Department of Homeland Security Daily Open Source Infrastructure Report for 18 May 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Defense Security Service has received funding to resume processing initial secret level security clearances for industry, and will begin working on initial top−secret requests and periodic reinvestigation requests for both secret and top−secret clearances when more funding is available. (See item 2)
- The Marshall Democrat−News reports the theft from a Missouri Union Pacific Railroad substation of 1,000 feet of copper cable −− valued at $3,000 −− was reported to the Saline County Sheriff's Department on Monday, May 15. (See item 14)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

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

1. *May 16, Capitol Times (WI)* — **Citizens Utility Board claims major flaws with new transmission line.** The Citizens Utility Board (CUB) has called on the Public Service Commission of Wisconsin to investigate "serious" flaws in the design of the controversial Arrowhead−Weston power line that it says could damage power plants and cause blackouts. The doomsday scenario would be a cascading outage similar to the huge blackout that hit the eastern U.S. in August 2003, said Charlie Higley, CUB executive director. The $420 million line is being constructed by Wisconsin Public Service Corp. under contract to American

Transmission Company (ATC). CUB stated that the 345−kilovolt line is undersized in capacity and will not perform as expected. Higley raised the issues after an in−depth analysis by Larry Thiele, an independent consulting electrical engineer. Higley said, "The Arrowhead line will likely not work when it's most needed...And that's when it's helping support other transmission lines in the region while power is flowing heavily. That's when the line is most vulnerable." CUB said Thiele's analysis shows that the Arrowhead line will not work properly if an outage occurs on the King−Eau Claire−Arpin transmission line, the only high−capacity line connecting Wisconsin directly to Minnesota.
Source: http://www.madison.com/tct/business/index.php?ntid=84025&ntp id=0

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

2. *May 17, Government Computer News* — **Department of Defense resumes security clearance investigations.** The Defense Security Service has come up with funding to immediately resume processing initial secret level security clearances for industry, the U.S. Department of Defense agency said Tuesday, May 16. Companies will not have to resubmit material for cases the Defense Industrial Security Clearance Office has been holding since the Pentagon halted processing April 28. The office will begin working on initial top−secret requests and periodic reinvestigation requests for both secret and top−secret clearances when more funding is received. The Defense Security Service stopped processing priority security clearances in April because of the lack of funds and the high volume of applications. In early May, it stopped processing industry requests for new personnel security investigations and periodic reinvestigations.
Source: http://www.gcn.com/online/vol1_no1/40800−1.html

[Return to top]

Banking and Finance Sector

3. *May 17, Government Accountability Office* — **GAO−06−495: Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs.** The Government Accountability Office (GAO) previously reported on how large information resellers like consumer reporting agencies obtain and use Social Security numbers (SSNs). Less is known about information resellers that offer services to the general public over the Internet. Because these resellers provide access to personal information, SSNs could be obtained over the Internet. In this report, GAO examines the types of readily identifiable Internet resellers that have SSN−related services and characteristics of their businesses, the extent to which these resellers sell SSNs, and the applicability of federal privacy laws to Internet resellers.

Highlights: http://www.gao.gov/highlights/d06495high.pdf
Source: http://www.gao.gov/highlights/d06495high.pdf

4. *May 16, Websense Security Labs* — **Multiple Phishing Alert: Creditunions.com, Kentucky Telco Federal Credit Union, United Heritage Bank, SurePayroll.** Websense Security Labs has received reports of four new phishing attacks. The first targets customers of Creditunions.com. The spoofed e−mail message claims that, due to multiple fraudulent activities, all customers are being asked to verify their accounts. Another phishing attack targets customers of Kentucky Telco Federal Credit Union. Users receive a spoofed e−mail message, which claims that the Internet banking services are due for renewal, and that they will be cancelled if action is not taken immediately. The third phishing attack targets customers of United Heritage Bank. Users receive a spoofed e−mail message, which claims that the Internet banking services are due for renewal, and that they will be cancelled if action is not taken immediately. A fourth phishing attack targets users of the SurePayroll service. Users receive a spoofed e−mail message, which claims that that their account will be suspended due to an unsuccessful access attempt. This email message is personalized by including the name of the individual targeted in the attack. All messages contain a link to a phishing Website where personal information is solicited.
   Screenshots of above attacks:
   Creditunions.com: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =487
   Kentucky Telco Federal Credit Union:
   http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =488
   United Heritage Bank: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =489
   Surepayroll: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =490
   Source: http://www.websensesecuritylabs.com/alerts/

