a software patch to plug the security gap. Core had only just begun examining this kind of supervisory control and data acquisition program when it found the problem. This may mean that more vulnerabilities are still hidden in software of this type.

Source: <http://technology.newscientist.com/channel/tech/electronic-threats/mg19826566.200-power-plants-open-to-hacker-attack.html>

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

Chemical Industry Sector

Nothing to Report

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

Nuclear Reactors, Materials, and Waste Sector

4. *May 15, Patriot Ledger* – (Massachusetts) **Plymouth power plant union puts off tally of strike vote.** Members of the Utility Workers Union of America Local 369 have voted

whether or not to authorize a strike at the Pilgrim nuclear power plant, but union officials opted against immediately tallying the vote as a show of good faith in the negotiations. Union officials said they expected overwhelming support to authorize a potential strike if a new contract cannot be reached by the time the current one expires at the end of the day Thursday. But they decided to wait to tally the results of the vote because they wanted to signal a willingness to work with plant owner Entergy Corp. now that a federal mediator is involved in the talks. On Wednesday, Local 369 petitioned the U.S. Nuclear Regulatory Commission to order Entergy to close Pilgrim if there is a work stoppage at the plant later this week. The union maintains that many of the replacement workers are unfamiliar with specific aspects of the power plant.

Source: <http://www.enterpriseneews.com/news/x1880506047/Plymouth-power-plant-union-puts-off-tally-of-strike-vote>

5. *May 15, Boston Globe* – (Massachusetts) **Razing urged for waste site.** Federal environmental officials are recommending that all buildings at the Starmet Corp. hazardous waste site in Concord, also known as the Nuclear Metals Superfund Site, be demolished because they are highly contaminated with depleted uranium and other hazardous substances and could pose a safety threat. Starmet and two other affiliated companies specializing in metal operations still do business on the site, employing 30 to 40 people there. The Environmental Protection Agency's recommendation is based on an engineering evaluation and cost-analysis study, which found contamination on rooftops, interior walls, and floors, and on machinery and heavy equipment in the buildings. The study also found that the buildings are deteriorating and in poor condition. The EPA is removing containers of flammable and hazardous substances from the buildings that present a risk of fire or explosion, and is overseeing a remedial investigation and feasibility study at the site to evaluate the extent of contamination, the risks posed by the contamination, and the cleanup options. Demolishing and disposing of the waste would cost an estimated \$64 million.

Source:

http://www.boston.com/news/local/articles/2008/05/15/razing_urged_for_waste_site/

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

Defense Industrial Base Sector

6. *May 15, USA Today* – (National) **Enemies securing U.S. night-vision gear.** Thefts and illegal exports of advanced military night-vision gear are rising sharply and U.S. officials say some of the equipment has reached enemies in Afghanistan and Iraq, where it could erode the advantage U.S. troops have in after-dark combat. The government has prosecuted more than two dozen businesses and individuals over the past 18 months for stealing night-vision gear or skirting prohibitions on foreign sales, according to a USA Today review of federal documents and public records. The newspaper also identified at least eight more cases under investigation. The Pentagon joined the departments of Justice, Homeland Security, Commerce, and State last year in a crackdown on illegal exports of combat-use military items and sensitive civilian goods with military uses. Night-vision goggles, scopes, and cameras used by U.S. troops account for more cases than any other technology.

Source: http://www.usatoday.com/news/military/2008-05-14-nightvision_N.htm

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

Banking and Finance Sector

7. *May 14, Associated Press* – (National) **Woman charged in scam after stealing \$18M.** A California woman is facing criminal and civil charges in connection to a real estate scam that targeted black investors in three states, bilking hundreds of them out of \$18 million, authorities said Wednesday. A federal grand jury in Los Angeles returned an 11-count indictment against her charging her with wire fraud, mail fraud and money laundering, the U.S. attorney's office said. The woman and her Pasadena-based company, Accelerated Funding Group, also are charged with several violations of U.S. securities laws, according to a civil complaint filed against her and the company by the Securities and Exchange Commission. Authorities claim the suspect lured investors in California, Nevada and Georgia into investing in her company, which purported to use the funds to help homeowners in default get current on their mortgage payments. Investors were promised their investments would grow by as much as 50 percent within a matter of days. Instead, the scammer was running a scheme that paid off early investors with more recent investors' money, authorities said. The scheme ended up snaring more than 600 investors between 2005 and 2007.
Source: http://www.usatoday.com/news/nation/2008-05-14-realestate-scam_N.htm

