Department of Homeland Security Daily Open Source Infrastructure Report for 21 October 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- Computerworld reports that two key systems that the U.S. Internal Revenue Service is deploying contain serious security vulnerabilities that pose a direct risk to taxpayer data, according to a report by the Treasury Inspector General for Tax Administration. (See item **24**)
- According to the Chattanooga Times Free Press, the Dalton, Georgia, police chief told residents Sunday he doubts anyone else was involved in the Friday morning bombing of a local law firm that killed the bombing suspect and injured four others. (See item **29**)

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. *October 20, Columbus Dispatch* – (Ohio) **2 men die in blast at oil rig.** An explosion at a remote Marion County, Ohio, oil well killed two men Sunday just after 2:30 p.m. Authorities say the two men were welding a catwalk on one of four large crude-oil storage tanks at the rig site when a tank exploded. Both men died instantly. Six fire departments responded, and the fire itself was extinguished in probably less than 20 minutes, said the chief of the Marseilles Volunteer Fire Department. Investigators from the state fire marshal's office were at the scene, and the Occupational Safety and Health Administration had been notified, although it was unclear whether the federal agency would get involved. The Marion County sheriff said the oil wells are operated by a

company called Mar Oil, and the property is owned by a family, although nothing else about either could be confirmed Sunday night.
Source:
http://dispatch.com/live/content/local_news/stories/2008/10/20/oil_rig.ART_ART_10-20-08_A1_OLBLAMB.html?sid=101

2. *October 19, Edmonton Journal* – (International) **Terrorists target U.S. via Alberta.** Alberta, Canada, has become a "prime location" for terrorists looking to capitalize on shaky economic times in Canada and the United States, terrorism experts said on Saturday at a national conference for emergency officials. "While Alberta might not be a first choice for mass-casualty attack terrorism – you are unlikely to see a major bomb going off in downtown Edmonton -- it certainly is a prime location for economic terrorism, because of the ability to disrupt the oil and gas industry," said a Calgary-based defense and security analyst. Her remarks come as the security of energy infrastructure is under scrutiny after two explosions at B.C. pipelines in Canada in the past week. She said that as the Canadian economy heads toward a slump, Alberta is an increasingly important revenue-driver. Longtime international foes of the United States are closely watching that nation's sharp economic decline, said a world expert in nuclear, biological, and chemical weapons. Terrorists "are in a waiting time right now," he said, adding Canada is chiefly vulnerable as a staging ground for attacks on the United States. "Times like these make us vulnerable, and it makes it a desirable time to hit economic markets, because you've got a better chance of driving them down and really bleeding the United States and Canada economically," the Calgary defense analyst said.
Source: http://www.canada.com/edmontonjournal/story.html?id=12b412bc-2f6b-4519-98bd-943e3ed0ebd2

3. *October 17, KWTX 10 Waco* – (Texas) **Central Texas gas line explosion burns field.** A man digging a large lake cut through an unmarked natural gas transmission line Friday in Leon County, Texas, and the ruptured line exploded. The fire burned a patch of pasture about 75- to 100-yards wide, according to an investigator with the Leon County Sheriff's Office. The investigator said the Centerville Volunteer Fire Department and deputies from his office responded to the site at about 1:30 p.m. Friday. He said no one was injured, and no evacuations were required because the site is in an extremely rural part of the county. Firefighters had the fire under control within about 20 minutes. He said he has called four gas transmission companies in an attempt to find who owns the line, but has not yet determined to whom it belongs.
Source: http://www.kwtx.com/home/headlines/31181379.html

4. *October 17, Gillette News-Record* – (Wyoming) **WyGen II gets a new transformer.** A new transformer installed at WygGen II on Thursday is expected to go online in a week. The previous transformer died October 7 during a scheduled maintenance outage. The transformer, the only one at the power plant east of Gillette, Wyoming, was running on less than 1 megawatt of power during the outage when its protective devices shut it down. "There was no fire, no explosion, we just had an electric signal that said we had a problem," said the vice president and general manager for the Neil Simpson complex at

Wyodak. Black Hills Corp. officials do not know what caused the incident, but they sent an oil sample from the transformer to a lab for chemical analysis. The new transformer will have the same converting capacity as the old one. It will receive 13,800 volts from the generator, which will convert to 2.30 kilovolts that will go on the transmission line. Source: http://www.gillettenewsrecord.com/articles/2008/10/17/news/today/news03.txt

