Department of Homeland Security Daily Open Source Infrastructure Report for 25 May 2007

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- KSBI−TV reports on Wednesday night, May 23, Tulsa, Oklahoma's International Airport came to a stand still when a surge knocked out power; planes sat on the runway while workers drove bags to the front of the airport into the hands of passengers, because the inbound baggage conveyor system did not work. (See item 15)

- The Bush administration on Wednesday, May 23, pressed senior Chinese officials to bolster the safety of food exports, a key issue for U.S. consumers after melamine, a chemical used in plastics and fertilizers, surfaced in imported pet food. (See item 20)

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 23, Associated Press* — **New York nuclear sirens promised by August 24.** When the owner of the Indian Point nuclear power plant in New York decided it couldn't meet an April 15 deadline for installing a new emergency siren system, it asked for an extension to August 31. The Nuclear Regulatory Commission (NRC) refused, fined Entergy Nuclear $130,000 and demanded that it come up with a new plan. On Wednesday, May 23, Entergy said its new plan was to have the sirens up and running by August 24, a week earlier than its original request. The 150 sirens are meant to alert residents within ten miles to any emergency at the

two−reactor installation in Buchanan on the Hudson River, 35 miles north of midtown Manhattan. Despite extensive testing by Entergy and a 2 1/2−month extension granted by the NRC in January, many sirens failed to respond to a radio activation signal during their final test before the deadline. NRC spokesperson Diane Screnci said the commission would examine the plan "to make sure it's acceptable."
Source: http://www.chron.com/disp/story.mpl/ap/fn/4830802.html

2. *May 23, The Northwestern (WI)* — **Power companies say they'll be able to handle summer peaks.** Wisconsin−based American Transmission Co. (ATC) said improvements continue to be made to the transmission system around the state as it heads into peak months for electricity consumption. "We're prepared well for moving into the summer, and we expect the ATC system is going to be able to handle reasonable things that get thrown at it," Teresa Mogensen, ATC director of system operations, said. American Transmission Co. builds, operates and owns about 9,100 miles of transmission lines and 480 substations in Wisconsin, Michigan, Minnesota and Illinois. Wisconsin Public Service Corp. spokesperson Kerry Spees said, "We should be able to handle the electric load even in extreme conditions...Although we know things are better now in the transmission arena, we're still very, very susceptible to problems if we lose one of the major transmission lines." Spees said the state's transmission system has been upgraded in the past few years. ATC says it expects to invest about $400 million in construction this year, which includes completing a transmission line from Wausau to Duluth expected to be finished by the summer of 2008.
Source: http://www.thenorthwestern.com/apps/pbcs.dll/article?AID=/20070523/GPG03/70523124/1247/OSHbusiness

3. *May 23, Reuters* — **U.S. finds no illegal activity behind pump spike.** The U.S. Federal Trade Commission said on Wednesday, May 23, it has not uncovered any anti−competitive behavior or other illegal business practices by oil companies that have caused current record gasoline prices. "We have not seen evidence of illegal activity at this time," Michael Salinger, director of the FTC's Bureau of Economics, said after testifying at a congressional Joint Economic Committee hearing on oil industry mergers and gasoline costs. The national price for regular unleaded gasoline hit a record high of $3.22 a gallon this week, up more than $1 since the beginning of February, according to the Energy Department. Oil industry critics charge the giant mergers of several oil companies almost a decade ago has left only five major domestic oil firms controlling the majority of U.S. refining capacity, giving them the ability to restrict supplies and set gasoline prices. The American Petroleum Institute trade group said the giant oil company mergers have led to production efficiencies and cut operating costs that have actually benefited consumers.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/05/23/AR2007052301315.html