8. *May 14, IDG News Service* – (National) **S.E.C. moves toward requiring interactive data filings.** The U.S. Securities and Exchange Commission has taken a major step toward requiring publicly traded companies to submit their reports to the agency in an interactive data format, with backers saying the change will make financial reports easier to analyze. All three SEC members voted to publish a proposal that would require public companies to file reports in eXtensible Business Reporting Language, or XBRL, a programming language related to XML that is being developed by a nonprofit consortium of about 450 companies. Under the proposal, which still needs final approval from the SEC after a public comment period, the transition from text and HTML reports to XBRL would take three years, with about 500 of the largest U.S. and foreign companies required to start filing XBRL reports after December 15. The smallest public companies and foreign companies not using U.S. generally accepted accounting principles (GAAP) could wait until the third year to file reports in XBRL. The SEC chairman said the change will make SEC reports easier to read and analyze. With XBRL, companies will use XML data tags to describe financial information in the SEC's online Edgar database. The SEC's move to XBRL, which follows similar efforts in other countries including Japan and China, has faced some criticism. Some companies have suggested the cost may not be worth the benefits.
Source:
http://www.nytimes.com/idg/IDG_852573C400693880002574490039DDA3.html?ref=technology

9. *May 14, Associated Press* – (National) **SEC charges Broadcom co-founders in stock options probe.** Federal officials on Wednesday charged Broadcom Corp.'s co-founders

with falsifying the company's reported income, which led to what is believed to be the largest accounting restatement to date because of backdating stock options. A civil complaint filed by the Securities and Exchange Commission (SEC) also charges a former chief financial officer and a general counsel. The four men are accused of violating federal securities laws by misrepresenting the dates on which stock options were granted to its executives and employees. The SEC said that as a result of the scheme, Broadcom restated its financial results in January 2007 and reported more than \$2 billion in additional compensation expenses. "This egregious misconduct resulted in the largest accounting restatement to date arising from stock option backdating and warrants the significant sanctions sought from these individuals," said the director of the SEC's Division of Enforcement. Backdating stock options involves retroactively setting the exercise price to a low point in the stock's value to increase profits for an executive or employee when shares are sold. If companies backdate options without properly disclosing and accounting for the move, it can cause profits to be overstated and taxes to be underpaid.

Source:

http://ap.google.com/article/ALeqM5iPee_KUjXz2Z_pTc5qJ1FLkQPaowD90LLKD80

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

Transportation Sector

10. *May 14, AVweb* – (National) **NTSB: Pilots need better information about turbocharger failures.** The emergency procedures provided to pilots for coping with turbocharger failures in flight are inadequate, the National Transportation Safety Board (NTSB) said, and the Federal Aviation Administration should require manufacturers to revise pilot operating handbooks. In a fatal crash in May 2004, the NTSB says, the turbocharger failed on a Cessna T206H, and investigators found that in-flight emergency procedures in the POH did not provide a way to assess the difference between an engine and a turbocharger failure. The POH also did not provide any clear guidance about how to handle such a failure once a pilot identified the problem. Manufacturers of aircraft equipped with turbochargers still have not voluntarily improved emergency procedures for turbocharger failures, and accidents and incidents continue to occur, the NTSB says.
Source:

http://www.avweb.com/avwebflash/news/NTSBSaysPilotsNeedBetterInformation_AboutTurbochargerFailures_197869-1.html

11. *May 14, AVweb* – (National) **FAA says emergency medical helicopters need safety improvements.** Three men died last weekend when an emergency medical-services helicopter crashed near Madison, Wisconsin, and this week the Federal Aviation Administration (FAA) responded with an update on its work to address safety concerns about such flights. The National Transportation Safety Board reported on the helicopter emergency medical services fleet in 2006, and asked the FAA to impose stricter requirements on all such operators. The agency said it is focusing on better training for flight crews; encouraging the use of technology such as night-vision goggles, radar altimeters, and terrain awareness and warning systems (though such systems do not work optimally in helicopters, the FAA says); and more detailed, airline-type FAA

oversight for operators. “Safety improvements are needed,” the FAA said.

Source:

http://www.avweb.com/avwebflash/news/FAASaysEmergencyMedicalHelicoptersNeedSafetyImprovements_197867-1.html

12. *May 14, Examiner* – (California) **Name mix-up slips by airport security.** A passenger walked right past several checkpoints at San Francisco International Airport (SFO), showing identification to at least three security screeners along the way, and was allowed on the plane with relative ease — without a legitimate boarding pass. The incident happened Wednesday night aboard a United flight from SFO to John F. Kennedy Airport in New York. The man said he was issued a boarding pass meant for a person with a different name. None of the airline and screening agents noticed or questioned that his identification did not match his ticket, he said. Even a scanner at the United gate alerted an airline employee that something was wrong with the passenger’s boarding pass, he said. But the employee decided to override the computer and allow him to board the plane, he said. Once on the plane, the passenger informed a flight attendant of the apparent mix-up and she discovered the airline had issued two of the same boarding passes, both under the wrong name. She called the man a “security breach” and asked him to disembark the plane immediately, he said. United officials eventually fixed the error and allowed him back on the flight, he said. According to the Transportation Security Administration (TSA), the man was never a security breach. He and his baggage were checked for weapons and drugs as he passed through the checkpoints and he was not an imminent threat, said a TSA spokesman.