[Return to top]

Chemical Industry Sector

5. *October 19, Daily Advertiser* – (Nevada) **Chemical spill prompts evacuation.** A chemical spill at Diesi's Lucky Capitol Casino in Henderson early Saturday morning led to an evacuation of the immediate area and a cleanup effort that extended well into the afternoon. The command report from Louisiana State Police Troop I stated that a call at 5:47 a.m. to the St. Martin Parish Sheriff's Office reported a leaking container in a transport truck at the casino. The container held a chemical called toluene, a clear, water-insoluble liquid commonly used as an industrial feedstock and as a solvent. The spill cleanup was handled by U.S. Environmental Services. A 50-foot area around the spill was evacuated, affecting the Lucky Capitol Casino and the Little Capitol truck stop nearby. The evacuation of the area was instituted because of toluene's flammable nature. Source: http://theadvertiser.com/apps/pbcs.dll/article?AID=/20081019/NEWS01/810190349

6. *October 17, Business Green* – (International) **U.S. joins EU in banning mercury exports.** All U.S. mercury exports will be outlawed from the beginning of 2013, while new rules governing the storage of mercury in the United States will be introduced from 2010. The EU took similar action last month with an export ban that will become effective from 2011. Together the moves are expected to drive up the price of the metal, as the two regions are responsible for between 40 and 50 per cent of annual global trade. It is hoped that companies still using the substance will come under financial pressure to develop safer alternatives.
Source: http://www.businessgreen.com/business-green/news/2228536/joins-eu-banning-mercury

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *October 19, Miami Herald* – (National) **Tons of nuclear waste piling up at power plants.** For 25 years, the federal government has considered storing radioactive waste at Yucca Mountain in Nevada. That has led to bitter opposition from environmentalists, those close to the proposed dump and even some nuclear experts. The U.S. Department of Energy is just now starting to consider a formal application for the nuclear repository. Estimated cost: $96.2 billion over the lifetime of the storage facility, which is expected to fill to capacity in 2133. Until this point, all nuclear plants have had to keep their waste on site, piling up at the rate of 20 tons per reactor per year. For its four reactors at Turkey Point and St. Lucie, the Florida Power and Light Company (FPL) says all the

waste accumulated since the 1970s would cover about five yards on a football field, to a height of 10 feet. FPL has joined industry lawsuits against the Department of Energy to make it respond more quickly in dealing with the waste. The waste could be the target of terrorists with the goal of making a fire at the site or to use the waste for a `dirty bomb.' Some supporters advocate reprocessing.
Source: http://www.miamiherald.com/602/story/731069.html

[Return to top]

Defense Industrial Base Sector

8. *October 20, Reuters* – (National) **Pentagon postpones big satellite contract until FY10.** The U.S. Defense Department has decided to postpone a decision in a multibillion dollar satellite communications competition between Lockheed Martin Corp. and Boeing Co. until fiscal year 2010, an industry source informed about the decision said on Sunday. The Pentagon's Defense Advisory Working Group decided on Saturday to terminate the current competition for the Transformation Satellite (TSAT) program, and put off awarding a contract until the fourth quarter of fiscal 2010, said the source. The Air Force had hoped to award a contract for the new advanced military communications satellite program in December. The TSAT program already suffered a 40 percent funding cut when the Presidential Administration announced its long term budget plans in February. Pentagon officials decided this weekend to scale down the program even further and postpone a scaled-down contract award for more than a year. The decision could have grave consequences for the military's goal of offering soldiers on the battlefield access to satellite communications anytime soon. The delayed award means the first TSAT satellite would not be launched until around 2019, raising serious questions about the ability of the U.S. Army to move ahead with its Future Combat Systems modernization program, which is meant to rely heavily on advanced satellite communications. The TSAT program is linked to another big program, the Advanced Extremely High Frequency (AEHF) satellite program run by Lockheed, which has exceeded congressional caps on cost growth after Congress added a fourth satellite to the program. The Pentagon now seems to prefer to continue evolving the AEHF satellites, rather than trying to leapfrog to a new generation of technology with TSAT.
Source: http://www.reuters.com/article/technologyNews/idUSTRE49J0EX20081020?pageNumber=1&virtualBrandChannel=0

