



Department of Homeland Security Daily Open Source Infrastructure Report for 14 June 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](#)
<http://www.dhs.gov/>

Daily Highlights

- The Department of Homeland Security has released a Fact Sheet: Securing Our Nation's Chemical Facilities, stating that chemical security is not solely a federal responsibility; it is a shared responsibility among federal, state, and local governments, and also with the private sector. (See item [8](#))
- The Associated Press reports the head of the FBI's Boston office is warning the region's top universities to be on the lookout for foreign spies or potential terrorists who might be trying to steal unclassified, yet sensitive, research. (See item [27](#))
- The St. Louis Post–Dispatch reports explosives, including dynamite and C–4, capable of causing extensive damage have been stolen from a St. Charles County, Missouri, firing range used by the sheriff's office and the FBI. (See item [35](#))

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 13, WTOL 11 (OH)* — **FBI investigates possible threat against Davis–Besse.** The FBI is investigating a possible threat against the Davis–Besse Nuclear Power Station near Oak Harbor, OH. Ottawa County Sheriff Bob Bratton says he called the bureau to report the threat on

Monday, June 11. Bratton says a waitress in a Port Clinton restaurant overheard two men talking about the nuclear power plant on Sunday. She told police one of the men wrote "boom" on a napkin. Bratton says the waitress told police the men were "Arab-looking." Patrols have been increased at the plant, but a spokesperson for First Energy, the owner of the plant, says local authorities don't think the threat is credible. The FBI continues to investigate.

Source: <http://www.wtol.com/Global/story.asp?S=6646196>

- 2. *June 13, Techworld* — Google and Intel set up energy-saving alliance.** In an initiative to improve computer power use — equivalent to shutting down twenty 500 megawatt coal-fired power plants — Google and Intel have set up the Climate Savers Computing Initiative (CSCI). The forty starting members, including AMD, Dell, HP, IBM and Sun, hope to better manage power-delivery and power management of computers to achieve this by 2010. Suppliers, businesses and individuals are being asked to join and help save \$5.5 billion in energy costs. Servers and PCs waste lots of power from the moment it enters their power cables. Google's Urs Holzle said: "The average desktop PC wastes nearly half of its power, and the average server wastes one-third of its power. The CSCI is setting a new 90 percent efficiency target for power supplies." Combining low-power screen technology with the CSCI power delivery and management work it is likely that computers will be significantly more power-efficient by 2010 and thereafter. The initiative's energy efficiency benchmarks will initially follow the EPA's Energy Star guidelines, but with increasing requirements during the next several years.

Source: <http://www.techworld.com/green-it/news/index.cfm?newsID=9135 &pagtype=all>

- 3. *June 13, Reuters* — BP reduces oil reserves estimate.** BP PLC has lowered its estimate of the world's proven oil reserves, for the first time in more than a decade, in its annual Statistical Review of World Energy published on Tuesday, June 12. This year's review, which covers the period to the end of 2006, included an assessment of the size of Canadian oilsands for the first time. They stand at 163.5 billion barrels. Global reserves are more than sufficient to meet current production levels for more than 40 years, although accessing the oil is getting tougher due to high exploration and production costs and also to more state control of production, BP said. World reserves stood at 1.208 trillion barrels at the end of 2006, fractionally lower than 1.209 trillion at the end of 2005. The one billion-barrel reduction reflected declines in reserves in Mexico and Norway, partly offset by increases in Russia and Brazil. Christof Ruhl, deputy chief economist at BP, said the last time the annual reserves figure had fallen in the statistical review was in 1990. BP's review is widely used as a reference throughout the global energy industry.

Source: <http://www.canada.com/calgaryherald/news/calgarybusiness/story.html?id=44b258e4-ae52-461f-83ae-676debac32fc>

- 4. *June 12, Thomson Financial* — Baltic states face energy deficit after nuke plant closing.** The Baltic countries face a massive energy deficit after the Ignalina nuclear power station is shut down in 2009, Latvian Prime Minister Aigars Kalvitis warned Tuesday, June 12, at a regional energy conference. Lithuania promised the European Union, which together with Latvia and Estonia joined the bloc in 2004, to shut down the Ignalina nuclear power plant, which operates Chernobyl-style reactors, by 2009. A replacement facility that the three plan to build, possibly with the involvement of Poland, would not come onstream before 2015. That would leave a gap of six years between the closure of Ignalina and the inauguration of the new plant, which might not be fully operational until several years after 2015. During that time, the

Baltic states will have to seek energy sources elsewhere. The three want to build a new nuclear power station to replace Ignalina, and are also developing energy links with their EU neighbors, to try to end their heavy energy reliance on Russia. All three countries were Soviet republics and still rely heavily on Russia for supplies of natural gas and oil. Their power grids are also still linked to that of their former ruler.