Source: http://www.examiner.com/a-1390304~Name_mix_up_slips_by_airport_security.html?cid=temp-popular

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

Postal and Shipping Sector

13. *May 15, WPVI 6 Philadelphia* – (Pennsylvania) **Giant bugs found in mail.** Large insects, some measuring a half-foot in diameter and all considered harmful to agriculture in the U.S., were found in a package after postal workers thought they heard the parcel making noises. In all, 26 beetles were in the package that was originally sent to Mohnton, Pennsylvania. The package was labeled as containing “toys, gifts and jellies,” according to the U.S. Customs Service, but postal officials in Mohnton thought they heard something alive inside. When the package was sent to Philadelphia, it was frozen by agriculture specialists. They X-rayed the package and found smaller containers holding the bugs inside. The package was shipped from Taiwan. Officials said some of the smaller containers inside the package were labeled with the symbols for male and female, and that might have been a sign that someone was intending to breed the beetles. It is illegal to ship live beetles into the U.S. without a permit.

Source: <http://abclocal.go.com/wpvi/story?section=news/bizarre&id=6142327>

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

Agriculture and Food Sector

14. *May 15, USAgNet* – (North Dakota) **ND drought task force urges water program activation.** The North Dakota State Water Commission voted Wednesday to put \$1 million into the Livestock Water Supply Assistance Program. The action followed a drought advisory panel’s recommendation that the commission immediately implement the program to help producers get water for their livestock. “The Livestock Water Supply Assistance Program offers financial assistance for producers to improve water systems in pastures or to bring water to grazing areas,” said the agriculture commissioner, who chaired the meeting of the Agricultural Task Force, created under the state’s Drought Mitigation Plan. The meeting of the task force was the first for the group since the governor of North Dakota declared an early-phase agricultural drought emergency last Friday.
Source: <http://www.usagnet.com/story-national.php?Id=1169&yr=2008>
15. *May 15, Reuters* – (National) **U.S. chicken industry may face \$8 corn – Pilgrim CEO.** The U.S. chicken industry, which has been cutting production in reaction to higher feed costs, may have to contend with even higher feed prices this year, said Pilgrim’s Pride Corp.’s chief executive on Thursday. “I think today the industry is thinking in terms of placing (chickens) for \$6 corn when I think we should realize the potential for \$8 corn is certainly there and I think we should be in a position to deal with that,” he said. Pilgrim’s Pride recently announced it was cutting production about five percent, largely in reaction to higher feed costs. To cope with higher feed costs, he said he would like to see a three to four percent reduction in U.S. chicken production. Recently the industry has reduced by two to three percent the number of eggs and young chicks placed in the production cycle, but it will be early this summer before that reduced supply reaches grocery stores.
Source: <http://www.reuters.com/article/marketsNews/idUSN1529681420080515?pageNumber=1&virtualBrandChannel=0>

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

Water Sector

16. *May 15, Associated Press* – (Michigan) **Michigan Legislature approves Great Lakes pact.** After months of waiting, the Michigan Legislature on Wednesday unanimously approved a regional compact to prevent Great Lakes water from being sent to thirsty regions. But the legislation will not head to the governor for her signature until Democrats and Republicans resolve differences over large-scale water withdrawals from Michigan’s lakes and waterways. All eight states adjoining the Great Lakes must ratify the 2005 compact for it to take effect. It has been approved by four, and the Wisconsin Legislature was working to sign off Wednesday night. Congress also must give approval. Bills endorsing the compact won passage in the Republican-led Michigan Senate and Democratic-controlled state House. They now trade places in both chambers. They are tied, however, to more contested legislation regulating water withdrawals,

pitting the environmental and conservation communities against the business community and Democrats against Republicans. The package cannot become law unless every bill is signed. The accord is a preventive measure to stop outsiders from staking a claim to Great Lakes water, as other areas in the U.S. struggle with drought conditions. With limited exceptions, the compact would prohibit diverting water from the lakes and the rivers linking them, which together hold nearly 20 percent of the world's fresh surface supply. The rules could affect virtually anything requiring lots of water, from sewage treatment to irrigation to manufacturing cars.

Source:

http://www.mlive.com/news/index.ssf/2008/05/michigan_legislature_approves.html

17. *May 14, Forbes* – (National) **The water-industrial complex.** In 2001, a water shortage in America's Pacific Northwest wiped out nearly a third of the U.S. aluminum industry. Low precipitation levels in the Cascade Mountains during the preceding winter robbed local reservoirs of the water needed to turn the massive turbines inside the region's main hydroelectric power plant, the Bonneville Power Administration. Electricity prices skyrocketed. Over the course of a few months, roughly a dozen aluminum plants closed. Nearly a decade later, only one has reopened. Like oil, water is an essential part of doing business in almost every industry, and unexpected shortages can trigger potentially catastrophic consequences. The trouble for investors: Companies disclose very little if any information about their exposure to water-related risks. "This is not an area that companies like to discuss quite frankly," says an economist at J.P. Morgan and the principal author of the recent report *Watching Water: A Guide to Corporate Risk in a Thirsty World*. "They don't want to call attention to a vulnerability and that applies very much to the water scarcity issue. Investors in general know very little about what is going on in companies' supply chains." "Watergy," as some are now calling it, is a very big deal for all industries. In the U.S., industry uses more water than agriculture thanks to its use in power generation. The industrial sector uses an estimated 45 percent of water in the U.S.; agriculture accounts for 42 percent; and domestic uses account for a mere 13 percent. Worldwide, agriculture uses about 70 percent of all water.