4. *May 22, SC Magazine* — **Los Alamos increases security in wake of data breach.** The theft of classified information by a contractor's former employee has forced the Los Alamos National Laboratory to implement a variety of tactical and strategic security policies commonly found in a private enterprise. The lab has disabled all ports, including USB ports, on classified computers −− some via physically gluing the port shut, others with locking devices or software −− and has begun encrypting personal information on laptop hard drives.
Source: http://scmagazine.com/us/news/article/659068/los−alamos−beef

s−security−wake−data−breach/

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *May 24, Newark Advocate (OH)* — **Man killed when tanker crashes, explodes in creek.** A 22−year−old Iraq veteran was killed Wednesday evening, May 23, when the tanker truck he was driving flipped off Cherry Valley Road into Raccoon Creek and exploded on impact in Newark, OH. Steven Hileman was driving a tanker carrying 6,000 gallons of unleaded fuel and 2,400 gallons of diesel fuel from Marathon's Heath terminal when he was killed in the crash on Cherry Valley Road near Reddington Road. The crash left Cherry Valley Road closed at least through Thursday morning. About half of the tanker's fuel burned, and a small amount spilled into the creek. Officials said no long−term health effects will result from the explosion, but Licking Memorial Hospital received some calls from people complaining about eye irritation, difficulty breathing and a metallic taste in their mouths. Police performed a voluntary evacuation of the homes nearest the scene because the fire and the spill were contained.
Source: http://www.newarkadvocate.com/apps/pbcs.dll/article?AID=/20070524/NEWS01/705240334/1002

[Return to top]

Defense Industrial Base Sector

6. *May 24, Government Accountability Office* — **GAO−07−461: Defense Infrastructure: Actions Needed to Guide DoD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure (Report).** The Department of Defense (DoD) relies on a network of DoD and non−DoD infrastructure assets in the United States and abroad so critical that its unavailability could hinder DoD’s ability to project, support, and sustain its forces and operations worldwide. DoD established the Defense Critical Infrastructure Program (DCIP) to identify and assure the availability of mission−critical infrastructure. The Government Accountability Office (GAO) was asked to evaluate the extent to which DoD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure. GAO analyzed relevant DCIP documents and guidance and met with officials from more than 30 DoD organizations that have DCIP responsibilities, and with Department of Homeland Security (DHS) officials involved in protecting critical infrastructure. GAO recommends DoD take several actions to improve the efficiency and effectiveness of DCIP operations. Actions include developing a comprehensive management plan; issuing a chartering directive defining the relationship between the directorates responsible for DCIP and antiterrorism missions; and identifying non−DoD−owned critical infrastructure for DHS to consider in its assessments. DoD concurred with all of GAO’s recommendations.
Highlights: http://www.gao.gov/highlights/d07461high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−461

[Return to top]

Banking and Finance Sector

7. *May 24, SC Magazine* — **Anti−phishing database launched to halt attacks.** The Anti−Phishing Working Group will share information and analysis on phishing attacks and trends stored in a central database that will be launched in July. Mike Dodson of Mirapoint said, “This new initiative means that phishing sites will be easier than ever to track and destroy, with fraudulent activities measurable in hours rather than days.” However, Dodson believes that “If banks adopted and promoted a unified code of conduct regarding email policy, clearly stating how they intend to communicate with their customers, then phishers would quickly run out of victims. But, the slew of competing policies currently in place just allows attackers to take advantage of this confusion."
Source: http://www.securecomputing.net.au/news/antiphishing−database−launched−to−halt−attacks.aspx

8. *May 24, Finextra (UK)* — **Card skimmers loot $100,000 from Westpac ATM users.** Australia's Westpac has suspended 900 customer cash cards following the discovery of a skimming device at an ATM in Melbourne. The withdrawals, totaling $100,000, affected approximately 75 customers and have been traced to Toronto in Canada. Westpac is midway through a program to equip all of its ATMs with anti−skimming technology. The "Jitter" system vibrates the card as it enters the ATM and renders the mag−stripe data unreadable. The bank has so far installed the technology at 70 percent of its cash machines nationwide and says incidents of skimming at protected machines has fallen to zero.
Source: http://finextra.com/fullstory.asp?id=16961