Source: <http://www.forbes.com/markets/feeds/afx/2007/06/12/afx3812008.html>

5. *June 12, Associated Press* — **INL: Public not at risk as nuclear lab responds to incident.**

Emergency crews at the Idaho National Laboratory (INL) on Tuesday, June 12, responded to what officials are describing as a "facility incident" inside the site's Reactor Technology Complex, but said no radiation was released and the public was not at risk. John Epperson, a spokesperson for the INL's joint information center in Idaho Falls said the Advanced Test Reactor, the 40-year-old centerpiece of this 890-square-mile federal nuclear reserve in southern Idaho, was not affected. He said state, county and tribal officials on the Fort Hall Indian Reservation to the south were notified of the incident.

Source: http://seattlepi.nwsource.com/local/6420AP_ID_INL_Incident.html

6. *June 11, Utility Automation & Engineering* — **Report finds rising utility investment in automation/IT.** InfoNetrix just released a new market research report depicting planned and existing investments in automation and information technology projects by North American electric utilities. The report is based on surveys conducted with utilities across the United States and Canada between March 2006 and December 2006. The findings underscore a rising level of utility investments in automation/IT since passage of the 2005 Energy Policy Act. "After more than two decades of deferring investments in T&D, rising concerns about declining grid infrastructure and an aging workforce coupled with reliability and security concerns, utilities now seem ready to step up investments in automation/IT," said Michael A. Marullo of InfoNetrix. "Utilities are increasingly realizing that investing in automation/IT is a good way to extend the useful life of critical assets," Marullo added. The Northeast Blackout of August 2004 and other grid incidents have also contributed to the current rise in spending for automation/IT projects as a hedge against reliability concerns.

Source: http://uaelp.pennnet.com/display_article/295027/22/ARTCL/non e/none/Report-finds-rising-utility-investment-in-automation/IT/

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

Chemical Industry and Hazardous Materials Sector

7. *June 13, Baltimore Sun* — **Hospital evacuates about 200 after rupture of natural gas line.**

About 200 people were evacuated from Anne Arundel Medical Center in Maryland Tuesday, June 12, after a contractor ruptured a natural gas line. Staff members, patients and visitors at the Wayson, Donner and Edwards pavilions at the Annapolis-area hospital were sent outside or to other buildings on the campus shortly before noon EDT. The three pavilions house medical offices, therapy rooms and outpatient surgery areas, but no surgeries were under way at the time and others were delayed. Anne Arundel County firefighters shut down the ramp to the hospital from westbound U.S. 50 while the Baltimore Gas and Electric Co. repaired the break in the gas line.

Source: <http://www.baltimoresun.com/news/local/bal-md.briefs13jun13>

[0.3515977.story?coll=bal-local-headlines](http://www.0.3515977.story?coll=bal-local-headlines)

8. *June 12, Department of Homeland Security* — **Fact Sheet: Securing Our Nation's Chemical Facilities.** Chemical security is not solely a federal responsibility; it is a shared responsibility among federal, state and local governments, and also with the private sector. Government and industry have to work together to implement the best possible measures to strengthen the security of America's chemical facilities, while not undercutting an important part of the nation's economy. Some of DHS' goals to strengthen chemical facility security are as follows:
- a) Apply a risk-based approach to protecting the chemical sector;
 - b) Ensure high-risk facilities are protected and that owners and operators across the sector are doing their part;
 - c) Secure not only chemical sites and facilities, but also chemicals in transit;
 - d) Target the highest risk chemicals and work with industry to demonstrably reduce risk without breaking the system;
 - e) Share knowledge, information, and intelligence about threats and vulnerabilities across the sector;
 - f) Develop a common understanding of risk, define roles and responsibilities, and establish clear metrics to measure progress against national priorities;
 - g) Ensure accountability so that the hard work done to protect this sector is not undermined by a small number of facilities not acting responsibly.