Source: http://www.forbes.com/home/2008/05/13/water-electricity-industry-biz-energy-cx_bp_0514water.html

18. *May 14, KMGH 7 Denver* – (Colorado) **Drilling begins at Leadville mine.** The Environmental Protection Agency (EPA) began drilling a relief well into a mine drainage tunnel Wednesday in an effort to stop a potentially catastrophic wave of contaminated water from flooding the town of Leadville, Colorado. The tunnel lies approximately 350 feet below ground and contains an estimated 500 million to one billion gallons of water that has become trapped behind various blockages over the past decades. Drilling the relief well is expected to take two to three weeks, and the installation of a pump will follow. The EPA estimates the well will be operational by mid-June. Water pumped from the well will be transported via a pipeline to a water treatment plant operated by the U.S. Bureau of Reclamation, which has agreed to treat the water before it is released into the Arkansas River.

Source: <http://www.thedenverchannel.com/news/16266062/detail.html>

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

Public Health and Healthcare Sector

19. *May 14, Washington Technology* – (National) **Better security needed for events.** The federal government must develop an effective national biosurveillance system and a national medical-intelligence program to counteract the risk of biological threats during mass gatherings, according to a new congressional report. The report recommended, among other things, the creation of a National Medical Intelligence Program to share information among medical providers and law enforcement authorities. Federal attempts to create a national system to track diseases have been largely unsuccessful so far, according to the report. Some such tracking is done by various programs in each state. The current federal tracking system is BioSense, which is operated by the Centers for Disease Control and Prevention. It consists of information technology networks allowing sharing of information among states and with federal authorities, and it allows for data mining to detect disease trends and patterns. To improve the system, additional funding is needed for technologies, which must be applied in a systematic fashion, the chairman of the Homeland Security Committee said.

Source: http://www.washingtontechnology.com/online/1_1/32807-1.html

20. *May 14, Reuters* – (International) **Bird flu pandemic seen needing multiple drugs.** Governments need to stockpile different sorts of flu drugs – not just Roche Holding AG’s Tamiflu – to counter the danger of resistance in a pandemic triggered by bird flu, British experts said on Wednesday. The warning could boost demand for GlaxoSmithKline Plc’s inhaled medicine Relenza, which has been largely overlooked in favor of Roche’s more convenient pill. Scientists analyzing the structure of a key flu virus protein found that both H5N1 and seasonal flu could develop resistance to Tamiflu, while still remaining highly susceptible to Relenza. There is also “a huge imperative” to develop further drugs since the best way to treat patients in the long term is likely to be a three- or four-pronged approach, similar to the multi-drug cocktails used to fight HIV and AIDS, said a researcher with the National Institute for Medical Research in London. Two older flu drugs are available but flu viruses have quickly developed resistance to them, although some experts believe they may be useful in cocktails with newer drugs. Both flu viruses and HIV have a high rate of mutation, which allows them to adapt to the treatments devised to tackle them.

Source: <http://www.reuters.com/article/healthNews/idUSL1393725920080514>

21. *May 13, China Daily* – (International) **Medics trained to deal with terrorist attacks.** Health professionals in Beijing are being trained to deal with the aftermath of terrorist attacks, the municipal health bureau said Monday. Some 130,000 medics are taking part in the scheme to ready them for possible incidents during the Olympics and Paralympics, the bureau said on its website. Medics will be taught about nuclear, biological, and chemical attacks, response and rescue procedures, and treatment, the bureau said. The training began on Monday and will run for a month. The bureau’s Party secretary said health organizations should also be on high alert to the possibility of terrorist groups attempting to steal potentially deadly chemicals, drugs or other toxic materials. Interpol has also warned of the threat of possible attacks by groups such as al-Qaeda during the Games.

Government Facilities Sector

22. *May 15, Associated Press* – (District of Columbia) **Preservation group lists endangered places in DC.** The D.C. Preservation League’s annual list of endangered places in the city includes the public school system’s entire inventory of buildings. The group says years of deferred maintenance have left many school buildings in an advanced state of disrepair. Ten sites are on this year’s list, including the Walter Reed Army Medical Center, the Georgetown streetcar tracks, and the west campus of St. Elizabeths Hospital. The selections were made by city residents.
Source: http://www.examiner.com/a-1392529~Preservation_group_lists_endangered_places_in_DC.html
23. *May 14, Washington Post* – (Maryland) **‘Bottle bombs’ explode in Pr. George’s high school.** Two Prince George’s County, Maryland, high school students were arrested today after two chemical “bottle bombs” exploded in their school’s hallways this morning, injuring no one, but disrupting the day, a county schools official said. One of the bombs burst in a hallway at Friendly High School about 9:15 a.m., a school system spokesman said, prompting a call to the fire department. After the first incident had been cleaned up, a second bomb exploded in the hallway near the administrative office about 10 a.m., he said. Following the second explosion, all students were sent to the football field as firefighters looked for additional devices. They returned to class by 12:45 p.m. Both bombs were crude devices made from plastic bottles, toilet cleaner, and an activating agent. Videos depicting such bombs’ construction and their use are widely available on YouTube and other Web sites. Such bombs are not particularly deadly, but they can injure those standing nearby. Last week, a student allegedly set off a similar device at Crossland High School. He was charged with possessing an explosive device and reckless endangerment.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/05/14/AR2008051401981_pf.html

