



Department of Homeland Security Daily Open Source Infrastructure Report for 22 June 2007

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports a missing computer backup tape containing personal information on Ohio state employees also holds the names and Social Security numbers of 225,000 taxpayers. (See item [9](#))
- United Airlines officials still don't know what caused their flight dispatch system to shut down Wednesday, June 20, grounding takeoffs all over the world; the dispatch system's backup also malfunctioned, raising questions about whether the computer meltdown could happen again. (See item [13](#))
- WBAY reports the owners of the Log Den restaurant in Egg Harbor, Wisconsin, shut down by bad water, continue to explore all possible means that could have contaminated their water, including deliberate tampering. (See item [23](#))

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. *June 20, Knight Ridder Tribune* — **Detectives taped, followed man accused in \$1.4 million theft from Duke Energy.** Private detectives secretly followed Bill Monahan last year, and even video-recorded him as he allegedly re-set gas well pumps in Weld County, CO, to bring in

more income. Monahan, who turned himself in to authorities Monday, June 18, is accused of tampering with gas wells so they would inaccurately show more gas output, which equaled more payments from Duke Energy. The gas company and Weld District Court affidavits accuse Monahan of stealing more than \$1.4 million. Duke energy is now known as DCP Midstream. The first court hearing for Monahan is July 9. Monahan shares ownership of about 40 gas wells with his father, Rex Monahan, court records show. Court records show Duke Energy officials and private detectives followed Bill Monahan on February 21, 22 and 23 of 2006, and watched him check several wells. In each of those cases, the wells were "manipulated to false measurement conditions," according to the affidavit. However, the detectives also said other wells were also manipulated at times Bill Monahan was not present.

Source: <http://powermarketers.net/content/inc.net/newsreader.asp?ppa=8knpp%5E%5BmtnorouZUfb%7DGL%7Dbfem%5Ev>

2. *June 20, Platts Energy Bulletin* — **FERC chief market enforcement officer says agency enforcement tools adequate.** The U.S. Federal Energy Regulatory Commission's (FERC) chief enforcement officer Wednesday, June 20, expressed confidence that the federal government can adequately police the expanding physical and financial energy markets. FERC Office of Enforcement Director Susan Court defended the commission's enforcement efforts as members of Congress and state officials have increasingly called on federal regulators to explain rising oil, natural gas and electricity prices. "FERC, without a doubt, has joined the ranks of federal enforcement agencies," Court said. "Its ability to enforce its rules and orders issued to carry out its responsibilities is as great as any agency in the federal government." Court addressed concerns that commission either does not have enough regulatory and investigative tools to monitor the vast gas and power markets, or is not using them to the extent it should, saying that FERC investigators have "adequate tools" to monitor markets and enforce laws barring manipulation. Coming off the market breakdown of the Western energy crisis in 2001–02 and the price spikes after Hurricanes Katrina, Congress strengthened FERC's authority in 2005 to aggressively pursue possible instances of market manipulation and penalize energy companies that ignore federal regulations or try to defraud customers.

Source: <http://www.platts.com/Natural%20Gas/News/6394862.xml?sub=Natural%20Gas&p=Natural%20Gas/News>

3. *June 20, Houston Chronicle* — **Group issues new refinery safety guidelines.** More than two years after 15 workers died in trailers as close as 121 feet from a Texas City refinery explosion, the U.S. oil industry's trade organization Wednesday, June 20, issued new guidelines recommending safe distances for such structures from processing units. The American Petroleum Institute's (API) new standard for siting portable buildings suggests three zones for placement of trailers that could be threatened by external vapor cloud explosions. The standard requires companies to conduct detailed blast safety analyses before placing any portable building closer than 1,930 feet to a process unit area. And it sets distance limits between buildings and process unit areas. "We're trying to give people tools so they can then look at their own individual circumstance," said Red Cavaney of API. The new API standard recommends against placement of light wood buildings closer than 330 feet to a process area. It also suggests a distance of 570 feet or more for all portable buildings from larger units that process up to a million cubic feet of hydrocarbons. API further recommends that no workers whose jobs aren't directly related to running a process unit be in a building closer than 330 feet.