9. *May 24, Websense Security Labs* — **Malicious Website/malicious code: Better Business Bureau scam.** Websense Security Labs has received reports of a new e−mail spam variant similar to an attack launched early this year. The spoofed e−mail purports to be from the Better Business Bureau (BBB). The message claims that a complaint has been filed against the recipient's company. Attached to the message is a Microsoft Word document, supposedly containing additional details regarding the complaint. The Word document actually contains a Trojan Downloader that, when opened, attempts to download and install a keylogger. This keylogger uploads stolen data to an IP address in Malaysia.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=777

10. *May 23, Associated Press* — **Federal agencies ordered to eliminate personal data.** Plagued by regular breaches in the security of personal data, federal agencies were ordered Tuesday, May 22, to eliminate the unnecessary collection and use of Social Security numbers by early 2009. That order and several other new security measures against identity theft were outlined in a memo to all department and agency heads from Clay Johnson III, deputy director for management of the Office of Management and Budget (OMB). Johnson gave the agencies 120 days to review all their files for instances in which the use of Social Security numbers is superfluous and "establish a plan in which the agency will eliminate the unnecessary collection and use of Social Security numbers within 18 months." Beyond that, agencies were directed to review all information they have that could be used to identify an individual citizen or employee, to ensure such records are accurate and "to reduce them to the minimum necessary for the proper performance" of their duties. OMB spokesperson Sean Kevelighan said that by requiring agencies to reduce such data to a minimum, the risk of harm from identity theft will

decline.
Source: http://www.theeagle.com/stories/052307/nation_20070523034.ph p

11. *May 22, Websense Security Labs* — **Phishing Alert: Pentagon Federal Credit Union.** Websense Security Labs has received reports of a phishing attack that targets customers of Pentagon Federal Credit Union. Users receive a spoofed e−mail message that provides a link to a phishing site which attempts to collect personal and account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=775

[Return to top]

Transportation and Border Security Sector

12. *May 24, Associated Press* — **United schedules earlier flights to ease summer crunch.** Passengers booking morning flights on United Airlines this summer may have to set their alarm clocks a bit earlier. United Airlines, the nation's second−largest carrier, said Tuesday, May 22, that it is scheduling earlier departure times in about 20 U.S. cities starting in June, eyeing a summer air−travel crush that's expected to be worse than usual. "We're trying to make this change to improve our schedule — to optimize our revenue, better use our aircraft and provide our customers with more connection options," spokesperson Robin Urbanski said. A flight currently scheduled to leave Boston for Chicago at 6 a.m. EDT, for example, will depart next month at 5:44, giving passengers a chance for at least a dozen more connections out of Chicago’s busy O'Hare International Airport.
Source: http://www.usatoday.com/travel/flights/2007−05−24−united−ear ly−flights_N.htm

13. *May 24, Capital Times (WI)* — **Drivers take to the road for the holiday.** More Americans are expected to travel by car this year to start the summer than last year, according to AAA Wisconsin's latest survey, even though gasoline prices are almost 10 percent higher this year than a year ago. AAA Wisconsin spokesperson Pam Moen said, "Last year, we also had all−time high prices for gas, but people traveled in record numbers on all holidays." While several gas stations in Madison dropped their regular gallon price to $3.35 today, the move is more an aberration than a trend, as the average Madison price hit a new all−time high of $3.402 a gallon for regular unleaded today, according to the Oil Price Information Service. Despite the price, people still will travel. There's no indication Wisconsinites or others in America are willing to give up their freedom to drive, no matter what the price of gasoline. AAA estimates 38.3 million Americans will travel at least 50 miles this holiday, up 1.7 percent from Memorial Day 2006, with most −− 84 percent −− going by motor vehicle.
Source: http://www.madison.com/tct/news/136216

14. *May 24, Press−Register (AL)* — **Moving cargo aboard barges.** With the Choctaw Point container terminal set to open next year on Mobile River, shippers should take the opportunity to consider using Alabama's inland waterway system to move containerized cargo aboard barges, a new study concludes. Not only could the river network provide a reliable alternative to truck and railroad traffic, but it would also reduce congestion and pollution, according to the executive summary of the report, prepared for the Coalition of Alabama Waterway Associations Inc., a nonprofit group that includes the Alabama State Port Authority and the