Emergency Services Sector

24. *May 15, IPextreme Inc.* – (National) **Pantel and IPextreme to develop reliable 911 emergency dispatch for VOIP phone users.** Pantel International Inc. – a manufacturer of radio communication equipment, specializing in console and control systems for police, fire, and ambulance agencies – and IPextreme® Inc. – the company bringing famous intellectual property to system-on-chip designers worldwide – today jointly announced the establishment of a strategic development initiative addressing the problem of automatic location of 911 emergency calls within an Internet protocol (IP) telephone network built on a ColdFire microprocessor platform. This initiative will enable emergency calls placed using Voice over IP (VOIP) telephone services to be

properly located based on the geographic location of the call. Currently, emergency calls placed using VOIP services are not automatically dispatched to the physical location of the call, but rather to the address listed on the caller's account. The ELI (Emergency Location Informant) is an innovative IP appliance that will enable the dispatch center to immediately identify the physical location of the call correctly, thus ensuring that first responders are directed to the proper location.

Source: <http://biz.yahoo.com/bw/080515/20080515005664.html?.v=1>

25. *May 15, KIFI 8 Idaho Falls* – (Idaho) **Radioactive spill drill in Blackfoot.** The Shoshone-Bannock tribes in Idaho planned an emergency management and response exercise to help train members on a hazardous materials situation. “The purpose was to practice unified commands through planning and a lot of agencies working together,” said the Interim Emergency Manager for Shoshone-Bannock Tribes. Firefighters, members of the Homeland Security, along with state and county emergency crews participated. The agencies participated in a lessons learned session Wednesday afternoon where they discussed what to change if a radioactive spill was to actually happen.

Source: http://www.localnews8.com/Global/story.asp?S=8326064&nav=menu554_2_1

26. *May 14, Billings Gazette* – (Montana) **‘Traumatic’ drill prepares emergency agencies for airport crisis.** The emergency drill at Billings Logan International Airport was more realistic due to about 60 Billings students – made up to appear as airplane crash victims – who were on the airport's training plane. The drill involved both Billings hospitals and about every emergency agency in town. The scenario was that a plane could not lower its front landing gear, said the supervisor of the airport firefighting squad and incident commander for the drill. Just like in a real situation, time was allotted for the plane to circle the airport a few times and try to fix the problem, he said. In the drill, however, the nose gear would not release. The plane landed, slid off the runway, and came to an abrupt stop, tossing the mock passengers forward and injuring them.

Source: <http://www.billingsgazette.net/articles/2008/05/14/news/local/20-airportdrill.txt>

27. *May 14, Associated Press* – (National) **Emergency network plan revived.** The Federal Communications Commission (FCC) agreed unanimously Wednesday to try again to create a nationwide emergency communications network after an earlier plan failed to attract sufficient support from private investors. The initial plan, approved last summer, would have used publicly owned spectrum to attract a private investor that would bear the cost of the network. The network would be used by police officers, firefighters, and other emergency crews responding to disasters or terrorism attacks. The commission wants public input on how to modify the plan to make it more attractive to the private sector. It is also asking whether the concept should be abandoned altogether and the public airwaves dedicated to the network be auctioned to the highest bidder for commercial use. Under the original plan, the agency set aside a swath of airwaves for auction to a commercial bidder that would be combined with a roughly equal portion of spectrum controlled by a public safety trust to create a shared emergency communications network. The winning bidder, in exchange for use of the public safety spectrum, would build the network and make a profit by selling access to wireless

service providers. The public safety spectrum failed to attract the minimum bid of \$1.3 billion required to award the license. Potential bidders quoted in an FCC investigative report said the failed plan lacked specificity and created too much risk for investors. Ideally, a new network would help solve the problem of public safety organizations not being able to communicate with one another and avail emergency personnel of many of the advances in wireless technology that are available to commercial users. Commission estimates on how much a national network might cost have ranged from \$6 billion to \$7 billion, but private sector estimates are more than double that amount.

Source: http://www.examiner.com/a-1390895~Emergency_network_plan_revived.html

28. *May 14, Congress Daily* – (National) **FEMA under fire for slow progress on new alert system.** House lawmakers Wednesday took aim at the Federal Emergency Management Agency's (FEMA) effort to modernize the nation's emergency alert system, saying progress has been too slow and legislative action may be needed to pressure the agency to work faster. Lawmakers expressed frustration that FEMA has not moved quickly enough to develop the so-called Integrated Public Alert and Warning System, which eventually will allow alerts to be sent via e-mail, cell phones, and hand-held devices. In a separate action, two members of the House Transportation and Infrastructure Committee introduced legislation that would establish standards and requirements that FEMA must meet for the new system. The Homeland Security Department was given responsibility to develop the system under a 2006 executive order.