Source: <http://www.chron.com/disp/story.mpl/business/energy/4905908.html>

4. *June 20, Computerworld* — **New reliability rules put a charge in IT spending by utilities.**

The era of voluntary reliability standards for electric utilities ended Monday, June 18, and power companies now face a set of federally mandated rules that can cost them up to \$1 million a day in fines if they turn the lights out on their customers. But the day of reckoning for one industry is an opportunity for another — namely, the IT industry. The new regulations are boosting IT spending by utilities, particularly for security technologies, according to analysts. Spending on cybersecurity tools is now the fastest-growing segment of the utility software market in North America, said Christine Richardson of IDC's Energy Insights unit.

Cybersecurity purchases are growing at an annual rate of 11.2 percent, compared with an overall growth rate of 7.1 percent, she said. The new reliability rules have triggered "a huge rush from companies to have products to make sure they are compliant," said Richardson, who predicted that cybersecurity spending by utilities will increase to nearly \$435 million by 2010. NERC spokesperson Susan Boucher said the increased IT spending being prompted by the regulations is less expensive than the possible alternative: another blackout that wreaks havoc on customers and the economy.

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025321>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

5. *June 21, Detroit News* — **Tanker fire slows traffic.** A fuel spill and tanker fire at a gas station early Thursday morning, June 21, affected traffic on M-59 and Airport Road in Waterford Township, MI. It was not clear whether the fire or spill happened first, police said. No injuries were reported. Eastbound traffic on M-59 was getting by through the center lane, police said. Westbound traffic was unaffected. Airport Road was closed south of M-59.

Source: <http://detnews.com/apps/pbcs.dll/article?AID=/20070621/UPDATE/706210451/1003/METRO>

6. *June 20, Bonita News (FL)* — **Man severely burned in propane explosion.** A propane fire behind a Bonita Springs, FL, restaurant Wednesday, June 20, severely burned one man. Daniel Velez of LB's Gas in Bonita Springs was refueling two propane tanks behind the Dixie Moon Cafe on the corner of Old 41 Road and Dean Street when, according to witnesses, the fueling hose began banging against the back of the restaurant, propelled by the fuel shooting out its end. Lora Reece, a waitress at the restaurant, said fellow employee Margarita Martinez saw the rear door fly open, revealing a back exterior wall engulfed in flames. Reece said the man had severe burns on his legs and arms, his eyebrows were singed off and his hands were bleeding. Old 41 Road and Dean Street were quickly closed near the restaurant.

Source: http://www.bonitanews.com/news/2007/jun/20/man_badly_burned_propane_explosion_behind_dixie_mo/

[[Return to top](#)]

Defense Industrial Base Sector

7. *June 21, Aviation Week* — **UAVs, other aircraft being misused.** Using unmanned aerial vehicles (UAVs) and pod-equipped combat jets to find improvised explosive devices (IEDs) is often a misuse of time and resources, said U.S. Air Force Gen. Ronald Keys, commander of Air Combat Command. Often, requests for airborne surveillance are based on the assumption that such aircraft help find IEDs and save ground forces from such attacks, he said. Certain military leaders feel they need the full-motion video feeds to locate the explosives. The truth, he said, is much different. Based on Air Force analysis, the number of IEDs found by UAVs, surveillance aircraft or combat jets outfitted with advanced targeting pods per 100,000 flight hours is very low, according to Keys. "It's a waste," Keys said Wednesday, June 20, during a morning keynote speech at the Transformation Warfare 07 conference and exhibit in Virginia Beach, VA. Unfortunately, the military is basing some of its decisions on anecdotes instead of real metrics, he said. Indeed, the only metric being used is whether the Air Force is meeting certain tasking orders, instead of making sure those assets and flights are effective and the best use of time and aircraft.

