



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 14 June 2004

Current Nationwide  
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- NBC News reports the Los Angeles Blood and Platelet Center has begun notifying about 145,000 donors that they could be victims of identity theft because a laptop computer containing their personal data was stolen. (See item [7](#))
- The Associated Press reports a potential incendiary device — motorcycle-type battery with wires leading into a brown bottle about eight ounces in size — was removed from near a Washington state ferry terminal. (See item [13](#))
- The Associated Press reports authorities in the Baltimore region are planning to build a network of around-the-clock surveillance cameras to target crimes from terrorism to drug dealing. (See item [35](#))
- The US-CERT has released "Technical Cyber Security Alert TA04-163A: Cross-Domain Redirect Vulnerability in Internet Explorer." (See item [36](#))

### DHS/IAIP Update *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [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:** [General](#); [DHS/IAIP Web 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://esisac.com>]

1. *June 11, Associated Press* — **Water supply worries plant.** The Laramie River Station near Wheatland, WY, is looking to buy about ten-thousand acre-feet of water normally used for irrigating farmland to ensure the plant can keep running into at least early 2006. The coal-fired

electricity generating facility is part of one of the largest consumer-owned power supply projects in the country. It is owned by six electrical co-ops that supply power to parts of Wyoming, Colorado, South Dakota, Minnesota and Nebraska. **The plant relies on water from Grayrocks Reservoir, located about seven miles away on the Laramie River. However, the drought has reduced the water in the reservoir to about 37 percent of capacity.** John Barnes of the Wyoming State Engineer's Office says this is the first time a coal-fired plant indicated to the state problems coming up with water for the cooling process.

Source: <http://www.kgwn.tv/home/headlines/826497.html>

2. *June 11, AFX News Limited* — **OPEC output exceeds May quota by twelve percent.** OPEC's 10 members with quotas pumped an average of 26.36 million barrels of crude oil per day in May, according to a Platts survey of OPEC and oil industry officials, exceeding their current agreed upon ceiling of 23.5 million barrels per day by more than 12 percent, with all 10 members exceeding their individual quotas. **The May output also exceeded the output ceilings agreed upon at the June 3 meeting of 25.5 billion barrels of crude a day, effective July 1, and of 26 million barrels per day, effective August 1,** Platts said. "The high crude prices which have prevailed since late last year have allowed OPEC to turn a blind eye to overproduction," Platts said. "That tacit acceptance of leakage beyond official levels is set to continue for the time being, according to OPEC sources."

Source: <http://www.ecommercetimes.com/story/34415.html>

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

## Chemical Industry and Hazardous Materials Sector

3. *June 10, The Courier-Journal News (Louisville, KY)* — **Plants detail impact of toxic releases; worst-case scenarios unlikely, industry says.** An unchecked release of toxic chemicals from any one of dozens of plants in the Louisville, KY, metropolitan area — from chemical plants to a commercial bakery — could sicken thousands of residents. And the potential impact can go far beyond a company's property, according to risk-management plans filed by the companies with the U.S. Environmental Protection Agency. **The plans outline what might happen if there's a spill or some other kind of chemical release if everything goes wrong — a scenario that companies and emergency responders agree is not likely and has never happened in the metro area.** Planning for accidents and understanding how they might affect surrounding neighborhoods gives the public, government and public-health coordinators a better idea of what could go wrong and how many people could be affected, officials told The Courier-Journal. **Among the six Kentucky and Indiana counties around metro Louisville, Jefferson County has the most industrial operations required to file plans outlining worst-case scenarios,** the newspaper found. The report is available at this url site.

Source: <http://www.courier-journal.com/localnews/2004/06/10toxic/A9-risk0601-15747.html>

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

## Defense Industrial Base Sector

4. *June 11, Daily Press (VA)* — **Navy may shrink fleet of attack subs.** The Navy could be heading toward a smaller submarine fleet, which would delay plans to increase submarine production, a leading naval analyst said Thursday, June 10. Today's fleet of 55 attack submarines could shrink to 50 boats or even 40 boats, depending on how the Navy rethinks submarines' missions, said Ronald O'Rourke, a veteran analyst for the Congressional Research Service. The Navy plans to begin buying two subs a year in 2009. It now buys one a year. Reducing the fleet to 40 submarines would delay the need for increased production until about 2012, O'Rourke said. However, **Navy officials have repeatedly delayed plans to increase sub production, mostly because of financial pressures. Despite a surge in defense spending since the Iraq war, Navy leaders have begun rethinking the rationale for subs that cost upward of \$2 billion a copy.** The Navy plans to conduct a fresh study on shipbuilding needs as part of its 2006 budget submission.