Source: <http://govexec.com/dailyfed/0508/051408cdpm2.htm>

29. *May 14, WGHP 8 Greensboro* – (North Carolina) **Car bomb simulation will help Greensboro prepare for terrorism.** Police, fire, and rescue teams will practice coordination of efforts in response to a simulated car bomb on Thursday in Greensboro, North Carolina. Although simulated, the incident will look real, according to the officer in charge of planning the event. The charred shell of a detonated vehicle will be placed in front of the former Post Office building at the corner of East Market and Bennett streets. The scene will include smoke, fire, body parts, and "victims" with realistic-looking injuries. The Greensboro Fire Department will be the first to respond to the scene, followed by emergency medical personnel and the police department's bomb squad. The police department's Mobile Command Unit will also be at the scene to coordinate efforts of the various agencies. Although car bombs are traditionally thought of as weapons in other countries, police here believe terrorists in the U.S. can use them to take advantage of unprepared towns and cities. The entire exercise will be filmed and distributed to public safety agencies worldwide.

Source:

<http://www.myfoxwghp.com/myfox/pages/News/Detail?contentId=6539592&version=2&locale=EN-US&layoutCode=TSTY&pageId=3.2.1>

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

Information Technology

30. *May 15, IDG News Service* – (International) **Non-tech criminals can now rent-a-**

botnet. Online fraudsters that are not highly skilled in the arts of cybercrime can now rent a service that offers an all-in-one hosting server with a built-in Zeus Trojan administration panel and infecting tools, allowing them to create their own botnet. EMC's security division, the RSA Anti-Fraud Command Centre (AFCC), cited an increase in the use of the Zeus Trojan in attacks against financial institutions in its April online fraud report, claiming the Trojan is "extremely user friendly and easy to operate." "Fraudsters who execute Zeus attacks simply need to take control of a compromised server or have their own back-end servers; once they have a server in place, they merely need to install the Zeus administration panel, create a user name and password, and start launching their attacks," the report stated. But the AFCC recently traced a new service that does all of the above for would be botnet barons. The service offers access to a "bullet-proof hosting server with a built-in Zeus Trojan administration panel and infection tools...the service includes all of the required stages in a single package, meaning that all the fraudster now has to do is pay for the service, access the newly hired Zeus Trojan server, create infection points, and start collecting data." RSA's banking and finance specialist said that those offering the Zeus package are mirroring what legitimate security vendors are offering -- security-as-a-service -- but in their case they are slinging malware-as-a-service.

Source:

http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/05/15/N-on-tech-criminals-can-now-rent-a-botnet_1.html

31. *May 14, Computerworld* – (National) **Phishing botnet expands by hacking legit sites.** A botnet is now using a SQL injection attack tool designed to hack legitimate Web sites, a move meant to add more hijacked PCs to its collection, according to a security researcher. The Asprox botnet, which specializes in sending phishing spam, is pushing an update to the infected PCs it controls, the director of malware research at Atlanta-based SecureWorks Inc. said. The update is an executable file -- "msscncr32.exe" -- that installs as a Windows service dubbed "Microsoft Security Center Extension." But the executable actually installs an SQL injection attack tool, he said. SQL injection attacks have become widespread as criminals increasingly target legitimate Web sites, figure out a way to hack them, then plant iFrames on those sites to redirect users to malicious servers. Those servers silently attack visitors' PCs, often trying multiple exploits, and if one works, they download additional code to the machine to hijack it from its rightful owner and add it to an army of infected systems. "There are multiple things out there launching similar attacks," said the researcher in explaining why there is confusion about how the tool is being spread. Some analysts have mistakenly concluded that the SQL injection tool is using wormlike tactics, according to the research director. "The tool does not spread on its own but relies on the Asprox botnet to propagate to new hosts," he said.

Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9085564&source=rss_topic17

32. *May 14, ars technica* – (International) **New international group to become the CDC of cyber security.** Next week, the biannual World Congress of IT (WCIT) will be the

venue for the launch of a new initiative from an organization that aims to become a platform for international cooperation on cyber security. The group calls itself the International Multilateral Partnership Against Cyber-Terrorism (IMPACT), and its advisory board features numerous tech luminaries. The group's forthcoming World Cyber Security Summit (WCSS), which will be part of the WCIT 2008, is an effort to raise IMPACT's profile as an international platform for responding to and containing cyber attacks. On a conference call this morning, one of IMPACT's principals described the organization's mission as becoming a kind of "CDC [Centers for Disease Control] for cyber security." The idea is that it will provide both a forum and an actual communications system for coordinating international responses to cyber attacks, especially when those attacks involve civilian networks as a target, a source, or both. The principal members of IMPACT are governments, but the organization will include experts from academia and the private sector, as well. Indeed, the group is premised on the understanding that universities and corporations own most of the networks and computers that are at increasing risk of cyber attack, and that these entities are also at the forefront of current information security research and development.