9. *October 17, Reuters* – (National) **U.S. to study space-based defense.** The U.S. Congress has approved $5 million for an independent study of possible space-based missile defenses, a potential step toward a system once mocked as "Star Wars." The seed money was included in a little-noticed part of the 2009 Defense Appropriations bill, signed into law by the U.S. President on September 30 as part of a catch-all funding measure. Last year, Congress rejected $10 million sought for such a study amid concerns it could lead to weaponization of space. The Presidential Administration had sought $10 million again this year to start a testbed in space, a sort of proof of concept. The $5 million appropriation lets the Pentagon hire one or more entities to review the feasibility and advisability of adding space-based interceptors to the growing numbers of

U.S. interceptor missiles on the ground and at sea.
Source:
http://www.reuters.com/article/scienceNews/idUSTRE49H05Y20081018?pageNumber=1&virtualBrandChannel=0&sp=true

[Return to top]

Banking and Finance Sector

10. *October 20, Computer Weekly* – (International) **Hackers crack Sarkozy's online bank account and steal cash.** Thieves hacked the French president's bank account, stealing cash after gaining access to the President's online passwords. The French secretary of state for consumer affairs also said more needed to be done to tighten the security of internet banking in France. The French President is said to have reported the theft last month, but no one has yet been charged with the crime.
Source: http://www.computerweekly.com/Articles/2008/10/20/232733/hackers-crack-sarkozys-online-bank-account-and-steal.htm

11. *October 19, Atlantic Journal Constitution* – (Georgia) **Several Georgia banks in jeopardy.** Dozens of Georgia banks are struggling with surging levels of delinquent loans, the result of a dangerous concentration on lending for metro Atlanta's once-thriving real estate development. The bad loans have caused one Georgia bank to fail this year and could put another dozen under by year's end. Some banking experts say a delinquency rate of even 2 percent suggests an institution faces serious financial challenges. In Georgia, 159 banks exceed that level. Twenty-five of them have seen seriously past-due loans rise into the double digits. Federal insurance guarantees the safety of depositors' money, but stockholders stand to lose their entire investments.
Source:
http://www.ajc.com/news/content/business/stories/2008/10/19/georgia_banks.html

12. *October 17, SC Magazine* – (International) **Darkmarket forum closed following police raids.** Darkmarket forum, described as a 'one stop shop' for criminals, was closed down following dawn raids in Manchester, Hull, and London, U.K., as well as Germany, Turkey, and the United States. The forum was used by criminals to buy and sell credit card details and bank logins and was running for around three years. Soca (Serious Organized Crime Association) claimed that there were 2,000 users registered on Darkmarket, but many of those were not unique. SC revealed earlier that the FBI had used Darkmarket to capture the details of thousands of hackers and spammers via an undercover agent posing as a forum member. About 60 people were arrested.
Source: http://www.scmagazineuk.com/Darkmarket-forum-closed-following-police-raids/article/119603/

[Return to top]

Transportation Sector

13. *October 20, Homeland Security Today* – (National) **Alliance calls for speedy aviation**

credential. The implementation of a personal identity verification (PIV) program such as one under consideration by the Transportation Security Administration (TSA) would streamline security processes, save money, and leverage government security expertise at U.S. airports, according to a recent white paper from a nonprofit association representing smart card technology companies. The Smart Card Alliance, in a paper titled "Interoperable Identity Credentials for the Air Transport Industry," argued for the finalization and adoption of identity authentication under the Aviation Credential Interoperability Solution (ACIS), a program being developed by TSA to implement Federal Information Processing Standard 201 for establishing PIV credentials. Airports would benefit if the Federal Aviation Administration handed complete responsibilities for aviation security to TSA, thereby providing a clear line of authority to aviation workers. TSA would deploy an interoperable aviation identification credential under ACIS, which would supply PIV credentials to a range of aviation workers from baggage handlers to aircraft maintenance personnel to managers. TSA, airports and other aviation stakeholders would realize significant cost savings by following in the footsteps of other federal organizations that have moved ahead with the adoption of FIPS 201 standards in their identity verification programs under Homeland Security Presidential Directive 12, which required them to adopt solutions like personal smart cards to provide logistical and physical access to government resources. Currently, most airports follow TSA security directives that require them to conduct a criminal history records check and a security threat assessment on people applying for aviation jobs. Airports and airlines must complete these checks before they can hire an individual and issue identity cards to them.
Source: http://www.hstoday.us/content/view/5677/128/