Source: http://www.dhs.gov/xnews/releases/pr_1181745031563.shtm

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

9. *June 13, Sydney Morning Herald (Australia)* — **Virus blight spreads to museum Website.** The Website of Sydney, Australia's Museum of Contemporary Art has been found to "host or distribute" malicious software, a day after reports surfaced of similar security breaches at the Website of the Sydney Opera House. Visiting the site "may harm your computer", Google warns users who try to click through to the Website, mca.com.au, from its search engine. Up until this month the warning was also displayed under links to the Sydney Opera House Website, which has since been repaired to remove Trojan software designed to capture sensitive information, such as Internet banking details, from victims' computers. The type of malware hosted on the site was not clear. Andrew Antal of MessageLabs security was certain the malicious code was the type designed to steal information. "Whether it's a trojan or a piece of malware the intent is still the same -- which is to actually steal information off people either in stealth or to take over their machine," he said. StopBadware.org lists almost 100 other infected Australian Websites. These can be found by searching the "Clearinghouse" on the StopBadware.org Website for items containing ".com.au".

Source: <http://www.smh.com.au/news/security/virus-blight-spreads-to-museum-site/2007/06/13/1181414340831.html>

10.

June 12, InformationWeek — **California man gets six-year sentence for phishing.** A

California man who was found guilty in January of operating a sophisticated phishing scheme that attempted to dupe thousands of AOL users received a prison sentence Monday of 70 months — a fraction of the 101 years he could have been given. In the first jury conviction under the Can-Spam Act of 2003, Jeffrey Brett Goodin was convicted of sending thousands of e-mails set up to appear to be from AOL's billing department to the company's users, prompting them to reply with personal and credit-card information. He then used the information to make unauthorized purchases, according to the U.S. Attorney's Office in Los Angeles. Assistant U.S. Attorney Rozella Oliver, who represented the government in the sentencing, said she had pushed for a minimum of 94 months, but the judge factored in mitigating circumstances, such as Goodin's lack of a criminal history. Goodin also was found guilty of 10 other counts, including wire fraud, aiding and abetting the unauthorized use of an access device (a credit card in this case), and possession of more than 15 unauthorized access devices.

Source: <http://www.informationweek.com/news/showArticle.jhtml?articleID=199903450>

11. *June 12, USA TODAY* — **Data theft arrests show how tens of millions are at risk.** Last fall, 19-year-old Irving Escobar crisscrossed northern and central Florida using counterfeit credit cards to buy stacks of \$400 gift cards from Wal-Mart stores, cashing them in to buy TVs, PCs and jewelry from Wal-Mart subsidiary Sam's Clubs in south Florida. With credit cards supplied by an unnamed recruiter, they bought gift cards in \$400 increments — just below the \$500 limit that requires a manager's approval. At one store, they hauled out 60 \$400 gift cards. Escobar returned some merchandise for cash refunds, and he probably sold some of the gift cards, according to Florida law-enforcement officials. "It was modern-day money laundering," says Amy Osteryoung, an assistant statewide prosecutor. But this scam was part of a sophisticated operation that started with the theft of credit card data on 45.7 million customers of TJX. Investigators believe it is the boldest tangible evidence of criminals cashing in on hacked data from TJX. What's more, the Florida scam took advantage of burgeoning markets for counterfeit credit cards and authentic gift cards — and it could be easily repeated anywhere. "Who's to say this scam wasn't happening in other states, with other retailers?" says Brian Riley, senior bank card analyst at TowerGroup.