Warrior−Tombigbee Waterway Association, both based in Mobile. "A lot of shippers aren't even aware what they can do with barges," Jerry Sailors, the coalition's secretary−treasurer and project manager for the study, said in an interview. Barges are typically used to move bulk cargo such as coal, grain and wood products, while containers −− essentially big metal boxes that can be easily loaded from ships on to rail cars or trucks −− are employed to transport higher−end goods. And although "container−on−barge" shipping has been successfully used in Europe and the Pacific Northwest, it has had "limited success" elsewhere in the United States, the report says.
Study: http://www.hansonengineers.com/project_reports/project_repor ts.htm
Source: http://www.al.com/business/press−register/index.ssf?/base/bu siness/1180017922238750.xml&coll=3

15. *May 24, KSBI−TV (OK)* — **Storms knocked out Oklahoma airport's power.** Wednesday night, May 23, Tulsa's International Airport came to a stand still when a surge knocked out power. Workers were unable to boot up their computers Thursday morning, because of a burned out power switch. Officials say the switch is hard to replace and a backup has to be ordered, delivered and installed. Generator power was being used. However, planes sat on the runway while workers drove bags to the front of the airport into the hands of passengers, because the inbound baggage conveyor system did not work.
Source: http://www.ksbitv.com/home/7667477.html

16. *May 24, Associated Press* — **Texas cruise−ship terminal evacuated after suspicious package detected.** Galveston's cruise−ship terminal was evacuated and ship passengers were kept on board after a police dog detected a suspicious package on the dock Thursday, May 24. Galveston port director Steve Cernak says the dog alerted officers to an unidentified substance in a package inside the Texas Cruise Ship Terminal at the Port of Galveston Thursday morning. Cernak says the K−Nine team was doing a routine sweep of the terminal before the scheduled arrival of the Carnival cruise ship Ecstasy when the package was detected. Cernak says he's unsure whether the dog was trained to detect explosives or other substances. But the terminal was evacuated and passengers kept aboard the Ecstasy as a precaution.
Source: http://www.kxan.com/Global/story.asp?S=6564017&nav=menu73_2_2

17. *May 24, Federal Computer Week* — **FAA to perform IT security for all of Transportation.** The Federal Aviation Administration (FAA) will provide information technology (IT) security for the Department of Transportation (DOT) by early fiscal 2008, which begins in October, said Dave Bowen, FAA chief information officer. The effort is part of a move to develop shared services to increase savings. FAA already conducts IT security around the clock to protect the air traffic control system and provides weekend and after−hours IT security for other DOT agencies. That's because IT security in other DOT agencies involves smaller operations and is limited to business hours. FAA is finalizing an agreement with the department to merge IT security operations and considering budgets for the service. FAA intends to get approval from the Office of Management and Budget to be named a Center of Excellence for IT security and market the IT security service to other agencies, particularly small agencies that lack the expertise and portfolio to afford a sophisticated security operation, said Dave Bowen, FAA chief information officer. FAA has saved $10 million through shared services.
Source: http://www.fcw.com/article102782−05−24−07−Web

18. *May 22, United Press International* — **System traces airliner bioterror pathogens.** Researchers in the United States have developed a system they say can identify terrorists who release bioterrorism agents aboard an airliner. Purdue University officials said Tuesday, May 22, the computer program is capable of tracing a pathogen to the specific seat where it was first released into the cabin whether it was intentional or inadvertent. The system is based on a series of sensors installed inside an airliner that detects the presence of germs in the cabin air. Using a series of mathematical models, the system can follow the substance to an area the size of a single seat and identify the individual passenger who was the point of origin so they can either be arrested or taken for medical care. The concept is called "inverse simulation" and makes use of data including airflow patterns and the temperature inside the cabin.
Source: http://www.upi.com/Security_Terrorism/Briefing/2007/05/22/system_traces_airliner_bioterror_pathogens/2653/