14. *October 18, Washington Post* – (Virginia) **Transfer of Dulles toll road to airport agency is upheld.** A state judge in Richmond dismissed a lawsuit yesterday that had challenged the transfer of the Dulles Toll Road to the authority that runs Reagan National and Dulles International airports, clearing the way to use toll revenue for an extension of Metrorail to Dulles. Virginia's Transportation Secretary said the transfer of control from the state to the Metropolitan Washington Airports Authority could occur by the end of the year, along with an expected announcement of a funding agreement from the Federal Transit Administration (FTA). If the court had voided the transfer, it would have put the Metrorail extension in jeopardy. The FTA is deciding whether to fund $900 million of the $5.2 billion project, and a legal ruling against using toll revenue could have cast doubt on the federal portion.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101701940.html

15. *October 18, Washington Post* – (Maryland) **Purple line to require demolition, sound walls.** Building the Purple Line through Montgomery and Prince George's counties could require demolishing up to 31 private properties, according to a six-year state study released yesterday. The highly anticipated 250-page report provided the first overall detailed look at its potential impact, from the number of estimated riders to the sights and sounds for those who would live, work and attends school along the 16-mile route between Bethesda and New Carrollton. Among the findings: Some of the 64

intersections with stoplights in that east-west corridor would need improvements, such as new turn lanes, to prevent traffic from worsening if vehicles shared travel lanes with light rail trains or express buses. Some street parking would vanish, and some property owners, including as many as four Montgomery County schools, could lose strips of land – both necessary to widen roads to accommodate a transitway. The Purple Line, which could cost as much as $1.6 billion, would be the region's first transitway designed specifically to connect suburbs, rather than running in and out of the District's core. It would run primarily above ground and along existing roads – either as a light rail system or busway-- with as many as 20 stops, including Metrorail and MARC stations. Sound walls and panels covering train wheels would be necessary to protect residents in up to 18 "potential annoyance zones" from the screech of metal train wheels turning sharp corners, planners wrote. Depending on the route and mode of transit chosen, as many as 19 business properties and as many as 12 residences would be condemned. The Purple Line is estimated to attract up to 68,100 trips daily, according to the study.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101701642.html

16. *October 18, Associated Press* – (Illinois) **3 injured when airplane hits maintenance truck.** Authorities say three people are injured after a small regional jet struck a maintenance truck on a runway at Chicago's O'Hare International Airport. No passengers were aboard the United Express jet, operated by SkyWest Airlines. It was traveling from a hangar to a gate with it collided with the truck early Saturday. The driver of the truck was transported to a hospital in critical condition. Two mechanics from the plane were hospitalized in good condition. A SkyWest spokesperson said it was not clear from surveillance footage who was responsible for the accident. A Department of Aviation spokesperson says a runway was closed for less than two hours. Flight operations were unaffected.
Source: http://www.msnbc.msn.com/id/27251730/

17. *October 17, Aero-News.net* – (National) **FAA creates 'lessons learned' online database.** The Federal Aviation Administration (FAA) has established a one-of-a-kind online safety library that teaches "lessons learned" from some of the world's most historically significant transport airplane accidents...especially how that knowledge can help maintain today's aviation safety record. By learning from the past, aviation professionals can use that knowledge to recognize key factors, and potentially prevent another accident from occurring under similar circumstances, or for similar reasons, in the future. Each accident entry features the accident investigation findings, resulting safety recommendations and subsequent regulatory and policy changes, if any. The entry also includes sections on the unsafe conditions that existed, precursors that pointed to an impending accident, and the basic safety assumptions made during the airplanes' design, or that led to the airplanes' continued operation. Most important, the lessons learned from the investigation are explained in detail, and grouped into relevant technical areas and common themes, such as organizational lapses, human error, flawed assumptions, preexisting failures and unintended consequences of design choices. The FAA's goal is to stock the library with 40 more historically significant accidents by the end of 2009.
Source: http://www.aero-news.net/index.cfm?printable=1&ContentBlockID=b2b8b3fc-

a8bf-431c-a9a6-dcc54951375b

[Return to top]