Source: <http://arstechnica.com/news.ars/post/20080514-new-international-group-to-become-the-cdc-of-cyber-security.html>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: <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

33. *May 14, SecurityFocus* – (National) **Admins warned of brute-force SSH attacks.**

Allowing secure shell access to a server tends to attract the occasional attempt to guess a valid username and password for the service. However, a spike in attacks this week has system administrators worried. According to the senior security analyst at UC Berkeley, "Given enough time, any password can be broken, and a lot of them can be broken with relative ease because humans are, to a degree, lazy and will almost always opt for non-random, easy to recall -- and hence easy to guess -- passwords." Over the weekend, a number of network administrators issued warnings over an order-of-magnitude increase in the number of attempts to guess the username and password of systems running secure shell (SSH), the encrypted access method that replaced the common telnet service. System administrators at universities and some companies have reported login attempts coming from hundreds and thousands of Internet addresses over the past week, a stark increase from the handful of attacks the administrators saw previously. The Internet Storm Center, a network monitoring team supported by the SANS Institute, warned system administrators on Monday to take steps to protect their systems, noting the sharp spike in attacks.

Source: <http://www.securityfocus.com/news/11518>

34. *May 14, IDG News Service* – (International) **Hacker writes rootkit for Cisco’s routers.** A security researcher has developed malicious rootkit software for Cisco Systems’ routers, a development that has placed increasing scrutiny on the routers that carry the majority of the Internet’s traffic. A researcher with Core Security Technologies developed the software, which he will unveil on May 22 at the EuSecWest conference in London. Rootkits are stealthy programs that cover up their tracks on a computer, making them extremely hard to detect. To date, the vast majority of rootkits have been written for the Windows operating system, but this will mark the first time that someone has discussed a rootkit written for IOS, the Internetwork Operating System used by Cisco’s routers. “An IOS rootkit is able to perform the tasks that any other rootkit would do on desktop computer operating systems,” said the developer. Rootkits are typically used to install key-logging software as well as programs that allow attackers to remotely connect with the infected system. A Cisco rootkit is particularly worrisome because, like Microsoft’s Windows, Cisco’s routers are very widely used. Cisco owned nearly two-thirds of the router market in the fourth quarter of 2007, according to research firm IDC. In the past, researchers have built malicious software, known as “IOS patching shellcode,” that could compromise a Cisco router, but those programs are custom-written to work with one specific version of IOS. The new rootkit will be different. “It could work on several different versions of IOS,” he said. The software cannot be used to break into a Cisco router -- an attacker would need to have some kind of attack code, or an administrative password on the router to install the rootkit, but once installed it can be used to silently monitor and control the device.

Source:

http://www.pcworld.com/businesscenter/article/145898/hacker_writes_rootkit_for_cisco_s_routers.html

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

Commercial Facilities Sector

35. *May 15, HS Today* – (National) **Threats to mass gatherings explored in House HS report.** The Majority Staff of the House Committee on Homeland Security released a report Tuesday examining homeland security challenges for large-scale public gatherings which detailed 30 shortcomings in planning by federal, state, and local governments, as well as the private sector for protecting the public should an act of terrorism or disaster occur. The report, “Public Health, Safety, and Security for Mass Gatherings,” states that large public venues like the Super Bowl, NASCAR races, concerts, and political conventions could be terrorist targets – a threat risk that repeatedly has been pointed out in threat assessments by the Department of Homeland Security’s Office of Intelligence and Analysis. The 64-page committee majority staff report focuses on bioterror risks affecting large gatherings of people in stadiums and at concerts which are especially vulnerable to terrorist attacks using biological agents that can be distributed quickly and lead to infections and illnesses.

Source:

http://hstoday.us/index.php?option=com_content&task=view&id=3353&Itemid=149

36. *May 15, SkyNews* – (International) **Al Qaeda ‘Planning Euro 2008 Attack’**. Al Qaeda is planning to attack the Euro 2008 football championships in Switzerland and Austria in June, Swiss police say. “The Euro 2008 tournament is a target cited by the Islamist terrorist network,” a federal police spokesman told Swiss newspaper La Liberte. He said messages had been posted on Islamist websites and police were “following the situation very closely”. One of the messages urges terrorists to “transform the safest countries in Europe to the hell seen in Iraq or Afghanistan”. “The time has come for the fighters of the faith. They must make their voices heard,” said another. Authorities fear the global media coverage of the tournament will make it an attractive target for an attack. Security will be tight in and around the grounds, and extra checks will be made on people buying tickets from “high-risk” areas in the Middle East, the newspaper reported.
Source: <http://news.sky.com/skynews/article/0,,30200-1316139,00.html?f=rss>
37. *May 14, Business Day* – (International) **South Africa: Chemical attack ‘Threat to 2010’**. Easily available industrial compounds made South Africa vulnerable to a chemical and biological weapons attack during the 2010 Soccer World Cup. The executive manager of Protechnik, a subsidiary of the state-owned arms manufacturer Armscor, said “Where we see a greater threat is from toxic industrial chemicals.” These substances, such as chlorine, were easier to get hold of and were already widely transported in South Africa. This is something a terrorist would find far more attractive than dealing with chemical war agents in a clandestine laboratory, he said. Given better technology, the gap between chemical and biological weapons was narrowing. However, the military, with help from Protechnik, a specialized chemicals company, was working at developing contingency plans that included acquiring detection equipment to be used to protect soccer stadiums and fan parks, said the official.
Source: <http://allafrica.com/stories/200805140403.html>