Source: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aerospacedaily&id=news/UAVS062107.xml&headline=UAVs.%20Other%20Aircraft%20Being%20Misused.%20ACC%20chief%20Says

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

Banking and Finance Sector

8. *June 22, FINextra* — **British don't trust banks.** Consumer confidence in the retail banking industry has "eroded significantly," with an overwhelming majority of UK customers — 71 percent — saying they do not trust their banks, according to research released by Unisys. Banking is now less trusted than the technology, health and education industries, says Unisys. The survey of 679 UK adults, which was conducted by The Ponemon Institute, reveals that poor customer treatment now surpasses security as a primary concern. Unisys says studies in previous years have found that security was the main factor affecting customers — a 2006 survey found that 47 percent of UK consumers would switch accounts to institutions offering stronger fraud detection and protection services. The attributes most cited for eroding trust were "disrespectful attitudes", poor privacy, weak IT — including Websites, poor corporate governance and a lack of investment in the local community. Online banks fared worse than High Street banks in the customer trust study, with the two worst-rated banks both being Internet-based. Elton Birden of Unisys says banks must look beyond firewalls and data breaches and understand that consumers consider everything when deciding where to place their trust.

Source: <http://finextra.com/fullstory.asp?id=17078>

9. *June 22, Associated Press* — **Ohio Governor: stolen tape had taxpayer info.** A missing computer backup tape containing personal information on state employees also holds the names and Social Security numbers of 225,000 taxpayers, Ohio Governor Ted Strickland (D) said. The tape, stolen last week from a state intern's car, was previously revealed to hold the names and Social Security numbers of all 64,000 state employees, as well as personal data for tens of thousands of others, including Ohio's 84,000 welfare recipients. The taxpayers' information was on the backup tape because they hadn't cashed state income tax refund checks. Strickland said

Wednesday, June 20, an expert's review could reveal the tape contained more sensitive data. The administration has maintained it does not believe the information has been accessed because it would require specific hardware, software and expertise. But data security experts said the unencrypted tape could be breached by someone with computer expertise, time and money.

Source: http://news.yahoo.com/s/ap/20070621/ap_on_hi_te/data_theft:_ylt=An0HIIdqZXJgCisMgRE5j1CMjtBAF

10. June 21, Sophos — Spammers use PDF files in latest pump-and-dump scam. Sophos has identified a German "pump-and-dump" stock spam campaign which uses an attached PDF file to hoodwink potential investors. In a new spam campaign, messages are being sent to German Internet users encouraging them to read an attached PDF file which urges them to invest in stock in a company called Talktech Media. The PDF file carries the bizarre name sexy_ganja_report.pdf. The pump-and-dump spam message comes complete with a PDF file encouraging recipients to purchase stock in Talktech Media. "Internet users without anti-spam protection are probably used to seeing messages in their inbox telling them to buy shares in companies they've never heard of, but usually the promotions are in the form of regular text or an embedded image," said Graham Cluley, senior technology consultant for Sophos. "In an attempt to get past anti-spam filters criminals are now using PDF file attachments to carry their slick enticements for people to invest."

Source: <http://www.sophos.com/pressoffice/news/articles/2007/06/german-pdf-spam.html>

11. June 20, Computerworld — UK sets the pace when it comes to cyber crime. Identity theft, phishing and Trojan attacks are on the rise, and virtual worlds are being targeted by scammers, said RSA. The UK is a popular target because it was the pioneer for fast online payments, and consumers are used to easy and instant payment transfers, said Uriel Maimon of RSA consumer solutions. New scams are also emerging in virtual worlds, such as Second Life, according to Maimon. End users tend to use the same password for their virtual world as they do for their online bank account, so attackers try to uncover this through phishing attacks. Phishing attacks are increasing because it is a "statistics game". Each attack is cheap to execute, sometimes as low as \$1 or \$2, and each attack can live for around 100 hours. "It's a funnel effect. In a phishing attack you can send out more than 500,000 emails. Of those, maybe only 300,000 are real e-mail addresses, and then another 100,000 get past the anti-spam software, and maybe about 1,000 users click through the link, and perhaps the attack leads to only 50 compromised identities trickling through, garnering hundreds of dollars on average per identity," he said.

Source: <http://www.techworld.com/security/news/index.cfm?newsid=9217>

12. June 20, Computer Weekly — Phishing sites on the rise. More than 100,000 new phishing sites were created last week alone, according to IBM's X-Force content research team. The company identified, studied and classified more than 114,000 brand new phishing sites between June 11 and 18. According to the findings, 99.8 percent of all these sites came from automated phishing kits. Only 0.2 percent of the sites identified did not appear to follow an automated deployment strategy for their phishing attack. Gunter Ollmann director of security strategy for IBM ISS said there has been a colossal increase in the number of phishing sites with organized crime behind them. She added that there have been a high number of attacks on business bankers involving several U.S. banks since mid-May. "The FBI and the US Department of Justice are investigating and say this is the biggest attack they've seen. A very small proportion

of our InterAct Treasury Management Services customers have been the victims of this spate of e-mail fraud.”