Postal and Shipping Sector

18. *October 20, GreenBiz* – (National) **USPS saves $5 million annually with transportation consolidation.** Since deploying a transportation optimization system two years ago, the United States Postal Service (USPS) has saved $10 million through consolidating delivery trips. The USPS has been using the Highway Corridor Analytic Program (HCAP), created in conjunction with IBM, since 2006. Developed with the ILOG CPLEX optimization software, the HCAP helps the USPS determine the best way to allocate mail among its transportation resources. The USPS has various transportation methods for moving around mail, depending on the type of mail and when it needs to be delivered. Using the HCAP, the USPS inputs its existing network and routes, and sets constraints such as pickup and delivery times, truck capacity, and start and end points. The program analyzes existing operations and figures out alternative loads and routes to reduce costs. The USPS piloted the program in select areas, finding savings of $1.3 million annually in Chicago, $3.7 million annually on the West Coast, and $400,000 annually in Greensboro and Pittsburgh, adding up to more than $5 million and about 615,000 gallons of gasoline saved a year. The USPS estimates that for every one-cent increase in gas prices, it pays $8 million a year, and it plans to continue using the program to develop efficient routes and loads elsewhere.
Source: http://www.greenbiz.com/news/2008/10/20/usps-transportation-consolidation

[Return to top]

Agriculture and Food Sector

19. *October 17, Packer* – (National) **Retailer's rejections send message on COOL.** When the country-of-origin labeling (COOL) law for fresh produce and other food went into effect September 30, the U.S. Department of Agriculture allowed for a six-month phase-in before enforcing compliance. Some retailers, however, are not waiting that long. The president of Consumers Produce Co. Inc. of Pittsburgh said some chain stores in the region are demanding immediate COOL compliance from suppliers. The director of corporate communications for Wal-Mart Stores Inc. said Wal-Mart stores have been instructed to reject produce that is not labeled correctly, but she could not confirm if they have. Some suppliers have sought to understand why the USDA regulation and buyer expectations seem to be different. Some of the problematic commodities include zucchini, roma tomatoes, yellow squash and green peppers. COOL regulations allow for signs to account for more than one country for bulk displays.
Source: http://www.thepacker.com/icms/_dtaa2/content/wrapper.asp?alink=2008-15812-306.asp&stype=topnews&fb

20. *October 17, Packer* – (National) **Coalition creating database on irrigation water.** A coalition of leading produce industry groups is compiling a database that it hopes will shed light on the degree of contamination in irrigation water and ease consumers'

concerns. The coalition is asking grower-shippers in California and Arizona to submit their test results starting with 2007 testing. The goal is to develop baseline information on irrigation water quality and to demonstrate the overall microbiological quality of irrigation water in produce growing regions. The database might provide a scientific basis for better water testing methods and demonstrate progress in good agricultural practices. Test results will be held in confidence, and there is no charge for grower-shippers to participate. The project will be on-going to determine whether there are differences between seasons and sources. The Pacific Institute, an Oakland, California-based research institute released a study in September that claimed grower-shippers are failing to do enough to conserve water in California.
Source: http://www.thepacker.com/icms/_dtaa2/content/wrapper.asp?alink=2008-125016-556.asp&stype=topnews&fb=rt1

21. *October 17, MeatingPlace.com* – (National) **FSIS issues draft guidance for N-60 E. coli testing claims.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) has issued a draft guidance on the use of labels bearing an FSIS-approved N-60 E. coli O157:H7 testing claim. Such special label claims are voluntary. An establishment may use them when it demonstrates such E. coli O157:H7 testing claims are truthful and not misleading. FSIS needs to approve the claims before the establishment can use them on labeling. This labeling claim is intended to provide the receiving establishment with this information in lieu of Certificates of Analysis that may not properly transfer with product through distributors. It asserts that the raw beef component has been produced under an integrated control program between the slaughter/dressing operation and the trim production operation and tested for the presence of E. coli O157:H7 using a particular sample method (for example, N-60 sampling). Labels bearing this claim would not be approved for products sold at retail or directly to consumers.
Source:
http://www.meatingplace.com/MembersOnly/webNews/details.aspx?item=10087

22. *October 17, Rutland Herald* – (New York; Vermont) **Vt. slaughterhouse recalls ground beef.** Vermont Livestock, Slaughter and Processing Co. LLC, in Ferrisburg, Vt., firm, is recalling about 2,758 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service announced. Subject to recall are 5-pound approximate weight vacuum packages of "VT BURGER CO GROUND BEEF." This product was shipped two packages per box, intended for restaurants, food service and institutional use and not available for direct retail purchase. The problem was discovered through a joint epidemiological investigation by FSIS (Food Safety and Inspection Service) and the Vermont Department of Health. FSIS has received 10 confirmed reports of illnesses associated with consumption of this product.
Source:
http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20081017/NEWS03/810170332/1004/NEWS03