Source: <http://www.dailypress.com/business/local/dp-26325sy0jun11.0.5502623.story?coll=dp-business-localheads>

5. *June 09, Financial Times* — **U.S. Air Force urges defense deals for Europe. The U.S. Air Force secretary has called for European defense contractors to get more access to Pentagon contracts to stimulate stiffer competition in the U.S. domestic aerospace industry. James Roche, who controls a \$90bn annual budget, warned that consolidation among U.S. contractors in the 1990s had left Washington overdependent on a small number of key suppliers in certain sectors.** He said the main way to correct this was to encourage overseas manufacturers to compete for defense department spending. Roche's push comes despite recent political pressure to restrict foreign participation in defense contracts to protect U.S. manufacturing jobs and punish reluctant allies in Europe. He conceded that political differences over Iraq could make co-operation more difficult in the short term, but said it was in the long term interests of the U.S. to encourage innovation and push down prices by competition. Although moves to direct more contracts to European companies would face considerable political hurdles, they could bode well for several high-profile competitions involving European companies.

Source: <http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1086445547861&p=1012571727088>

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

## **Banking and Finance Sector**

6. *June 10, The Taipei Times (Taiwan)* — **Hackers prey on Internet banking.** The numbers and personal codes of more than 100,000 Internet banking and auction-site clients are feared to have been stolen by hackers from across the Taiwan Strait. **Criminal Investigation Bureau officials in Taiwan said on Wednesday, June 9, that they had arrested a Taiwanese man named Chen Chung-shun and seized a huge amount of confidential data, including 45 million e-mail addresses, almost 200,000 bank and auction-site account numbers with their corresponding personal secret codes, and information on three figurehead bank accounts.** Investigators believe Chen has been collaborating with Chinese hackers since February to steal Internet bank codes by planting "shell" or "revised" versions of "Trojan horse" programs into the personal computers of customers using Internet banking services. Chen had reportedly gathered 45 million Taiwanese e-mail addresses, and in mid-February, he started

sending advertising e-mails containing shell or revised Trojan horses to those e-mail addresses. By mid-March, he had sent out over 18 million e-mails. Officials said the ring withdrew the money from the International Commercial Bank of China ATM machines in China, or transferred it to hundreds of figurehead accounts which had been established in the names of 10 Taiwanese people.

Source: [http://www.taipeitimes.com/News/taiwan/archives/2004/06/10/2\\_003174478](http://www.taipeitimes.com/News/taiwan/archives/2004/06/10/2_003174478)

7. *June 10, NBC4-TV (CA)* — **Blood donors could be victims of identity theft. The University of California Los Angeles Blood and Platelet Center has begun notifying about 145,000 donors they could be victims of identity theft because a laptop computer containing their personal data was stolen.** The computer, taken from a locked UCLA van in November, contained the names, Social Security numbers, dates of birth and blood types of donors. UCLA Healthcare officials said they did not realize the significance of what they had lost until early May, during an internal evaluation of data security. The information on the computer was password-protected but did not have the sophisticated encryption codes UCLA now uses, meaning the laptop's data could be accessible to a tech-savvy criminal, said Dr. Michael McCoy, spokesperson for UCLA Healthcare.

Source: <http://www.nbc4.tv/news/3403445/detail.html>

8. *June 10, MercoPress (South America)* — **Bomb explodes outside bank in Chilean capital. The group calling itself "Julio Guerra, Southern Operation" took responsibility for the blast in a phone call to Santiago, Chile's Bio Bio radio station. The pre-dawn explosion caused considerable structural damage to a Banco del Estado office in the La Cisterna municipality, some six miles from downtown Santiago. The caller said the attack had been staged in retaliation for delays in passing a bill on behalf of people imprisoned for crimes sanctioned in anti-terrorist legislation. Large chunks of concrete broke off the second story of the Banco del Estado building and three ATMs were destroyed, military police Chief Lt. Col. Esteban Marcusovic said. "The explosion of this bomb is particularly serious, because it demonstrates greater destructive power and shows that this group is bigger and better organized," Deputy Interior Secretary Jorge Correa Sutil said. Also, attacks on restaurants and apartments have been occurring.**