Source: http://www.wzzm13.com/news/news_article.aspx?storyid=76403

12. *June 12, Computerworld* — **Personal data on 17,000 Pfizer employees exposed; P2P app blamed.** A Pfizer Inc. employee who installed unauthorized file-sharing software on a company laptop provided for use at her home has exposed the Social Security numbers and other personal data belonging to about 17,000 current and former employees at the drug maker. Of that group, about 15,700 individuals actually had their data accessed and copied by an unknown number of persons on a peer-to-peer network, the company said in letters sent to affected employees. The incident has prompted an investigation by Connecticut Attorney General Richard Blumenthal; some 305 Pfizer employees in that state were affected by the breach. News of the Pfizer breach coincides with the release of a study by Dartmouth University's Tuck School of Business that looked into the dangers posed by file-sharing applications. The study examined data involving P2P searches and files related to the top 30 U.S. banks over a seven-week period between December 2006 and February 2007. A surprisingly high number of people sharing music and other files on peer-to-peer systems are inadvertently exposing all sorts of bank account data and similar personal information on their

computers to criminals lurking on the networks to harvest data, according to the report.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024491&intsrc=hm_list

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

Transportation and Border Security Sector

13. *June 13, KGTV (CA)* — Security breach briefly shuts down California airfield. Lindbergh Field's Terminal Two was shut down briefly after a small security breach took place, according to airport officials. Around 10 p.m. PDT on Tuesday, June 12, San Diego Harbor Police said they noticed an alarm at a checkpoint may not have been working properly. As a precaution, passengers were taken off their planes and re-screened through security. Many departing flights were delayed and those aboard planes that had just arrived were kept on the tarmac for several hours.

Source: <http://www.10news.com/news/13494177/detail.html>

14. *June 13, WTVF (TN)* — Nashville airport's pilot program to cut security wait time. A new technology will change the way those with casts or prosthetic limbs go through security lines. The Nashville International Airport has been chosen for a pilot program. The airport is scheduled to get a new portable X-ray machine called the Cast Scope. The X-ray machine screens passengers with casts, braces or prosthetic limbs. It can detect weapons or explosives in only a few seconds. The Cast Scope is expected to cut down on security screening time because it's a portable machine. Nashville International is one of three airports in the country chosen for this program. Ronald Regan Washington National and Tampa International airports are also using the new technology.

Source: <http://www.newschannel5.com/Global/story.asp?S=6651771>

15. *June 13, CheapFlights (United Kingdom)* — Passengers for Spain must provide personal data. Passengers flying to Spain have been reminded that, starting Wednesday, June 13, they will have to provide their airlines with personal information. The so-called advance passenger information (API) includes full given names, surnames, nationality, date of birth, and travel document number (usually the passport number). Spain is the first country in Europe to introduce compulsory API, but the policy will likely be extended to other European Union states within the next year. The move is aimed at improving aviation security in Spain.

Source: http://news.cheapflights.co.uk/flights/2007/06/passengers_for_.html

16. *June 13, Federal Computer Week* — GPS central to air traffic control's future, experts say. Airline industry leaders stressed the importance of Global Positioning System (GPS) satellites in the Federal Aviation Administration's (FAA) plan for revamping and expanding the United States, antiquated air traffic control system at an industry roundtable in Washington, DC, on June 12. FAA's new program will rely on Automatic Dependent Surveillance-Broadcast (ADS-B), which uses transponders aboard planes and GPS satellites to determine aircraft position with much greater accuracy. "It is the surveillance technology necessary to provide the command and the control of aircraft competing for the limited and increasingly more restricted airspace that will be essential to meet the growing demands of our national airspace system,"

said Capt. Bart Roberts of American Airlines at the event. FAA has started using a system based on ADS-B along the Eastern Seaboard and has conducted operational evaluations in Alaska and the Ohio Valley. Experts say ADS-B will let pilots and air traffic controllers determine an aircraft's position with respect to other planes and geographic features with far greater accuracy. Experts say the ADS-B technology will enhance a pilot's situational awareness, increase safety, improve navigation and boost capacity.

Source: <http://www.few.com/article102973-06-13-07-Web>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

17. *June 13, Agriculture Research Service* — Scientist pinpoints when weeds are most meddlesome. "Field intelligence" gathered by an Agricultural Research Service (ARS) scientist could give sweet corn growers a new edge in their war on weeds. Based on field studies he has conducted near Urbana, IL, since 2004, ARS ecologist Marty Williams has identified specific timeframes during the sweet corn growing season when competition from weeds will inflict yield losses. Moreover, this so-called critical period for weed control is influenced by the sweet corn planting date, notes Williams, who works in ARS' Invasive Weed Management Research Unit at Urbana.