[Return to top]

Water Sector

Nothing to report

[Return to top]

Public Health and Healthcare Sector

Nothing to report

[Return to top]

Government Facilities Sector

23. *October 20, Central Florida Future* – (Florida) **UCF residence hall evacuated after explosion.** A University of Central Florida (UCF) residence hall was evacuated late Sunday night after an explosion in one of the rooms, a UCF Police Department investigator said. The explosion that caused the evacuation was caused by a student who was attempting to make Adderall, a prescription psychostimulant used to treat attention deficit hyperactivity disorder. "We had a student on campus attempting to make Adderall in his room. There was a small explosion but no damage to the room, no students were injured," the investigator said. There was no fire from explosion. Smoke caused the building's fire alarm to activate. The UCF Police Department, Orange County Sheriff's Office, and Hazmat teams from the Orange County Fire Department responded to the scene. The UCF Department of Environmental Health and Safety was brought in to help with declaring the floor to be safe.
Source:
http://media.www.centralfloridafuture.com/media/storage/paper174/news/2008/10/20/News/Ucf-Residence.Hall.Evacuated.After.Explosion-3494868.shtml

24. *October 17, Computerworld* – (National) **Two new IRS systems have major security weaknesses, federal report says.** Two key systems that the U.S. Internal Revenue Service (IRS) is deploying contain serious security vulnerabilities that pose a direct risk to taxpayer data, according to a report by the Treasury Inspector General for Tax Administration. The 29-page report is dated September 24 but was just publicly released on Thursday. It identifies weaknesses in several areas — including access control, monitoring of system access, and disaster recovery — in a new Customer Account Data Engine (CADE) system that the IRS is rolling out, plus a related Account Management Services system. According to the Inspector General's report, systems administrators and other privileged users are able to access, modify, and delete taxpayer data with impunity because of a lack of monitoring capabilities in the two systems. In addition, contractors working for the IRS can make configuration changes without prior notice or approval, the report said. Similarly, there are no processes in place for verifying whether data that is archived on backup tapes is being stored properly and can easily be recovered if needed, according to the report. In addition, a vulnerability scan of the mainframe environment that hosts the CADE system uncovered at least one critical vulnerability that posed a risk to taxpayer data, plus several configuration errors, the

report said. It added that sensitive personal information about taxpayers was being transmitted without being encrypted or otherwise disguised within IRS computing centers, and also was not encrypted when it was stored. And, the report said, the IRS used live taxpayer data in at least 18 test environments for application development purposes.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117447&intsrc=news_ts_head

[Return to top]

Emergency Services Sector

25. *October 20, Occupational Health & Safety* – (National) **DHS adopts NFPA standards for hazmat/WMD incidents.** The U.S. Department of Homeland Security has adopted two additional National Fire Protection Association (NFPA) standards for first responders: NFPA 472, Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents and NFPA 473, Standard for Competencies for EMS Personnel Responding to Hazardous Materials/Weapons of Mass Destruction Incidents. These two standards set minimum requirements for personnel responding to incidents involving hazardous materials and weapons of mass destruction. NFPA 472 sets minimum competency levels for personnel responding to such incidents, and NFPA 473 covers the requirements for basic life support and advanced life support personnel in the pre-hospital setting.
Source: http://ohsonline.com/Articles/2008/10/20-DHS-Adopts-NFPA-Standards.aspx

[Return to top]

Information Technology

26. *October 18, CyberInsecure* – (International) **MSN Messenger used as lure in another malicious spam wave.** Websense Labs are reporting a new malicious spam lure that uses the threat of a virus to encourage users to download a malicious Trojan. The email explains that by downloading the application linked within the email, users can protect themselves against a virus that spams messages to a user's contacts. The email offers an update to Live Messenger Plus which is actually a Trojan. The URLs provided in the email redirect the user to a two-stage downloader named dsc.scr. As a distraction for the user, a dialog box is displayed explaining that the user will be redirected to msn.com.br. A browser then opens pointing to a different site. A scheduled task is then created, and modifications are made to autoexec.bat to disable GBPlugin and other tools promoted by Brazilian banks to protect against such key loggers and other malware. The malware then goes on to conduct information-stealing activities.
Source: http://cyberinsecure.com/msn-messenger-used-as-lure-in-another-malicious-spam-wave/