5. *May 16, Clarion Ledger (MS)* — **BancorpSouth alerts customers to "phishing" attempts over weekend.** Bankers and Mississippi state officials warned consumers Monday, May 15, of a new round of scam e−mails that popped into incoming boxes over the weekend. One e−mail links to a pirated version of the BancorpSouth Website where prompts will accept credit card numbers, personal identification numbers, and other information. Although BancorpSouth is based in Tupelo, the fact that it operates in five other states makes it a target for scams. The bank is the largest Mississippi−based bank with $11.8 billion in assets. When filled out, the Website shows a statement asking the account holder to "allow at least 72 hours for the case to be investigated and we strongly recommend not to make any changes to your account in that time." Doing so gives the scam operators time to clean out the bank account.
   Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/2006 0516/NEWS/605160375

6. *May 16, Finextra* — **Pre−paid Internet payment card launched in the UK.** A plastic payment card that can be loaded with funds at e−pay mobile top−up terminals and used to pay for purchases made via the Internet has been launched in the UK. TeleGlobal says its new Snap card will enable customers who do not have a credit or debit card, or do not want to use their credit card on the Internet, to make online purchases. Erik Holst−Roness, chief executive of TeleGlobal, says: "The kind of people who will benefit range from kids who want to download music and games, to the thousands of families without credit cards, to people who don't want to put their credit details on the Internet or those who just want to make their online purchases

private." He says online merchants can now connect with an entirely new group of consumers without the fear of fraud.
Source: http://finextra.com/fullstory.asp?id=15319

7. *May 15, Computerworld Today (Australia)* — **Social engineering replaces guns in bank heists.** Australia's banking industry is under threat due to a heavy reliance on Single Socket Layer (SSL) encryption that hackers are increasingly finding their way around. There are no "stick−em−up" dramatics in today's million−dollar bank heists, but it simply involves the use of SSL−evading Trojans and refined phishing techniques. Australia's Computer Emergency Response Team (AusCert) says its research proves attacks are on the rise. AusCert general manager Graham Ingram said a false sense of security surrounds SSL encryption. This reliance on Internet browser encryption means banking sessions can be hijacked by Trojans and key−logging programs, especially if users engage in lax security protocols and don't use current anti−virus signatures. The bottom line is that social engineering tricks are circumventing Internet banking encryption. Neal Wise, director of security firm Assurance, said SSL does serve a good purpose but leaves users prone to a "man in the middle"−type attack.
Source: http://www2.csoonline.com/blog_view.html?CID=21091

[Return to top]

Transportation and Border Security Sector

8. *May 17, Taunton Gazette (MA)* — **Tipped train closes roads, schools.** Residents of Taunton, MA, were returned to their homes Wednesday, May 17, a day after heavy rains caused a train carrying hazardous materials to derail, prompting authorities to shut roads, call for evacuations, and close two city schools. Emergency crews worked throughout the night to clean up the mess caused by six train cars owned by CSX Railroad, which derailed at 5:30 a.m. EDT Tuesday, May 16, authorities said. Officials believe that heavy rains washed out the tracks, causing the wreckage and forcing the evacuation of residents in about a dozen homes. Four of the derailed cars were carrying a hazardous material called sodium hydroxide, also known as lye or caustic soda, authorities said. It took the crew and officials over 12 hours to correct the train cars, working well after midnight.
Source: http://www.tauntongazette.com/site/news.cfm?newsid=16648672&BRD=1711&PAG=461&dept_id=24232&rfi=6