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

18. *June 12, Animal and Plant Health Inspection Service* — USDA proposes to adjust export certification user fees for plants and plant products. The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) Tuesday, June 12, announced a proposal to adjust the user fees charged for export certification of plants and plant products. These user fees would be increased for fiscal years 2007 through 2012 to reflect the anticipated costs associated with providing export certification services each year. In addition, APHIS is also proposing to add a new user fee for exporters who obtain federal export certificates for plants and plant products from state or county cooperators in order to recover administrative costs associated with that service. These proposed changes, which are the first in 10 years, would enable APHIS to properly recover the costs of providing export certification services for plants and plant products.

Source: http://www.aphis.usda.gov/newsroom/content/2007/06/plantfee_shtml

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

Food Sector

19. *June 13, Associated Press* — Japan finds no problems after inspecting U.S. meatpacking facilities. Japan said Wednesday, June 13, it has found no safety problems at dozens of U.S.

meatpacking facilities it inspected last month. Japanese officials inspected 28 meatpacking plants in 14 states in May to evaluate their compliance with restrictions Japan imposed over mad cow disease concerns. Public broadcaster NHK said that the two countries are expected to hold talks on easing restrictions on U.S. beef as early as this month. Japan only allows imports of U.S. beef from cattle not more than 20 months old. The U.S. has called for that restriction to be eased.

Source: http://mdn.mainichi-msn.co.jp/business/news/20070613p2g00m0b_u004000c.html

20. *June 13, Globe and Mail (Canada)* — **Tainted chocolate seized by police after trip to landfill.** When Toronto, Canada, police officers patrolling Tuesday, June 12, came across two men "suspiciously" unloading large skids from a rental vehicle, they pulled over to investigate. What they discovered were eight large, shrink-wrapped pallets holding tens of thousands of Hershey's chocolate products — potentially contaminated with salmonella. The chocolate bars were part of a huge Hershey Canada recall from last November triggered by the discovery of salmonella in an ingredient at a Hershey's factory in Smiths Falls, Ontario. Hershey Canada had contracted waste-management company Turtle Island Recycling to dispose of the affected chocolate bars, police said. "When we ruled out that the product had not been stolen from a factory, we discovered that it had actually come from the landfill," said Detective Tam Bui. "It turned out that one of the individuals works at Turtle Island and had intercepted the pallet" before it was disposed of, he said.

Source: <http://www.theglobeandmail.com/servlet/story/LAC.20070613.HERSHEY13/TPStory/National>

21. *June 12, Yonhap News (South Korea)* — **South Korean housewives launch watchdog to check safety of U.S. beef.** South Korean housewives launched a nationwide monitoring team on Tuesday, June 12, to check the safety of U.S. beef, which is expected to go on sale again soon after a three-year import ban because of fears about mad cow disease. One of the key missions of the team, consisting of more than 200 housewives, is aimed at inspecting whether local retailers of U.S. beef will comply with a law requiring them to identify the meat's origin and results of health inspections to ensure public safety, said the Korea Life Cooperative Federation (KLCF). "The monitoring team was designed to block sales of U.S. beef carrying a risk of mad cow disease," said Lee Jeong-joo, chairman of the federation. The "on-the-spot" monitoring team will visit discount stores, meat distributors and family restaurants to carry out its mission, Lee said.

Source: <http://english.yonhapnews.co.kr/business/2007/06/12/25/0502000000AEN20070612002500320F.HTML>

[[Return to top](#)]

Water Sector

22. *June 12, Reuters* — **Marines drank tainted water for 30 years.** As many as 75,000 people may have drunk water contaminated by dry cleaning fluid at the Marine base at Camp Lejeune in North Carolina, the U.S. Centers for Disease Control and Prevention (CDC) said on Tuesday, June 12. The contamination lasted for 30 years until the affected wells were closed, and Marines and their families drank the affected water during their average two-year assignments at the base, the CDC said. The water was polluted with tetrachloroethylene, also known as PCE,

a dry cleaning solvent that has been linked with cancer, the CDC said. "But the effects of consumers' exposure to drinking water contaminated with PCE are not known. Some health studies have found adverse effects in occupational settings. However, exposure to PCE alone typically does not mean a person will experience adverse health effects," the CDC said. The affected area is the Tarawa Terrace family housing area, and the contamination lasted from November 1957 through February 1987, the agency said. An off-base dry cleaners leaked the fluid into a septic system near the housing area's well.