Source: <http://www.mercopress.com/Detalle.asp?NUM=3775>

9. *June 09, The Denver Channel* — **Counterfeit \$100 bills showing up.** Counterfeit \$100 bills are circulating in Fort Morgan, CO, and authorities are trying to figure out where they came from. Fort Morgan State Bank reported Monday, June 7, that an area merchant had received two counterfeit \$100 bills. **Officials said the fake notes were actually \$5 bills that had been bleached out, with \$100 bills printed over them. Counterfeit pens will not work on these bills, according to the bank.** The serial number on the bills is the same: CB36391339E. Chamber of Commerce officials warned businesses and individuals to check carefully for counterfeit currency -- matching the watermark of the president to the picture printed on the bill.

Source: <http://www.thedenverchannel.com/news/3400449/detail.html>

10. *June 09, Canadian Press* — **Royal Bank warns of e-mail fraud. The Royal Bank of Canada is warning its customers about an e-mail fraud that asks clients for personal information regarding their accounts, an apparent scam aimed at taking advantage of the bank's**

**recent computer system problems.** The Royal Bank said it learned Wednesday, June 9, that e-mails are being sent out asking customers to verify account numbers and personal identification numbers, or PINs, through a link included in the e-mail. **The message states that if they don't click on the link and key in their client card number and passcode, access to the account will be blocked.** Royal Bankd spokesperson Judi Levita said she wasn't aware of any Royal clients who had fallen prey to the e-mail fraud, but feared some customers might believe that it was necessary for them to provide the information given the bank's recent computer problems. A recent software update caused the bank's computers to malfunction, preventing customer accounts from being updated. The error impacted payroll deposits that were scheduled to enter many accounts.

Source: <http://cnews.canoe.ca/CNEWS/Canada/2004/06/09/pf-492507.html>

11. *June 09, The Hindu Business Line (India)* — **E-mail fraud on ICICI Bank customers. Online fraudsters targeted ICICI Bank customers through spam mail that asked them to disclose passwords and other information, but the bank said no financial loss was reported so far.** E-mails from "support@icici.com" with the subject "Important information from ICICI Bank" and "Official information from ICICI Bank" started circulating from Monday, June 7. Once opened, the mail asked customers to click on a link and provide personal information. "It's not easy to say how many of our customers have got it. First, we felt it will be a large number. But now our assessment is it's a small number," and ICICI Bank the spokesperson said. ICICI Bank sent e-mail to its customers, warning them about the fraud and urging not to respond to such mails. The ICICI Bank spokesperson said the bank has alerted the cyber crime cells about the spam mails. However, the origin of the spam mail had not been traced, he said. ICICI Bank is India's second largest bank.

Source: <http://www.thehindubusinessline.com/2004/06/10/stories/2004061001880800.htm>

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

## **Transportation Sector**

12. *June 10, Department of Transportation* — **Federal Transit Administration approves new phase of work on rail to Dulles. The Federal Transit Administration (FTA) nudged rail to Dulles a step forward by allowing the project to move into preliminary engineering.** Preliminary engineering is the second phase of a three-part process in which the project's design, scope and cost are refined before construction can begin. This approval does not guarantee that the project will be approved to enter the Final Design phase of project development. The FTA will continue to monitor and evaluate the project throughout the development process as information concerning costs, benefits and impacts is refined. In order to be considered for any future grants, all federal requirements must be met as rail to Dulles continues through the rigorous project development process. The Dulles Corridor Rail Project — Extension to Wiehle Avenue — is a joint venture between the Virginia Department of Rail and Public Transportation and the Washington Metropolitan Area Transit Authority.