Source: <http://www.computerweekly.com/Articles/Article.aspx?liArticleID=224917&PrinterFriendly=true>

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

Transportation and Border Security Sector

13. June 21, *Chicago Sun–Times* — Dispatch system grounded United flights. Officials at United Airlines say they still don't know what caused its flight dispatch system to shut down Wednesday morning, June 20, grounding takeoffs all over the world for two hours and delaying flights for the rest of the day. The dispatch system's backup also malfunctioned, raising questions about whether Wednesday's computer meltdown could happen again. The dispatch system that backfired performs critical functions such as determining the weight of an aircraft, relaying flight plans to pilots, and confirming that maintenance checks have been completed. United has an electronic backup system that's supposed to kick in if the flight dispatch system fails, but it also was disabled by the outage, United spokesperson Robin Urbanski said. That concerns aviation experts such as Diego Klabjan, an airline consultant and associate professor of civil and environmental engineering at the University of Illinois at Urbana–Champaign. "How can both of them fail at the same time?" Klabjan said. ". . . They should definitely have . . . an option where you can make flight plans by hand."

Source: <http://www.suntimes.com/news/metro/437534.CST–NWS–delay21.article>

14. June 21, *United Press International* — Chicago police soon to monitor bus cams. New technology will soon allow Chicago police officers to view live video from city buses in their patrol cars. Chicago Transit Authority spokesperson John Flynn said the agency is outfitting buses with radio equipment that transmits short distances so video signals can be picked up by Wi-Fi hot spots and nearby police cars. Flynn said eventually city emergency dispatchers will also have the ability to monitor the transit cams as well. Chicago has made a bid to host the 2016 Summer Olympic Games and Flynn said the new technology will enhance public safety and make the city's bid more attractive.

Source: http://www.upi.com/NewsTrack/Quirks/2007/06/21/chicago_police_soon_to_monitor_bus_cams/3249/

15. June 21, *Associated Press* — Continental apologizes for sewage on transatlantic flight. Passengers who endured a two-day transatlantic odyssey with sewage overflowing from a jet's lavatories are getting an apology from Continental Airlines for the "poor conditions." Flight 71, with 168 passengers onboard, took off June 13 from Amsterdam bound for Newark, NJ, but only got as far as Shannon, Ireland, because of a problem with the lavatory. The flight resumed the next day after repair work seemed to restore smooth flow in the lavatory system, a Continental spokesperson said Thursday, June 21. But during the flight from Shannon to Newark, renamed Flight 1970, "the problem developed again," spokesperson Dave Messing said. When the plane landed in Newark, he said, it was determined that the blockage was caused by someone flushing latex gloves down the toilet.

Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20070621/NEW_S07/70621031

16. *June 20, Bloomberg* — Plane crashes force Indonesia to boost safety as airlines boom.

Recent crashes have triggered alarms in Indonesia, where domestic passenger traffic has quadrupled in seven years with the growth of budget carriers. The rate of fatal crashes in the nation is 15 times greater than the world average, according to Ascend, a London-based aviation adviser. President Susilo Bambang Yudhoyono replaced the transportation minister and ordered the new minister to impose tougher standards within two years. “Our safety measures aren't enough to cope with demand growth,” said Bambang Susantono, chairman of the Indonesian Transport Society, an independent group of transportation experts. “There's a shortage of radar stations, some airports have poor runway conditions, we don't have enough airworthiness inspectors.” Indonesia had 3.77 fatal accidents for every one million takeoffs in the three years ended March 31, according to Ascend. The global rate was 0.25. The U.S. and Australia have warned their citizens against using local airlines, citing poor safety ratings. A government report issued March 22 said none of Indonesia's 20 airlines fully complied with international safety standards. The 20 criteria included maintenance, training, management and safety records.