9. *May 17, Associated Press* — **Teen creates disturbance at Buffalo airport.** A teenager was charged with disorderly conduct after shouting "It's time to die" while ripping off a backpack and reaching inside it at Buffalo Niagara International Airport. Alif Chowdhury, 16, and his father, Ehsan Chowdhury, both of Garden City, NY, were outside the terminal prior to their scheduled flight to John F. Kennedy International Airport about 9:30 p.m. EDT Monday, May 15, when passersby became suspicious of the youth's behavior and alerted airport police. When questioned by officers, Ehsan Chowdhury was cooperative but his son become more agitated and combative, said C. Douglas Hartmayer, spokesperson for the Niagara Frontier Transportation Authority, which operates the airport. "He did say things like −− apparently to his dad −− 'It's time to die…I'm not afraid to die,'" Hartmayer said. "And he ripped off his backpack and tried to pull something out of his backpack while saying, 'I'll kill you. It's time to die.'" Officers subdued the youth, who was dressed in a long white robe. He was charged with

two counts of disorderly conduct and taken to Erie County Medical Center in Buffalo for a psychiatric evaluation. FBI spokesperson Maureen Dempsey said agents interviewed the youth and determined there was no terrorism threat.
Source: http://www.usatoday.com/travel/flights/2006−05−16−airport−th reats_x.htm

10. *May 17, Southern Illinoisan* — **Illinois ranks high in Amtrak subsidies.** Illinois is second only to California when it comes to subsidizing Amtrak service, according to updated figures from the nation's passenger rail service. Under the state's new budget, Illinois will pay a total of $24 million to Amtrak in order to boost the number of trains running through the state. Illinois' amount is up from $12 million last year. California spends $72.8 million. In all, 12 states will spend about $161 million to subsidize Amtrak service in the coming years. In the Midwest, those include Michigan and Wisconsin, both of which spend $6.2 million, and Missouri, which has budgeted $7 million to increase the number of trains.
Source: http://www.southernillinoisan.com/articles/2006/05/17/top/16 347600.txt

11. *May 17, NBC10 (RI)* — **Southwest planes turn around minutes from Rhode Island airport.** Two Southwest Airlines flights left Baltimore on Monday night, May 15, bound for Rhode Island, but it the flight became a back−and−forth odyssey for dozens of passengers. NBC 10 reported that the planes turned around in flight just before midnight. The passengers said the pilots told them they were turning back because there was no one in the control tower at TF Green Airport in Warwick, RI. When they landed early Tuesday morning, May 16, the passengers had to camp out the rest of the night at the airport in Baltimore. The control tower at TF Green closes at midnight, and a spokesperson from Southwest Airlines said the airline did request that it remain open. A Federal Aviation Administration spokesperson, however, said based on control tower recordings, Southwest's version of events is not true. "Southwest made a decision to return to Baltimore after the pilot attempted to make a landing ... [and] missed his approach," spokesperson Jim Peters said. "Based on conversations, it was not necessary for the tower to be open when that plane landed." Peters said it is possible for flights to land without someone being present in the control tower.
Source: http://www.turnto10.com/news/9227658/detail.html

12. *May 16, eWeek* — **Logan airport to implement baggage, passenger RFID tracking.** Boston's Logan International Airport officials plan to implement an RFID project that will track customers and their baggage from arrival to final destination. Dubbed SEATS, or Secure Environment for Airport Terminal Systems, the system tracks passengers from the time they arrive at the airport and check into a self−service boarding pass kiosk to the time they board an airplane. Baggage, tagged with the chipless RFID sticker, is simultaneously tagged. An integrated boarding pass kiosk and bag accepter again scans the traveler's ID and takes a photo that is printed on baggage tags. An agent check−in and bag accepter scans the photo ID and verifies the bag tags, and an in−line bag−conveyer reader with ramp loader and reader track the bag through the system. Finally, a gate boarding pass reader confirms the passenger has boarded. Because the system is based on chipless RFID technology, it's said to be able to withstand exposure to the static electricity that's generated by huge luggage conveyers and baggage scanning systems found in airports.
Source: http://www.eweek.com/article2/0,1895,1962690,00.asp

13.