Source: <http://www.reuters.com/article/domesticNews/idUSN1228270320070612?feedType=RSS&rpc=22>

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

Public Health Sector

23. June 13, Reuters — Some Muslim states not ready to fight bird flu: WHO. Some Muslim countries are ill-prepared to tackle an outbreak of bird flu because of poor resources and public apathy, a World Health Organization (WHO) official said at a meeting of Islamic nations on Wednesday, June 13. Health ministers of the 57-nation Organization of the Islamic Conference (OIC) open a two-day meeting in the Malaysian capital on Thursday, June 14, to map out a common plan to tackle a possible influenza pandemic and fight polio and malaria. WHO official Hassan El Bushra told reporters the OIC could help member states produce bird flu vaccine and anti-viral drugs. But officials said the wide economic disparity among OIC nations — which range from wealthy oil-rich Saudi Arabia to poor war-torn Somalia and Afghanistan — could undermine the group's ambitions to jointly fight bird flu.

Source: http://in.today.reuters.com/news/newsArticle.aspx?type=worldNews&storyID=2007-06-13T144101Z_01_NOOTR_RTRMDNC_0_India-302876-1.xml&archived=False

24. June 13, Associated Press — Glaxo to donate flu vaccine for poor. Pharmaceutical company GlaxoSmithKline PLC has agreed to donate 50 million doses of H5N1 vaccine to the World Health Organization (WHO) in an attempt to create a pandemic vaccine stockpile for poor countries, company officials announced Wednesday, June 13. The vaccines will be delivered over a three-year period and should provide enough doses for 25 million people; two shots per person will be needed. While the stockpile is a reassuring development in pandemic preparedness planning, many questions remain. WHO has not said how the vaccine stockpile might be distributed — a key concern since nearly every country worldwide will be clamoring for vaccine to save its population during a pandemic. Nor has WHO addressed the question of how the vaccines might be delivered. In most countries that will need the vaccine, health infrastructures are weak and it is uncertain if people could get the vaccine, even if it were available.

Source: http://biz.yahoo.com/ap/070613/pandemic_vaccine_stockpile.html?v=1

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

Government Sector

25. *June 13, Government Computer News* — **Facial recognition around the world.** Many other countries are moving much more aggressively than the United States on implementing face recognition technologies — particularly for surveillance. “Worldwide, outside of the United States, there is a strong market for video surveillance requirements,” said Roger Kelesoglu, business development executive at Cognitec Systems. “In the United States, it’s more used for [identification] cards.” Joseph Atick, executive vice president at L-1 Identity Solutions, agrees. He added, however, that “that’s not to say that the intelligence agencies are not utilizing facial recognition” for such surveillance purposes. In short, in the United States as well as overseas, the public may not be aware of the most cutting-edge implementation of face recognition technologies. Still, information that has been made public shows a broader adoption of these technologies overseas. The Australian Customs Service already has an automated border processing system called SmartGate that uses face recognition. It compares the face of the individual with the image in the e-passport microchip, certifying that the person presenting the passport is the rightful owner. In September 2006, the German Federal Criminal Police Office announced it had awarded a contract to provide a system to identify suspects by comparing surveillance images to a digital photo archive.

Source: http://www.gcn.com/print/26_13/44425-1.html?topic=techreport

26. *June 12, NOAA News Online* — **NOAA expands Great Lakes research.** On Tuesday, June 12, the National Oceanic and Atmospheric Administration (NOAA) announced the establishment of a new Great Lakes Cooperative Institute to conduct collaborative research through a consortium of universities and institutions in the Great Lakes region. Research efforts will focus on forecasting; invasive species, control, impact, and assessment; the Great Lakes Observing System; protection and restoration of resources; and Great Lakes education and outreach. The Cooperative Institute for Limnology and Ecosystems Research is comprised of a consortium of academic institutions. NOAA currently supports 21 Cooperative Institutes in 17 states focusing on research ranging from satellite climatology and fisheries biology to atmospheric chemistry and coastal ecology. Cooperative Institutes are located at parent institutions whose geographic expanse extends from Hawaii to Massachusetts and from Alaska to Florida. NOAA is dedicated to enhancing economic security and national safety through the prediction and research of weather and climate-related events and information service delivery for transportation, and by providing environmental stewardship of our nation's coastal and marine resources.