Source: <http://www.bloomberg.com/apps/news?pid=20601080&sid=a5ETMSBvppCY&refer=asia>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

17. *June 21, Oklahoman* — Livestock emergency vehicles readied. Six mobile units to help contain contagious animal diseases are ready for use in the event of a serious outbreak, Oklahoma officials said Wednesday, June 20. The units will clean and disinfect livestock transport vehicles and other equipment contaminated during a naturally occurring or man-made animal disaster, said Jack Carson, state Agriculture, Food and Forestry Department spokesperson. It's believed Oklahoma is the first to build specific response units dedicated exclusively to an agricultural emergency, he said. The units, for example, could be used in areas where livestock is quarantined, Carson said. Law officers, veterinarians and others going inside the quarantined area will have to be disinfected by the units, which will be set up in buffer zones, he said. Each unit costs \$80,000, which includes the pressure washing system, disinfectant/chemicals, generator and other necessary equipment, in addition to the trailer that hauls all the equipment. All six were built and assembled in Oklahoma.

Source: <http://newsok.com/article/3068800>

18. *June 21, Agricultural Research Service* — Foreign herbivores may be key to curbing invasive weeds. Joint research with scientists in Argentina, Australia and China could lead to discovery of new biological control agents for several exotic weeds plaguing Florida and other U.S. states. Some of the worst offenders are hydrilla, Brazilian pepper, Chinese tallow and Australian pine. These and other aggressive invasive weeds occupy diverse habitats and cause

many environmental problems, especially a decrease in biodiversity within infested areas. Entomologist Greg Wheeler and colleagues at the Agricultural Research Service (ARS) Invasive Plant Research Laboratory in Fort Lauderdale, FL, have been focusing on this growing problem in the U.S. The Fort Lauderdale scientists have been collaborating with counterparts at the ARS South American Biological Control Laboratory in Hurlingham, Argentina, and the ARS Australian Biological Control Laboratory in Indooroopilly, Australia, as well as with China's Academy of Science. Together, the researchers are conducting extensive field surveys to discover herbivorous insects and mites that feed on the invasive weeds in their native ranges. The researchers have recovered many promising new candidate biological control agents, including weevil, thrip, psyllid, moth and mite species. Several are undergoing — or have completed — preliminary testing to determine their safety for U.S. release.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

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

Food Sector

19. June 20, Agence France–Presse — China to overhaul food safety rules. China promised Wednesday, June 20, to overhaul its food safety rules, amid rising concerns abroad over the risks of consuming its produce. "The top priority for building a food safety standards system is to revise as soon as possible the rules for farm produce and processed food," said the director of the General Administration of Quality Supervision, Inspection and Quarantine, Liu Pingjun. Liu said that at the end of 2006, some of China's 1,965 national food safety standards, of which 634 are mandatory, dated back 12 years. He pledged to ensure none of the rules were more than four and a half years old and complied with international standards, although the statement did not specify how that would be accomplished.

Source: http://news.yahoo.com/s/afp/20070620/hl_afp/chinafoodsafetytrade_070620180836;_ylt=AiMb1AiR3jK9S8bj_q848WJOrgF

20. June 20, Greenville News (SC) — Poultry workers test positive for TB. South Carolina health officials tested 286 employees at a Greenville poultry–processing plant for tuberculosis after a case of tuberculosis (TB) was reported there, and nearly half had a positive skin test. The investigation at Columbia Farms after tests on the first individual confirmed active TB, said Thom Berry, spokesperson for the state Department of Health and Environmental Control. The positive skin tests on 131 of the workers means they were exposed to TB sometime in their lives, not that they have active disease, he said. Of those workers, 63 had chest X–rays, revealing two possible cases of active disease, though officials are still awaiting confirmatory tests, he said. Berry said investigators were not surprised by the number of positive skin tests because so many of the employees are foreign–born. People born in other countries are nearly nine times more likely to have TB than those born in the U.S., according to the U.S. Centers for Disease Control and Prevention.