May 16, GovExec — **President sets plan to increase Border Patrol, send in Guard.** President George Bush has announced a temporary program to send National Guard troops to the southern border to support border control agents. Bush said that as many as 6,000 Guard members will be deployed to the border with Mexico while the government implements an initiative to add 6,000 border control officers by the end of 2008. Bush said the initial commitment of the Guard would be one year, and then the number would decline as new border control officers are hired. Border control agents will perform direct law enforcement activities, while Guard members will assist by operating surveillance systems, analyzing intelligence, installing fences, and vehicle barriers, building patrol roads and providing training, Bush said. Bush said the federal government would also help to increase the use of local and state police to combat illegal immigration.
Source: http://www.govexec.com/story_page.cfm?articleid=34087&dcn=to daysnews

14. *May 16, Marshall Democrat−News (MO)* — **Theft reported from Missouri railroad substation.** A theft from a Union Pacific Railroad substation and an attempted burglary at an AT&T Wireless substation were reported to Missouri's Saline County Sheriff's Department on Monday, May 15. Authorities said an employee with Union Pacific contacted the sheriff's department around 9:45 a.m. CDT Monday to report a theft from a substation located near the Eastwood viaduct on the eastern edge of Marshall, MO. The employee told a deputy that a suspect had apparently crawled under a gate and taken items including 1,000 feet of copper cable encased in black insulation, a steel plate, and a fire extinguisher. The copper cable was valued at $3,000, the steel plate at $300, and no value was given for the fire extinguisher. A call was received by the sheriff's department a little after 10 a.m. on Monday from an employee with AT&T Wireless to report an attempted forced entry at the company's Marshall Junction repeater site. Nothing was taken.
Source: http://www.marshallnews.com/story/1152970.html

[Return to top]

Postal and Shipping Sector

15. *May 17, DMNews* — **U.S. Postal Service expands personalized postage for businesses.** The U.S. Postal Service (USPS) has signed contracts with three qualified PC Postage vendors, letting the vendors produce customized postage to be used on First−Class Mail, Priority Mail, and Express Mail for personal and commercial use. This type of postage allows the buyer to personalize postage with pictures or images using Customized PC Postage technology. This is the third phase of the market test for customized postage. It will run through May 16, 2007, with an option for the USPS to extend the test for a second year. The third test removes the restrictions around commercial images that were in place for the second market test. Customized postage has two parts: A customer−supplied image and a state−of−the−art secure bar code. All customized postage is compatible with the Postal Service's automated mail processing systems. Authorized vendors will determine pricing and are expected to price their products based on the value provided to the consumer. The USPS said its role is to authorize and monitor qualified providers.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3692 9

16.

May 17, Associated press — **UPS announces $1 billion expansion.** UPS Inc. announced a $1 billion expansion at its main air hub, next to Louisville, KY's main airport, on Wednesday, May 17, that will add more than 5,000 jobs as the world's largest shipping carrier anticipates strong growth in global commerce. The project will add 1.1 million square feet to the company's vast sorting complex known as UPS Worldport. The computerized sorting system installed four years ago will feature 197 miles of conveyors once the expansion is finished by 2010. The expansion will help meet customer demands for "more speed, more reach and more capacity," said Bob Lekites, UPS vice president of airline and international operations. "We're making Worldport, already the world's largest package facility, even bigger." "We anticipate strong growth in global trade to continue for years to come," UPS Chairman and CEO Mike Eskew said in a statement. "Expanding the centerpiece of our worldwide infrastructure is absolutely necessary to support the long−term needs of our customers." State officials were expected to consider an incentive package Wednesday for the Atlanta−based shipping company. About 260 flights come in and out of the air hub each day that connect it with more than 200 countries and territories worldwide.
Source: http://www.nytimes.com/aponline/business/AP−UPS−Expansion.html?_r=1&oref=slogin