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

19. *May 24, Associated Press* — **Pin found in middle schooler's salad.** A student at Rocky Run Middle School in Fairfax, VA, found a straight pin at the bottom of her salad container Wednesday, May 23. She reported the discovery to school officials. The school then contacted police. Pins were found in food three times at Rachel Carson Middle School in Fairfax last month.
Source: http://www.wtopnews.com/?nid=25&sid=1149029

20. *May 23, Reuters* — **U.S. pushes China on food safety.** The Bush administration on Wednesday, May 23, pressed senior Chinese officials to bolster the safety of food exports, a key issue for U.S. consumers after a toxic chemical surfaced in imported pet food. The safety of food imports from China came under intense scrutiny after melamine, a chemical used in plastics and fertilizers, surfaced in U.S. pet food this year, killing pets and prompting wide recalls. Pet food scraps were used in some livestock rations, briefly halting marketing of some poultry, hogs and fish. Among the host of measures the administration is seeking are more transparent food regulation and permission to send U.S. audit teams to China. Currently, all vegetable protein imports from China are on "import alert," which means they get immediate inspection. The U.S. Food and Drug Administration is also beginning to check all shipments of toothpaste from China after a lethal chemical was found in Chinese toothpaste sold in the Dominican Republic and in Panama.

Source: http://www.alertnet.org/thenews/newsdesk/N23233687.htm

[Return to top]

Water Sector

21. *May 24, Agence France−Presse* — **Danaher to buy water treatment company ChemTreat.** Danaher Corp said it will buy ChemTreat Inc, a U.S. provider of water treatment services and products, for about $435 million. Danaher, the maker of industrial, medical and consumer products, said it expects the deal to be 'modestly accretive' to its earnings in 2008. ChemTreat generated 200 mln usd revenues in the most recent fiscal year and targets the boiler, cooling water and industrial waste water markets, Danaher said.
Source: http://www.forbes.com/business/feeds/afx/2007/05/24/afx37546 52.html

[Return to top]

Public Health Sector

22. *May 23, Agence France−Presse* — **Nigeria reports bird flu outbreak.** Health authorities reported Wednesday, May 23, an outbreak of the H5N1 bird flu virus in Nigeria's northern state of Zamfara, the official NAN news agency said. The virus was confirmed through tests on affected birds in Namaturu village and more than 200 birds had been culled to curtail the spread of the disease, said Aminu Abdulrazak from the state health ministry. Nigeria, Africa's most populous nation with some 140 million people, earlier this year reported west Africa's first human bird flu death. A 22−year−old woman died in Lagos on January 17 weeks after plucking and disembowelling a chicken.
Source: http://news.yahoo.com/s/afp/20070523/hl_afp/healthflunigeria_070523191253;_ylt=Ag8fljhGUkRFTk4TIJkHMwyJOrgF

23. *May 23, KUSA (CO)* — **Colorado man recovering from hantavirus.** A 30−year−old man is recovering after catching hantavirus, the second case of the potentially deadly disease this year. The Weld, CO, Department of Public Health and Environment announced Tuesday, May 22, the man is recovering from a case of hantavirus pulmonary syndrome. The man was exposed to the virus in northeast Colorado sometime during April. The first case of hantavirus in Colorado resulted in the death of a 28−year−old woman from Alamosa County earlier this month.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.9news.com/news/local/article.aspx?storyid=70613

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *May 23, Federal Emergency Management Agency* — **FEMA and federal agencies team up for hurricane response.** Federal Emergency Management Agency (FEMA) Administrator R. David Paulison, and Department of Homeland Security (DHS) Secretary Michael Chertoff joined with leaders from the National Oceanic & Atmospheric Administration (NOAA), the Air Force Reserve, and the U.S. Coast Guard stressing a strong commitment to federal agency teamwork as the overall plan for 2007 Hurricane season preparedness. In previewing the agency's preparedness for the approaching hurricane season Secretary Chertoff emphasized three points. First, that all storm responses are state and local issues initially. Second, the federal government is prepared to respond with a set of tools never before assembled. He noted that those tools included new communication equipment, more ready supplies in place, and even the ability to more rapidly register and track potentially displaced storm victims. Chertoff's third point was that individual preparedness was necessary prior to any storm. Chertoff also cited the enhanced ability of federal, tribal, state and local emergency response agencies to work to together. Over the past year there has been a significant effort by DHS and FEMA to strengthen communication, relations, and to clarify roles at all levels of emergency management.
Source: http://www.fema.gov/news/newsrelease.fema?id=36522