Source: <http://greenvilleonline.com/apps/pbcs.dll/article?AID=/20070620/NEWS01/706200388/1004/NEWS01>

21. June 19, U.S. Food and Drug Administration — Diced yellow onions recalled. Gills Onions, LLC is recalling diced yellow onions. The recall comes after the Washington State Department of Agriculture, during routine testing, detected *Listeria monocytogenes* in one retail bag of

diced yellow onions. Gills Onions is working with both State and Federal officials to determine the cause. At this time there have been no reported illnesses associated with this product. *Listeria monocytogenes*, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Although healthy individuals may suffer only short-term symptoms such as high fever, severe headache, stiffness, nausea, abdominal pain and diarrhea. *Listeria* infection can cause miscarriages and stillbirths among pregnant women. As a precautionary measure, both retail and food service diced packs are being recalled. The retail product was labeled with the Trader Joe's brand name and was distributed to stores in Arizona, California, Nevada, New Mexico, Oregon and Washington. The foodservice packages were labeled under the Gills Onions Brand and the Sysco Natural Brand.

Source: http://www.fda.gov/oc/po/firmrecalls/gills06_07.html

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

Water Sector

22. *June 21, Chicago Tribune* — Two workers killed at water reclamation plant. Two men died Wednesday, June 20, after collapsing in an underground vault at a water treatment plant in Stickney, IL, authorities said. After one man collapsed in the vault, which is 10 feet below street level, the other man went in to help him. Both apparently succumbed to fumes or a lack of oxygen, said Stickney Fire Chief Larry Meyer. Both men worked for a subcontractor of Metropolitan Biosolids Management LLC, of Evanston, IL, which is building a facility inside the treatment plant to dry sewage material into pellets for soil fertilization. One of the workers was in the vault inspecting a new water main for leaks.

Source: http://www.chicagotribune.com/news/local/chi-twodead_21jun21_1.347303.story?track=rss

23. *June 20, WBAY (WI)* — Sheriff's department investigates restaurant water contamination. The owners of a Door County, WI, restaurant shut down by bad water continue to explore all possible means that could have contaminated their water, including deliberate tampering. The Door County Sheriff's Department is also now involved in the search. The Log Den in Egg Harbor reopened the weekend of June 16 after spending more than a week closed. The owners of the restaurant shut the doors after more than 200 people became sick. Water tests confirmed the presence of norovirus in a well just outside the restaurant. The virus causes vomiting, diarrhea, and fatigue. The health department has already said the restaurant's septic system is not the problem. Next week it'll begin inspecting other septic systems in nearby.

Source: <http://www.wbay.com/Global/story.asp?S=6689075>

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

Public Health Sector

24. *June 21, Associated Press* — Vietnamese woman dies of bird flu. A 28-year-old woman died of bird flu Thursday, June 21, in the Vietnamese capital, becoming the second person to die from the virus in Vietnam in two weeks, officials said. Phan Thi Xuyen died at the Hanoi

Hospital of Tropical Diseases, 13 days after she was admitted with symptoms of the H5N1 bird flu virus, said Nguyen Hong Ha, deputy hospital director. Xuyen became ill in her home province of Ha Nam after she came into contact with sick poultry. Tests conducted by a Vietnamese laboratory confirmed she had been infected with the H5N1 virus. Vietnam had reported no bird flu deaths from November 2005 until June 10, when a man from Ha Tay province died at a Hanoi hospital.

Source: <http://www.iht.com/articles/ap/2007/06/21/asia/AS-GEN-Vietnam-Bird-Flu.php>

25. June 21, RIA Novosti (Russia) — First H5N1 case confirmed at Czech poultry farm. The state veterinary authority confirmed that turkeys on a farm to the east of the Czech capital had died from the lethal H5N1 strain of the bird flu virus, the Czech news agency CTK said Thursday, June 21. The agency said all the birds at the farm will be slaughtered and that veterinary services are conducting checks at neighboring farms. It is the first time the virus has been detected among domestic poultry in the country. The first bird flu case was reported in the Czech Republic in the spring of 2006, with 13 registered incidents since then.