[Return to top]

Agriculture Sector

17. *May 17, USAgNet* — **Drought conditions push cow slaughter up.** Through late April 2006 cow slaughter was above last year's. Federally inspected cow slaughter totaled 1.626 million head from January through April this year, about 47 thousand head (three percent) more than last year. All of the increase was attributable to an increase in beef cow slaughter. Beef cow slaughter during the first four months of 2006 totaled 0.878 million head, up about 72 thousand head (nine percent) compared to the same period in 2005. Poor pasture conditions in some key states, such as Texas, are motivating the increase in beef cow slaughter. This becomes apparent when the comparisons between 2005 and 2006 are made month−by−month. Early in the year beef cow slaughter was larger than in 2005, but the increases in weekly slaughter volume averaged less than five percent during January and about one percent during February. However, during March and April weekly beef cow slaughter averaged 13 and 17 percent above 2005's.
Source: http://www.usagnet.com/story−national.cfm?Id=921&yr=2006

18. *May 17, Illinois Farm Bureau* — **Extension diagnostic system upgraded for quicker response to soybean rust.** The diagnostic system that provided some of the first images of the soybean aphid invasion in 2003 recently received an upgrade to improve response time to Asian soybean rust and other crop threats. University of Illinois Extension and the Illinois Department of Agriculture (IDOA) recently announced plans to upgrade Extension's Digital Distance Diagnostics Imaging System. New digital cameras −− used to capture images of any unknown insect, weed, or disease −− will replace outdated cameras and will eliminate the need for floppy disks. The updated cameras also will provide a higher resolution of samples and allow plant pathologists to zoom in on particular features of a plant to diagnose potential problems.
Source: http://farmweek.ilfb.org/viewdocument.asp?did=9127&r=0.67399 23

19. *May 16, Associated Press* — **Animal−rights activist who filmed egg farm sentenced.** An animal−rights activist drew a maximum six−month jail sentence Tuesday, May 16, for sneaking onto New York state's largest egg farm to videotape thousands of chickens confined to small wire cages. Adam Durand was convicted earlier this month on three counts of criminal trespassing, a misdemeanor. He was sentenced to two consecutive terms of 90 days, fined $1,500, ordered to serve 100 hours of community service and placed on probation for a year. Durand denied breaking into a shed during three nighttime visits in 2004, saying he climbed in through a hole in a wall. He also said he had no intention of removing birds from the farm operated by supermarket chain Wegmans where 700,000 hens produce more than a half−million eggs a day. Two friends who accompanied Durand to the farm pleaded guilty to trespassing and petit larceny, and were placed on probation.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−egg farm0516may16,0,7018327.story?coll=ny−region−apnewyork

[Return to top]

Food Sector

20. *May 17, United Press International* — **Tainted muffins sicken 18 in Texas.** At least 18 employees of a Dallas, TX, high school reportedly became ill after consuming muffins suspected of being laced with a drug. They were treated at a local hospital after complaining of dizziness, nausea and increased heart rate. Authorities suspect the muffins in the teachers' lounge were laced with a street or over−the−counter drug. A school official said two boxes of muffins were delivered by a man who apparently was recorded on a security video. The man said the sweets were part of an Eagle Scout project, the report said. The FBI is assisting Dallas authorities investigating the incident.
Source: http://upi.com/NewsTrack/view.php?StoryID=20060517−120513−57 14r

[Return to top]