25. *May 23, NBC 5 (IL)* — **Officials: City prepared for emergency.** New details released on Wednesday, May 23, revealed just how well prepared Chicago might be for an emergency. In January, a federal report ranked Chicago low among cities for disaster preparedness, but the Chicago Office of Emergency Management and Communications said a staged evacuation of more than 3,000 people from four buildings last September went well. "The results of the exercise were positive," said Cortez Trotter, the city's chief emergency officer. "It was a good report." Trotter said Chicago was the first city to hold a massive emergency drill. Officials said there were plans for an even larger drill in the near future. Officials, though, came up with at least 14 recommendations, NBC5's Lauren Jiggetts reported. Among the areas that needed work was ensuring that emergency notification reaches intended recipients and increased training for building personnel as initial responders. Officials also said workers should keep "go packs" at their desk with items like a flashlight, toothbrush and walking shoes. Officials also said there should be straightforward directions for evacuees.
Source: http://www.nbc5.com/news/13377814/detail.html

26. *May 22, National Oceanic & Atmospheric Administration* — **NOAA predicts above normal 2007 Atlantic hurricane season.** Experts at the National Oceanic & Atmospheric Administration (NOAA) Climate Prediction Center are projecting a 75 percent chance that the Atlantic Hurricane Season will be above normal this year. "For the 2007 Atlantic hurricane season, NOAA scientists predict 13 to 17 named storms, with seven to 10 becoming hurricanes, of which three to five could become major hurricanes of Category 3 strength or higher," said retired Navy Vice Admiral Conrad C. Lautenbacher, undersecretary of commerce for oceans and atmosphere and NOAA administrator. An average Atlantic hurricane season brings 11 named storms, with six becoming hurricanes, including two major hurricanes. "With expectations for an active season, it is critically important that people who live in East and Gulf coastal areas as well as the Caribbean be prepared," said Bill Proenza, NOAA National Hurricane Center director. "Now is the time to update your hurricane plan, not when the storm

is bearing down on you." The Atlantic hurricane season runs from June 1 through November 30, with peak activity occurring August through October.
Source: http://www.noaanews.noaa.gov/stories2007/s2864.htm

[Return to top]

Information Technology and Telecommunications Sector

27. *May 24, InformationWeek* — **Philadelphia launches wi−fi access test zone.** Philadelphia, PA, has approved a 15−square−mile Wi−Fi test zone. About 5,000 paying customers are expected to sign up by July and 12,000 by the end of the year. Consumers in the 15−square−mile test area can sign up beginning Thursday, May 24. Free access will be offered to city residents and visitors in several designated access areas throughout the city.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=199701767

28. *May 24, CNET News* — **Flawed Symantec update cripples Chinese PCs.** A Symantec antivirus signature update mistakenly quarantined two critical system files in the Simplified Chinese version of Windows XP last week, crippling PCs throughout China. According to the Chinese Internet Security Response Team (CISRT), users of Norton Antivirus, Norton Internet Security 2007 and Norton 360 who installed an antivirus signature update released by Symantec on May 17 could not reboot their PCs. The update reportedly mistook two Windows system files−−"netapi32.dll" and "lsasrv.dll"−−as the Backdoor.Haxdoo Trojan horse. The two files were subsequently quarantined. CISRT said the flawed Symantec update only affects users of the Simplified Chinese version of Windows XP Service Pack 2 that have been patched with a particular Microsoft software fix available since November 2006. According to Symantec China's Website, affected customers can resolve the problem by initiating another LiveUpdate, if they have not restarted their PCs after installing the flawed update. Systems that have already been restarted can be returned to the previous state by recovering the two system files from the Windows XP disc.
Source: http://news.com.com/Flawed+Symantec+update+cripples+Chinese+PCs/2100−1002_3−6186271.html?tag=cd.lede