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

National Monuments & Icons Sector

38. *May 15, Washington Post* – (District of Columbia) **High arsenic levels found at Fort Reno Park in NW**. A 33-acre federal park in northwest Washington was abruptly shut yesterday and will remain closed indefinitely after soil analysis found arsenic levels far above what the federal government considers safe, officials said. Fort Reno Park, near Woodrow Wilson High School, was closed at 6 a.m. A scientist with the U.S. Geological Survey said he informed the D.C. Department of the Environment that soil samples contained arsenic levels up to 25 times higher than federal regulations allow. After receiving the report late Tuesday, D.C. officials informed the National Park Service, which runs the site. In a statement, the Park Service said it “moved immediately to close Fort Reno Park to the public with snow fencing set up around the perimeter.” The cause of the high levels of arsenic and the health implications for people who use the park were unclear yesterday, officials said. Exposure to excessive amounts of arsenic can significantly increase the risk of cancer. The Environmental Protection Agency will be conducting testing today at Fort Reno as well as on the grounds of Wilson High School, across the street from the park, said a spokeswoman for the mayor’s office. City officials said the testing would take up to ten days. Officials from the fire department,

the department of the environment, and the city's emergency management agency will operate a command post set up in the area today.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2008/05/14/AR2008051403411.html>

39. *May 15, Washington Post* – (National) **Sites in National Forests at grave risk, study by preservation group indicates.** Millions of historic sites, crumbling and collapsing in national forests around the country, are in danger of being lost forever, according to a study set to be released today by a prominent preservation group. The National Trust for Historic Preservation estimates that only a small slice of about two million “cultural resources” that sit on 193 million acres managed by the U.S. Forest Service have been properly preserved. Their deterioration has been accelerated by vandalism, theft, fire, damage from off-road vehicles, and other recreation, as well as oil and gas extraction, mining, timber harvesting, and grazing, the study found. The resources include Native American archaeological sites, Civil War battlefields, ranger stations, fire lookout towers, cabins, and camps built by the Civilian Conservation Corps. The study credited the Forest Service for its attempts to preserve and maintain some of the sites, but said it faces an overwhelming task. The Forest Service, part of the U.S. Department of Agriculture, does not know how many sites of archaeological, historic, or cultural importance exist on the land it maintains, because a complete audit has never been performed. The agency examined 20 percent of its land and identified about 325,000 “cultural resources” as of last year. Of those, 50,000 were determined to be eligible for listing in the National Register of Historic Places, and a tiny fraction – 27 – were awarded National Historic Landmark status. The trust wants the Forest Service to develop a plan to determine the number of historic sites on its land and to set priorities for preservation. It also wants the agency to allow some of the historic buildings to be leased for public use.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/05/14/AR2008051403473.html?nav=rss_politics/fedpage

40. *May 15, Associated Press* – (Florida) **F/A-18 bomb misses target, sparks fire in Fla.** Officials are investigating how a Navy fighter jet dropped a 500-pound laser-guided bomb a mile off target and sparked a wildfire in the Ocala National Forest. About 150 acres burned after an F/A-18 Super Hornet fighter dropped a bomb that landed outside the target range, a news release from Naval Air Station Jacksonville said Wednesday. A fire management officer with the U.S. Forest Service told the Ocala Star Banner Tuesday's fire was contained.

Source: http://www.militarytimes.com/news/2008/05/ap_navy_bomb_051408/

41. *May 14, Associated Press* – (District of Columbia) **Study: Sea wall sinking around Jefferson Memorial.** The sea wall protecting the Jefferson Memorial from the Tidal Basin is sinking in spots and needs repair, a study concluded. The domed landmark built in the late 1930s and early '40s is not in danger, but should be monitored, according to the yearlong engineering study commissioned by the National Park Service. The study released Tuesday attributes the sinking mainly to soft soil under the wall that has compressed over the years. In some places, the wall has sunk almost a foot since the

memorial was built. The experts recommended reinforcing the wall by installing pilings through underlying mud flats and anchoring them in bedrock far below. The repair project could cost more than \$10 million.

Source: http://ap.google.com/article/ALeqM5j92A9jafPrEw-TM4XL_R711mDnAD90LHB700

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

Dams Sector

Nothing to Report

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

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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 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 or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at 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.