Water Sector

21. *May 16, Monterey County Herald (CA)* — **Tainted water likely causing rashes, burning.** The skin and eye irritation San Jerardo, CA, residents have been experiencing could be linked to the high contamination levels in its water system, Monterey County health officials have found. A health assessment done to evaluate residents of the San Jerardo Cooperative, a farm worker community, found that 80 percent of the adults surveyed had skin rashes and 71 percent had either burning eyes or itchy skin after showering, health officer Hugh F. Stallworth told The Herald. Health Department nurses evaluated 55 residents from San Jerardo −− 48 adults and seven youths, or about 20 percent of the cooperative's population. The sample was not random, as only those who wanted to be evaluated −− or could take the time off work −− took part in the testing. But the size of the group and the type of complaints are a good indication that the problem comes from the water.
Source: http://www.mercurynews.com/mld/mcherald/living/community/145 93235.htm

[Return to top]

Public Health Sector

22. *May 17, Associated Press* — **World Health Organization confirms more bird flu deaths.** The World Health Organization (WHO) on Wednesday, May 17, confirmed five more bird flu deaths in Indonesia, raising the total number of fatal human cases of H5N1 in the sprawling archipelago to 30. Four of the new deaths were in North Sumatra province and one was in the country's second largest city, Surabaya, in East Java province. Indonesia last year overtook Thailand to become the country with the second−highest bird flu death toll after Vietnam, which has 42 confirmed deaths. While those countries have recently reported success in containing the virus, it continues to rapidly spread across Indonesia. The virus has infected poultry populations in 27 of 33 Indonesian provinces.
Source: http://edition.cnn.com/2006/HEALTH/conditions/05/17/indonesi a.birdflu.ap/

23. *May 17, Associated Press* — **New antibiotic aimed at resistant germs.** Researchers have found a potentially valuable new antibiotic in a scoop of soil from South Africa. Using a novel screening technique, scientists have found a chemical compound that is effective against germs that have developed resistance to existing antibiotics. The discovery could provide a vital weapon in the ongoing battle against infectious bacteria, which are constantly evolving defenses to the drugs used against them. Researchers tested extracts of fungi, plants and other natural substances against bacteria with a genetically engineered Achilles' heel. Because the bacteria were weakened, any compound that harmed them would have a more dramatic effect and thus be easier to identify. The scientists also chose the genetic handicap carefully, placing it in a metabolic pathway that is not attacked by any major existing antibiotics. That increased the likelihood that any promising compound they discovered would be something for which the bacteria had not yet developed a resistance.
Source: http://www.forbes.com/business/businesstech/feeds/ap/2006/05 /17/ap2753815.html

24. *May 16, Government Health IT* — **Credentialing strategy sought.** Protecting the public health, particularly in emergencies, requires sophisticated information systems that can quickly and accurately assess the qualifications of doctors and nurses in multiple jurisdictions, said panelists at a recent meeting of health care information technology specialists in Washington, DC. To get ready, public and private organizations at the national, state and local levels are developing independent IT solutions for verifying health care professionals' identities, credentials, expertise and competence, panelists said. A primary objective of enhanced verification is to thwart the "fakers, con artists and artful dodgers" who would subvert the system for confirming medical professionals' qualifications. Last year's hurricane disaster on the Gulf Coast underscored the necessity of bolstering the verification of medical credentials. Much of the health care infrastructure in the affected area was hobbled by hurricanes Katrina and Rita, and verifying the credentials of doctors who arrived to provide aid was difficult. Confirming the qualifications of doctors who had left the area to practice medicine elsewhere was challenging, too.
Source: http://govhealthit.com/article94540−05−16−06−Web

[Return to top]

Government Sector

25. *April 17, Government Accountability Office* — **GAO−06−383: Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information (Report).** A wide array of cyber and physical assets is critical to America’s national security, economic wellbeing, and public health and safety. Information related to threats, vulnerabilities, incidents, and security techniques is instrumental to guarding these critical infrastructures against attacks and mitigating the impact of attacks that may occur. The ability to share security−related information can unify the efforts of federal, state, and local government as well as the private sector, as appropriate, in preventing and minimizing terrorist attacks. The Critical Infrastructure Information Act of 2002 was enacted to encourage nonfederal entities to voluntarily share critical infrastructure information and established protections for it. The Department of Homeland Security (DHS) has a lead role in implementing the act. The Government Accountability Office (GAO) was asked to determine (1) the status of DHS’s efforts to implement the act and (2) the challenges it faces in carrying out the act. GAO is recommending that the Secretary of Homeland Security, among other things, better define DHS’s and other federal agencies’ critical infrastructure information needs, and explain how DHS and the other agencies will use the information received from the private sector. In oral comments on a draft of this report, DHS concurred with our findings and recommendations.
Highlights: http://www.gao.gov/highlights/d06383high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−383