27. *October 17, Internet News* – (International) **Adobe sites hit by malware.** Adobe has had to deal with two of its websites compromised by an SQL injection attack. The

manager of the U.S. offices of security vendor Sophos Laboratories, confirmed the sites had been affected. The manager said after Sophos contacted Adobe, the software issues at both of its websites had been cleaned up; a follow up check by Sophos found them "clean" and no longer at risk. One of the Adobe websites infected was its Vlog It support section, an area providing tips for video bloggers. Sophos today notified users about this. The other infected Adobe site Sophos discovered is Serious Magic which produces high-quality video and communication software. The Vlog It site was affected by malware known as Mal/Badsrc-C. It was delivered by a botnet known as Asprox, which was also used in the attack on Adobe's Serious Magic site.
Source:
http://www.internetnews.com/security/article.php/3779021/Adobe+Sites+Hit+by+Malware.htm

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

28. *October 20, Mobile Marketing News* – (International) **Expert warns of new mobile virus.** A new mobile virus that is causing havoc with many people's handsets has been highlighted by an expert. A researcher from Adaptive Mobile, a British firm that tracks malware and provides security software for mobile firms, told BBC News that the Beselo virus has been responsible for a rise in spam from 0.5 percent of traffic to 6 percent over the last 12 months for a typical network operator. Beselo spreads via MMS or by searching for nearby Bluetooth devices - a true 'airborne virus' that has grounded many affected mobile phones. There are thought to be around 400 mobile viruses in circulation today and there are compelling reasons why experts think that number is about to grow.
Source:
http://www.mobilemarketingnews.co.uk/Expert_warns_of_new_mobile_virus_18833519.html

[Return to top]

Commercial Facilities Sector

29. *October 20, Chattanooga Times Free Press* – (Georgia) **Dalton: No other suspects in bombing.** The Dalton, Georgia, police chief told residents Sunday he doubts anyone else was involved in the Friday morning bombing of a local law firm that killed the bombing suspect and injured four others. He said the bombing suspect rammed an SUV into the front of the building before running around the back of the building, bursting

out a window, and placing a metal explosive device the size of a five-gallon bucket inside, where it exploded. An attorney at a local firm said he and others were still trying to sort out what had happened. "It was a freakish, random act," he said. The bombing suspect had been in an ongoing property dispute with his son, and an attorney at the firm represented the son in the dispute.
Source: http://timesfreepress.com/news/2008/oct/20/dalton-no-other-suspects-bombing/

30. *October 17, IDG News Service* – (National) **Man charged in Scientology Web attack.** An 18-year-old New Jersey man will plead guilty to the January online attacks that took down the Church of Scientology's Web site, federal prosecutors said Friday. The New Jersey man was part of an underground hacking group called Anonymous that has made the church a target of several attacks. He was charged on October 17 but has agreed to plead guilty sometime in the next few weeks, the U.S. Department of Justice said in a statement. He faces 10 years in prison on computer hacking charges. This is not the first time Anonymous has been connected to a high-profile hacking incident. Last month the group claimed credit for accessing Republican vice presidential candidate's Yahoo e-mail account and posting some of its contents online.
Source:
http://www.pcworld.com/businesscenter/article/152445/man_charged_in_scientology_web_attack.html

[Return to top]

National Monuments & Icons Sector

31. *October 18, Red Bluff Daily News* – (California) **Forest pot farm busted.** Tehama County Sheriff's Deputies (TCSD) put a stop to a 2,500-plant marijuana operation Thursday in Lassen National Forest, confiscating 500 pounds of processed marijuana and two shotguns in the process. The arrests mark the closure of a three-month collaborative investigation between the TCSD and the U.S. National Forest Service, according to a TCSD press release. Deputies and officers of the U.S. Forest Service raided the Beaver Creek encampment, northeast of Campbellville, at about 10 a.m. Four men were arrested on suspicion of cultivation of marijuana and possession of marijuana for sale. Each faces a bail of $20,000.
Source: http://www.redbluffdailynews.com/ci_10754875