Source: <http://en.rian.ru/world/20070621/67610784.html>

26. June 20, Reuters — Fever in travelers often a sign of serious problem. Fever in travelers returning home is a marker of potentially grave illness, according to researchers who report the findings from global surveillance of travel-related illnesses. "Predominant causes of fever in returned travelers vary by destination," lead investigator Mary E. Wilson told Reuters Health. "Febrile illnesses in returned travelers are often serious. Malaria, especially falciparum, remains the most important infection to identify." Wilson, of Harvard Medical School, and colleagues studied data gathered at 31 clinics on six continents that specialize in travel or tropical medicine, to get a picture of what illnesses afflict travelers. Of nearly 25,000 travelers seen at the clinics over a 10-year period, 28 percent cited fever as their chief reason for seeking care. Overall, 26 percent of patients with fever were hospitalized, compared with only three percent of patients who did not have fever. Malaria, diagnosed in 21 percent of those with fever, was the most common culprit. Other causes of fever, among them dengue, rickettsia and hepatitis, varied by region visited.

Source: <http://uk.reuters.com/article/healthNews/idUKCOL07079420070620>

[[Return to top](#)]

Government Sector

27. June 21, Government Accountability Office — GAO-07-1023T: Social Security Numbers: Use is Widespread and Protection Could Be Improved (Testimony). Since its creation, the Social Security number (SSN) has evolved beyond its intended purpose to become the identifier of choice for public and private sector entities, and it is now used for myriad non-Social Security purposes. This is significant because a person's SSN, along with name and date of birth, are the key pieces of personal information used to perpetrate identity theft. Consequently, the potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs. Accordingly, this testimony focuses on describing the (1) use of SSNs by government agencies, (2) use of SSNs by the private sector, and (3) vulnerabilities that remain to protecting SSNs. For this testimony, the Government Accountability Office (GAO) primarily relied on information from GAO's prior reports and

testimonies that address public and private sector use and protection of SSNs. These products were issued between 2002 and 2006 and are listed in the Related GAO Products section at the end of this statement.

Highlights: <http://www.gao.gov/highlights/d071023thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1023T>

- 28. *June 15, Government Accountability Office* — GAO-07-752: Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain. (Report).** Federal agencies have taken actions to mitigate the availability of SSNs in public records by implementing the use of truncation for documents provided to state and local record keepers. While these actions provide some additional protection against using these records to perpetrate identity theft, the Government Accountability Office's (GAO) review demonstrates that identity thieves may still be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources. Thus, truncation does not provide complete protection against identity theft. Yet despite this limitation, GAO's analysis suggests that truncation provides better protection compared with records that display full SSNs. In this regard, as GAO noted in its May 2006 report, Congress may wish to further improve SSN protection by enacting truncation standards or assigning an agency to do so. In addition, Congress may wish to solicit input on promising truncation practices from the Commissioner of Social Security as part of this process. However, in the absence of such standards, federal agencies can still take steps to protect SSNs by further reducing their exposure in records they generate and provide to record keepers.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-752>

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

Emergency Services Sector

- 29. *June 21, North County Times (CA)* — Preparedness critical in massive fires.** As the population in Riverside County, CA, continues to boom, more and more homes encroach on what had been just open land — areas such as the Cleveland National Forest. That can mean disaster should an out-of-control wildland fire spread to places where people live. With that in mind, nearly 600 firefighters and law enforcement officers gathered Wednesday, June 20, in Lake Elsinore, Lakeland Village, and the El Cariso Village community along the Ortega Highway to participate in a multiagency training drill to help be better prepared for the day a large fire threatens those areas, which border the national forest. Wednesday's drill — using no real flames and making no actual evacuations — addressed how a multitude of agencies would work together when responding to a huge fire. The training drill was scripted throughout, with fire crews being dispatched to various locations to protect structures or sites where they'd be placed should there have been an actual blaze. There were mock reports of fires jumping across roads, heading toward homes. All agencies involved in the drill deemed Wednesday's training a success.