29. *May 23, US−CERT* — **Microsoft Office ActiveX control vulnerability.** US−CERT is aware of reports of a vulnerability in a Microsoft Office 2000 ActiveX control. Excessive data passed to the OUACTRL ActiveX control may result in a buffer overflow allowing arbitrary code execution or causing a denial−of−service condition. This vulnerability was fixed in the Microsoft UA Control Vulnerability update, which is included in Microsoft Office 2000 SP3: http://www.microsoft.com/downloads/details.aspx?familyid=1e9388cc−76fa−40cf−a84a−6284f5a15533&displaylang=en
Source: http://www.us−cert.gov/current/index.html#microsoft_office_activex_control_vulnerability

30. *April 30, Government Accountability Office* — **GAO−07−368: Information Security: FBI Needs to Address Weaknesses in Critical Network (Letter Report).** The Federal Bureau of Investigation (FBI) relies on a critical network to electronically communicate, capture, exchange, and access law enforcement and investigative information. Misuse or interruption of

this critical network, or disclosure of the information traversing it, would impair FBI’s ability to fulfill its missions. Effective information security controls are essential for ensuring that information technology resources and information are adequately protected from inadvertent or deliberate misuse, fraudulent use, disclosure, modification, or destruction. GAO was asked to assess information security controls for one of FBI’s critical networks. To assess controls, GAO conducted a vulnerability assessment of the internal network and evaluated the bureau’s information security program associated with the network operating environment. This report summarizes weaknesses in information security controls in one of FBI’s critical networks. GAO recommends several actions to fully implement an information security program. In a separate classified report, GAO makes recommendations to correct specific weaknesses. FBI agreed with many of the recommendations but disagreed with the characterization of risk to its information and noted that it has made significant strides in reducing risks. GAO believes that increased risk remains.
Highlights: http://www.gao.gov/highlights/d07368high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−368

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: 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

31. *May 23, Xinhua (China)* — **Threat to blow up Mumbai World Trade Center.** Security at India's financial capital Mumbai's World Trade Center was increased Wednesday, May 23, after the police got an anonymous letter threatening to blow up the high−rise twin towers on Thursday, Indo−Asian News Service (IANS) reported. "The letter threatened to blow up the twin towers on May 24. The letter, however, did not give any specific reason for blowing it up," IANS quoted deputy commissioner of police Brijesh Singh assaying. "Following the threat we have beefed up security in and around the twin towers and are also conducting a thorough search of the premises. We are keeping a close watch on people visiting the buildings. We are not taking any chances," Singh said.
Source: http://news.xinhuanet.com/english/2007−05/23/content_6142438 .htm

[Return to top]

General Sector

32. *May 24, Associated Press* — **ELF arsonist gets 13 years in prison.** Declaring that fires set at a police station, an SUV dealership, and a tree farm were acts of terrorism, a federal judge Wednesday, May 23, sentenced a member of a radical environmental group to 13 years in prison. Stanislas Meyerhoff, 29, has admitted to being a member of a Eugene cell of the Earth

Liberation Front (ELF) known as The Family, which was responsible for more than 20 arson fires from 1996 through 2001 in five Western states that caused $40 million in damage. U.S. District Judge Ann Aiken commended Meyerhoff for having the courage to "do the right thing" by giving authorities information about his fellow arsonists after his arrest. But Aiken said his efforts to save the Earth by setting fires were misguided and cowardly, and contributed to an unfair characterization of others working legally to protect the environment as radicals. In a statement before being sentenced, Meyerhoff denounced the ELF, saying its goals of promoting a public discussion about stopping practices that harm the Earth actually cut off debate and harmed people.
Source: http://www.charlotte.com/118/story/133129.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 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.