[Return to top]

Emergency Services Sector

26. *May 15, Federal Computer Week* — **Military interoperability test begins.** Combined Endeavor 2006, a two−week operation to test the interoperability of vital communication systems for multinational forces, began on Monday, May 15 in Lager Aulenbach, Germany. The U.S. European Command, in cooperation with the German Ministry of Defense, is sponsoring the communications and information systems interoperability exercise. Forty−one countries, including members of NATO and Partnership for Peace, are participating. The vendor providing the core network infrastructure for the exercise will test communications deployed in humanitarian, peacekeeping, and disaster relief efforts.
Source: http://fcw.com/article94524−05−15−06−Web

27. *May 15, Clayton News−Daily (GA)* — **Georgia officials test emergency response below fifth runway.** There is a three−car pile up involving a gasoline tanker leaking gas and a car on fire inside a tunnel just below where jumbo jets are touching down and taking off at Hartsfield−Jackson Atlanta International Airport in Atlanta, GA. All of those elements add up to a calamity that Clayton County Fire Chief Alex Cohilas said would be a worst case scenario for public safety agencies in charge of handling wrecks, fires, and spills where the new fifth runway crosses Interstate 285. It’s the only one in the country that crosses a major freeway, so the runway has required its own specific response plan, Cohilas said. To tune up for the Atlanta airport’s fifth runway opening later this month, fire and emergency personnel reacted to a

staged−version of the potential crash on Monday, May 15.
Source: http://www.news−daily.com/homepage/local_story_135235901.htm l?keyword=leadpicturestory

28. *May 15, Mount Vernon News (OH)* — **Exercise helps test Ohio county's preparedness.** Knox County, OH, tested its preparedness on Saturday, May 13 with a morning exercise designed to evaluate disaster response in the county, and to highlight areas for improvement. The exercise centered around a fictional automobile accident off of Ohio 3 which left multiple victims and leaking stockpiles of propane and anhydrous ammonia. The exercise began with a 9−1−1 call. The Emergency Operation Center (EOC) was activated immediately and within a half−hour of the accident, officials from all over Knox County were congregated in the same room, gathering facts from their personnel at the scene and sharing the information with the other agencies. Agencies present at the EOC included the Knox County Sheriff's Office, Ohio Department of Transportation, Knox County Health Department, Knox Community Hospital, Knox County Commissioners, Knox County Emergency Management Agency, and the Ohio State Highway Patrol. The exercise also took media relations into account. During the briefing, reports of rumors came into the EOC, including phone calls claiming the incident was a planned attack and reports that the town of Fredericktown was being affected. Officials said that in a real situation they would immediately work with local media outlets to squash any potentially harmful rumors.
Source: http://www.mountvernonnews.com/local/06/05/15/drill.html

[Return to top]

Information Technology and Telecommunications Sector

29. *May 16, eWeek* — **Researchers warn of fake anti−spyware.** The latest report issued by Finjan's Malicious Code Research Center highlights the growth of several emerging breeds of cyber−attack, including the increasing popularity of so−called "ransomware" and viruses that are being spread via fake anti−spyware applications. The anti−virus software maker's research arm said in its Web Security Trends Report, issued on May 16, that the growth of "rogue anti−spyware" and the emergence of hackers looking to hold stolen corporate data up for ransom are two of the fastest growing trends in the security threat landscape. Virus rootkits continue to pose one of the most prevalent and challenging obstacles for IT administrators to overcome, according to the study. In these attacks, hackers disguise the malware in programs advertised online as free anti−spyware applications. Once downloaded onto a user's computer, the applications may deliver their own payloads of malicious code or expose affected machines to subsequent attacks. In some cases, the false anti−spyware tools even run fake computer security scans that claim to find existing spyware programs on infected devices. The software then directs the computer's user to a Website where the user is encouraged to purchase a full version of the free application already on the PC.
To download report, follow link and click on "Security Trends Report":
http://www.finjan.com/Content.aspx?id=827#SecurityTrendsRepo rt
Source: http://www.eweek.com/article2/0,1895,1963097,00.asp