Source: http://www.nctimes.com/articles/2007/06/21/news/californian/4_02_446_20_07.txt

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

Information Technology and Telecommunications Sector

30. *June 21, eWeek* — **Apple shuts down IPv6 security hole.** Apple has slammed the door shut on denial-of-service (DoS) attacks and a security bypass that Type 0 routing headers in IPv6 let in. The company on Wednesday, June 20, put out an update, Mac OS X 10.4.10, that addresses the problem by disabling support for the headers. This vulnerability has been left wide open in IPv6 even though it was well-known and shut down in IPv4; by default, all routing engines now turn it off. This particular type of packet header can be used to crazily bounce network packets back and forth between hops on their route, clogging up bandwidth and potentially causing a DoS. Apple said in its security advisory that the issue doesn't affect systems prior to Mac OS X 10.4. The update is available for Mac OS X 10.4 through Mac OS X 10.4.9 and Mac OS X Server 10.4 through Mac OS X Server 10.4.9. It can be obtained from Mac OS X's Software Update pane under System Preferences or via Apple's Software Downloads site. Apple's Software Downloads site: <http://www.apple.com/support/downloads/>
Source: <http://www.eweek.com/article2/0,1895,2148908,00.asp>
31. *June 21, VNUNet* — **China publishes spammers blacklist.** Internet authorities in China have published a blacklist of more than 100,000 Web addresses which have been used to send spam. The online list is intended to help service providers and e-mail recipients filter out spam. China has been ranked as one of the world's most prolific sources of unsolicited commercial e-mail by various sources, including online security firms. The latest official action appears to have been prompted by complaints from inside China, particularly from users troubled by email-borne viruses.
Source: <http://www.vnunet.com/vnunet/news/2192526/china-rejects-spam-diet>
32. *June 20, IDG News Service* — **McAfee: Infrastructure, digital home attacks coming.** Online criminals looking for new areas to attack in the next few years will find green fields in the Internet infrastructure and the digital home, researchers with McAfee's Anti-Virus Emergency Response Team (AVERT) labs said Tuesday, June 19. McAfee offered its take on the top security trends for 2007, at a press event in San Francisco, saying that well-known problems such as phishing, spam, bots, and rootkits are on the rise. But in the years ahead, new areas will be top concerns, said Craig Schmugar, virus research manager at McAfee's AVERT labs. "In the short term, it will be the infrastructure side of things," he said. "In the long term, it will be digital entertainment." Schmugar said that the recent flaw in Windows DNS servers, which was exploited in a small number of online attacks, is a good example of things to come. These servers are a critical part of the Internet's infrastructure, used to convert the domain names users type into their browsers into the IP addresses that identify computers on the Internet. McAfee also expects to see hackers focus more on Wi-Fi attacks as PC users become accustomed to connecting to wireless networks wherever they go.
Source: http://news.yahoo.com/s/infoworld/20070620/tc_infoworld/89510:_ylt=Al9vDkVOQVjAhtiXSm6BAKYjtBAF
33. *June 20, VNUNet* — **USB Flash drive worm spreads AIDS info.** Security experts have disclosed details of a worm that copies itself onto removable drives, such as USB Flash drives, in an attempt to spread information about AIDS and HIV. The LiarVB-A worm hunts for removable drives such as floppy disks and USB memory sticks, as well as spreading via network shares. It creates a hidden file called 'autorun.inf' to ensure that a copy of the worm is

run the next time the drive is connected to a Windows PC. "Much of the malware we see is designed to generate income for the hackers, but this worm is different in that it spreads information about AIDS instead," said Graham Cluley, senior technology consultant at Sophos. Source: <http://www.vnunet.com/vnunet/news/2192450/usb-flash-drive-worm-spreads>

34. *June 20, PC Pro (UK)* — **Hacking of Internet-delivered broadcast reveals security**

vulnerability. A Czech Webcam was streaming lovely pastoral pictures of a local beauty spot, until hackers gained access and inserted pictures of the area being "nuked." Unfortunately, the video was also then broadcast live on television. The incident occurred on Sunday morning, June 17, on Czech TV program Panorama. Hackers interrupted the regular Webcam transmission with video "footage" of a nuclear explosion. The stunt was pulled by a group of "artists" known as Ztohoven. Their Website promptly went offline as massive numbers of users investigated the pranksters. Security experts warned that this type of hacking demonstrates the security vulnerabilities involved when transmitting information across the Internet.

"Internet-delivered broadcasts and Internet TV transmissions are still in their infancy, but this doesn't stop hackers from attacking weak points in the transmission infrastructure," says Geoff Sweeney, chief technology officer of behavioral analysis software company Tier-3.

Source: <http://www.pcpro.co.uk/news/116024/hackers-nuke-czech-beauty-spot.html>

Internet Alert Dashboard

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