32. *October 17, WBIR-10* – (Tennessee) **Huge drug bust leaves behind big mess.** In June, agents with the Governor's Task Force on Marijuana Eradication discovered a huge crop of marijuana plants growing inside the Cherokee National Forest near Newport. The plants were removed, but now officials are back to clean up the rest of the mess. June's drug bust was one of the largest in the state in years, but it left behind an even larger amount of trash. In addition to the more than 350,000 marijuana plants recovered, investigators also found propane tanks, pesticide containers, and hundreds of feet of irrigation tubing. Agents with the governor's Task Force on Marijuana Eradication planned an extensive cleanup effort, some of which could help in the continuing investigation. But removing the leftover mess from the remote location will not be easy: the trash will have to be loaded onto a cargo net and then air-lifted by a Black Hawk

helicopter to a place where it can be disposed of. Officials say the trash was not only an environmental hazard, but also could have been potentially dangerous to hikers or campers in the area.
Source: http://www.wbir.com/news/local/story.aspx?storyid=66884&catid=2

[Return to top]

Dams Sector

33. *October 19, Waterloo Cedar Falls Courier* – (Iowa) **Waterloo levees held up well, but were damaged by floods.** The Cedar River levees suffered a few battle scars while holding back most of the record floodwaters rolling through Waterloo, Iowa, in June. The U.S. Army Corps of Engineers' survey of Waterloo's flood control system estimated damage at more than $1.2 million in a recent report to the city. The most notable damage to the system was the loss of riprap cover along the west banks of the Cedar and significant silt accumulation in a pump station outfall channel and in the project's 50-year bypass channel around the sewage treatment plant in the Riverview Recreation Area. The associate city engineer said he believes repairing the actual damage may be closer to $1.5 million, most of which should be federally funded. An estimated 60,000 cubic yards of silt will need to be removed from the bypass channel, which routes some floodwaters around the sewage treatment facility, and the pump station outfall channel. The city is also working to prioritize and identify funding sources for other improvements to the flood control system, which would include lift stations in several areas to pump water over the levees when gatewells are closed during high-water events.
Source: http://www.wcfcourier.com/articles/2008/10/19/news/metro/10695383.txt

34. *October 18, Anderson Independent-Mail* – (South Carolina) **Army Corps of Engineers to study new Broadway Dam.** In late September, the U.S. House of Representatives Transportation and Infrastructure Committee passed a resolution authorizing the U.S. Army Corps of Engineers to conduct a study regarding a new dam at Broadway Lake in Anderson County, South Carolina. The idea has been raised that a new dam is needed to address the flood threat posed by the existing, inadequate facility, which was originally constructed by the federal government's Works Progress Administration. According to the Congressional Research Service, this authorization allows the Corps to investigate a problem and determine if there is a federal interest in proceeding further. Early in the study process, the Corps assesses the level of interest and support of nonfederal entities that may be potential sponsors. Nonfederal sponsors are state, tribal, county, or local agencies or governments that join the Corps in the effort.
Source: http://www.independentmail.com/news/2008/oct/18/army-corps-engineers-study-new-broadway-dam/

35. *October 18, Associated Press* – (Montana) **Crews temporarily fix Hebgen Dam intake structure.** The intake structure at the Hebgen Dam in Montana has been temporarily fixed, and water flow into the Madison River is back to normal levels for this time of year. Crews have been working on the dam since August 31, when several stoplogs were discovered missing. The malfunction sent water rushing into the river at spring runoff

levels. The latest repairs reduced water flow to about 700 cubic feet per second, normal for the Madison at this time of year. PPL officials hope early snowfall in the Madison Valley will help replenish Hebgen Lake.
Source:
http://www.montanasnewsstation.com/Global/story.asp?S=9199210&nav=menu227_8

36. *October 18, Associated Press* – (Louisiana) **Termites may be threat to New Orleans levees, report says.** Subterranean termites that have infested New Orleans, Louisiana, since World War II may be a much bigger threat to this city's levees and floodwalls than many experts suppose, a new entomological paper says. For the past 70 years, New Orleans has been battling the voracious wood-eating Formosan termites that arrived on military ships returning from the Pacific. But that battle has mostly taken place at the neighborhood and street level. A new article in the Entomological Society of America's magazine, American Entomologist, says there is ample evidence termites are infesting the city's levees and floodwalls and potentially weakening flood defenses. The U.S. Army Corps of Engineers, which is overseeing levee reconstruction, said it was aware of the termite threat but did not consider it a factor in the 50 major breaches during Hurricane Katrina that contributed to the flooding in New Orleans. The Corps believes a combination of design flaws and the massive storm surge from Katrina broke the levees.
Source:
http://www.dallasnews.com/sharedcontent/dws/news/texassouthwest/stories/DN-termites_18tex.ART.State.Edition1.4ade89f.html

[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
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
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