30. *May 16, Security Focus* — **Apple Mac OS X multiple security vulnerabilities.** Apple Mac OS X is reported prone to multiple security vulnerabilities. These issues affect Mac OS X and

various applications including Safari, Preview, Finder, QuickTime, and BOMArchiveHelper. A remote attacker may exploit these issues to execute arbitrary code and/or trigger a denial−of−service condition.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/17634/info
Solution: http://www.securityfocus.com/bid/17634/solution
Source: http://www.securityfocus.com/bid/17634/discuss

31. *May 16, CNET News* — **Sun promises to open−source Java.** Open−source advocates have urged Sun Microsystems for years to open−source the Java programming language, but the company has resisted, citing compatibility concerns and fear of losing control. Now the company has promised that Java will become open−source. At the JavaOne developer conference in San Francisco on Tuesday, May 16, Sun Microsystems CEO Jonathan Schwartz and Rich Green, the company's new executive vice president of software, officially announced that Java will become open−source. "At this point, it is not a question of whether, but it is a question of how" Sun will open−source Java, Green said. The previous concerns have not gone away, said Green, who rejoined the company earlier this month. "There are two battling forces here," he said. One force is the demand for Sun to open up Java, and the other is concern for compatibility. "This is something for us to go figure out," he said. Green didn't give a timeline or details of how Sun would proceed.
Source: http://news.com.com/Sun+promises+to+open−source+Java/2100−7344_3−6072760.html?tag=nefd.lede

32. *May 16, Information Week* — **Rival teams Sun, Microsoft form alliance for Java and .Net.** Sun Microsystems and Microsoft are teaming up to make their rival camps work more cooperatively. On Wednesday, May 17, the two will announce new ways in which Java and Microsoft's .Net framework will cooperate in offering security, messaging, and quality of service in building enterprise services.
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=2VMP3AT0CEFZGQSNDBGCKHSCJUMEKJVN?articleID=187203342

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT reports that Apple has released Apple QuickTime 7.1 to correct several vulnerabilities. Apple QuickTime 7.1 resolves multiple vulnerabilities in the way different types of image and media files are handled. An error in the AppKit framework allows an application to read characters entered into secure text field in the same window session. An attacker could exploit these vulnerabilities by convincing a user to access a specially crafted image or media file with a vulnerable version of QuickTime. Since QuickTime configures most web browsers to handle QuickTime media files, an attacker could exploit these vulnerabilities using a web page.

US−CERT recommends that Apple QuickTime users:

Upgrade there software to Apple QuickTime 7.1:
http://www.apple.com/support/downloads/quicktime71.html

Disable QuickTime in your web browser to prevent attackers from exploiting this vulnerability by persuading a user to access a specially crafted file with a web browser.

Note: Disabling QuickTime in your web browser will defend against this attack vector.

For more information please review:

Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/

Standalone Apple QuickTime Player:
http://www.apple.com/quicktime/download/standalone.html

Mac OS X: Updating your software:
http://docs.info.apple.com/article.html?artnum=106704

VU#570689 Apple QuickTime FlashPix integer overflow:
http://www.kb.cert.org/vuls/id/570689

VU#289705 Apple Quicktime JPEG integer overflow:
http://www.kb.cert.org/vuls/id/289705

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 12198 (−−−), 25 (smtp), 41170 (−−−), 6588 (AnalogX), 49200 (−−−), 32459 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General 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 dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 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.