Source: <http://www.noaanews.noaa.gov/stories2007/s2875.htm>

27. *June 12, Associated Press* — **FBI warns universities to watch out for spies.** The head of the FBI's Boston office is warning the region's top universities to be on the lookout for foreign spies or potential terrorists who might be trying to steal unclassified, yet sensitive, research. FBI agents met recently with officials at Harvard University, Massachusetts Institute of Technology, the University of Massachusetts, and other schools to train professors, students and security staff on how to recognize anyone who might be trying to exploit research, Special Agent in Charge Warren Bamford said. Bamford stressed that the FBI is not seeking to censor information or stop the free flow of information, just raise awareness. Worcester Polytechnic Institute President Dennis Berkey said the FBI told researchers to protect laptops, especially in foreign countries, and to be wary about who contacts them about their work.

Source: http://www.govexec.com/story_page.cfm?articleid=37165&sid=60

Emergency Services Sector

28. *June 11, wwaytv3.com (NC)* — **North Carolina county holds terrorism drill.** A terrorism drill took place Sunday, June 10, in Brunswick County, NC. Heather Heigl with Brunswick County Emergency Services said, "There is a terrorist plot that the terrorist tried to blow up the natural gas and the parazylyene line, and that was just a diversion technique on their way to the Brunswick County nuclear power plant." Then the mock terrorists escape in their car and cause an accident. Heigl said, "An innocent by-stander comes by to offer help and that's when the terrorists high-jack the innocent person and take them as a hostage into the Belville Elementary School." The exercise did help emergency officials find ways to improve. Thompson said, "We noticed that some of our contact list for notification there were some areas where we need to make some corrections on, update some information." Overall, the exercise was a success. The SWAT team captured the terrorists and emergency responders practiced important, life-saving emergency procedures.

Source: http://www.wwaytv3.com/brunswick_county_holds_terrorism_drill/06/2007

Information Technology and Telecommunications Sector

29. *June 12, US-CERT* — **Technical Cyber Security Alert TA07-163A: Microsoft Updates for Multiple Vulnerabilities.** Microsoft has released updates to address vulnerabilities that affect Microsoft Windows, Windows Secure Channel, Internet Explorer, Win32 API, Visio, Outlook Express and Windows Mail as part of the Microsoft Security Bulletin Summary for June 2007. The most severe vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system. Microsoft has provided updates for these vulnerabilities in the June 2007 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Administrators are encouraged to note any known issues that are described in the Bulletins and test for any potentially adverse effects. System administrators may wish to consider using an automated patch distribution system such as Windows Server Update Services (WSUS).

June 2007 Security Bulletins: <http://www.microsoft.com/technet/security/bulletin/ms07-jun.msp>

Source: <http://www.us-cert.gov/cas/techalerts/TA07-163A.html>

30. *June 12, Federal Computer Week* — **Air Force moves to populate Cyberspace Command.** The Air Force is developing plans for a dedicated force to populate the ranks of the service's new Cyberspace Command, its commanding general said Tuesday, June 12. Lt. Gen. Robert Elder, commander of the 8th Air Force and chief of the new command, said the service will finish deliberations on a force structure for the command within a year and then start filling those positions. Once service officials have laid out career paths and training guidelines for the jobs, Elder said, recruits will be able to join what he called the Air Force's cyberforce just as they could opt to become fighter pilots or navigators. He estimated there are now 40,000 men and women in the service conducting cyberoperations in one form or another. He said the

question will be defining which of those service members would fall under the ranks of the new Cyberspace Command.

Source: <http://www.fcw.com/article102972-06-12-07-Web>

31. *June 12, Security Focus* — **Flaw hunters go off on Safari.** Less than a day after Apple released a beta version of its Safari Web browser for Windows, three vulnerability researchers have already found a handful of bugs, many which appear to work against the currently shipping version of the browser for Mac OS X. Security researcher David Maynor, infamous for his row with Apple over three wireless flaws he presented at the Black Hat Security Briefings in 2006, claims to have found six vulnerabilities in Safari. Four of the vulnerabilities are simple denial-of-service bugs that crash the browser, but two of the flaws allow remote execution, he said. Two other researchers have found bugs as well. Thor Larholm, a well-known Danish security researcher, claims to have discovered another remotely exploitable flaw, while Israeli researcher Aviv Raff described a memory corruption that may be exploitable.

Source: <http://www.securityfocus.com/brief/523>

32. *June 11, Government Computer News* — **Standard for Web-based digital signatures completed.** A standard to enable digital signing of electronic documents via a Web application has been finalized by the Organization for the Advancement of Structured Information Standards (OASIS). Digital Signature Services Version 1.0 (DSS), approved by OASIS this month, defines an Extensible Markup Language interface to process digital signatures for Web services and other applications without complex client software. The Web-based scheme should simplify the creation and verification of digital signatures and could improve security by centralizing storage and management of cryptographic signing keys. A digital signature uses cryptography to bind the creator's signature or assertion to an electronic document or other form of data, which in turn can be used by others to authenticate the source of the data and ensure that it has not been tampered with since its creation. This serves much the same purpose as a traditional written signature and enables electronic transactions at a level of trust and assurance similar to paper-based transactions. Because digital signatures require creation and management of cryptographic keys, implementation can be complex, especially in large enterprises. The goal of DSS is to help overcome the complexity.

Source: http://www.gcn.com/online/vol1_no1/44444-1.html

33. *June 11, TechWorld (UK)* — **Law puts damper on Web security research.** Web security research is being seriously hampered by laws that punish researchers for even attempting to locate flaws in Web software, much less disclosing those flaws, according to a new study. The report is the first by the Computer Security Institute, a research and training organization under the aegis of CMP Technology. It draws on discussions by a broad working group, including security researchers and representatives of U.S. law enforcement agencies. The upshot is that current legal frameworks designed to allow prosecution of Web attackers also make it next to impossible to legally spot security flaws in the "Web 2.0" applications quickly becoming ubiquitous on the Internet. Those researchers who do feel safe probing Web software for flaws are probably not aware of their real legal position, the report said.

Free PDF of the report is available (registration required):

http://www.gocsi.com/forms/fbi/csi_workinggroup.jhtml

Source: <http://www.techworld.com/security/news/index.cfm?newsID=9113 &pagetype=all>

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

34. *June 12, Associated Press* — Explosives found in South Dakota mailboxes. Brown County, SD, authorities are investigating reports of explosives that were found in two mailboxes. A mail carrier discovered one of the explosives southwest of Aberdeen, and a bomb squad was called from Sioux Falls to dispose of it. A pop bottle filled with chemicals was found in Aberdeen in another mailbox, but authorities say it had already exploded. No one was hurt in either incident. Source: <http://www.kxmb.com/News/132769.asp>

[[Return to top](#)]

General Sector

35. *June 13, St. Louis Post-Dispatch* — Material to make bombs is stolen. Explosives capable of causing "extensive damage" have been stolen from a St. Charles County, MO firing range used by the sheriff's office and the FBI, federal officials said Tuesday, June 12. Officials are still trying to determine how much dynamite, C-4 and other explosives were taken and exactly who was responsible. Mike Schmitz of the federal Bureau of Alcohol, Tobacco, Firearms and Explosives said investigators believe more than one person was involved in the theft, but it is too early to know the intent of the thieves, including whether terrorism could be involved. The theft, discovered by the FBI on Tuesday, happened sometime in the past ten days. The explosives, including C-4, dynamite and safety fuse, were being stored at the St. Charles County training center and firearms range at 1835 South Highway 94, Schmitz said. The range is located in a rural area. They were stored properly in the federally approved storage magazine, which resembles a large construction Dumpster, Schmitz said. The metal explosives magazine where the materials were stored is used by the FBI and the sheriff's office for training and for rendering other explosives or suspected explosives safe, Schmitz said. "These items are all extremely dangerous," Schmitz said.

Source: <http://www.stltoday.com/stltoday/news/stories.nsf/stcharles/story/D58ACE075F7151F3862572F90011F21A?OpenDocument>

[[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.