Source: <http://www.dot.gov/affairs/fta1704.htm>

13. *June 10, Associated Press* — **Potential incendiary device removed from near a Washington state ferry terminal. The device was a motorcycle-type battery about half the size of a car battery with wires leading into a brown bottle about eight ounces in size, Washington**

**State Patrol Lt. Helmut Steele said. The bottle was less than half full of an unknown liquid, he added.** A bomb squad "rendered the device safe" and it was removed for further investigation, including identification of the liquid, Steele said. He would not say how the apparatus was neutralized or taken from the scene. A passenger getting off the ferry on the Kitsap Peninsula noticed a 12-foot aluminum skiff tied to the dock at the terminal about 9:45 p.m. Thursday, June 10, and alerted a crew member who took a closer look and spotted the device, Steele said. A crew member untied the small boat from the dock, and it drifted onto a nearby beach and was tied to a piece of driftwood by the time the first state troopers arrived, he said. **Ownership of the skiff was under investigation. No written threats or warning notes were found, nor did investigators know of any earlier verbal threats, security problems or other sign of trouble at the ferry terminal,** Steele said. Southworth-Vashon ferry service is part of a run linking West Seattle, Vashon and Southworth. Service between Vashon and the Fauntleroy dock in West Seattle was not affected. Other ferry runs and overland roads link the Seattle area and the Kitsap Peninsula.

Source: [http://seattletimes.nwsources.com/html/localnews/2001953776\\_w ebdevice11.html](http://seattletimes.nwsources.com/html/localnews/2001953776_w ebdevice11.html)

14. *June 10, Washington Technology* — **DHS consolidates screening efforts.** Department of Homeland Security (DHS) Secretary Tom Ridge has approved the creation of an office within the Department of Homeland Security that will coordinate all screening efforts, said Asa Hutchinson, DHS undersecretary for Border and Transportation Security. **The Office of Screening Coordination is part of the Border and Transportation Security Directorate,** Hutchinson said. It will coordinate the efforts of programs such as U.S. Visit, the entry-exit system at air, land and sea borders; the National Targeting Center, which provides targeting technology, methodology and subject-matter expertise to various federal agencies; and the Computer Assisted Passenger Prescreening System II, which identifies potentially dangerous airline travelers.

Source: [http://www.washingtontechnology.com/news/1\\_1/homeland/23740-1.html](http://www.washingtontechnology.com/news/1_1/homeland/23740-1.html)

15. *June 10, Associated Press* — **Glove shortage for airport screeners threatens safety, union says.** The union representing some of the baggage screeners at Newark Liberty International Airport says there has been a chronic shortage of the latex gloves used for baggage searches. The federal Transportation Security Administration (TSA) acknowledged there have been brief glove shortages resulting from "delivery issues," but insisted Thursday, June 10, that those issues had been resolved. The situation is not only a hazard to the screeners, said the union, but also undercuts the mission of the TSA to secure the nation's airways by making screeners reluctant to search bags thoroughly. In addition to going through X-ray machines, many of the tens of millions of bags checked or carried onboard aircraft at Newark each year are hand-searched. **Screeners are supposed to wear disposable latex gloves provided by the TSA. The gloves are supposed to be worn for only one bag, then thrown away to avoid the possibility of cross-contamination.**

Source: <http://www.nynewsday.com/news/local/transportation/ny-bc-nj--airportscreeners-0610jun10.0.6963063.story?coll=nyc-manhead lines-trans>

16. *June 10, Associated Press* — **Fuel prices spur airlines to focus on conservation.** Pilots for Ted, United Airlines' low-fare carrier, flew 14 mph slower at cruise altitude over the Memorial Day weekend. At American Airlines, planes flying trans-Atlantic flights now carry less emergency fuel, to lighten their loads. And at JetBlue Airways, pilots are using one engine

instead of two to taxi along congested runways. **With high oil prices stifling the airline industry's recovery, U.S. carriers are finding ways to cut back on the amount of fuel they use, placing an emphasis on fuel efficiency not seen since the 1980s energy crisis.** Some carriers said they recently lowered their fuel-burn rate in the air and on the ground by as much as three percent on certain routes. That is not nearly enough to counter the industry's anticipated loss of \$3 billion in 2004, but the amount saved is not chump change either for a business that spends roughly one out of every seven of its pennies at the pump.

Source: [http://www.thedesertsun.com/news/stories2004/business/200406\\_10002247.shtml](http://www.thedesertsun.com/news/stories2004/business/200406_10002247.shtml)

17. *June 09, CongressDaily* — **U.S. Coast Guard expects facilities, vessels to meet deadline. A top U.S. Coast Guard official said on Wednesday, June 9, that he expects most of the facilities and vessels required to submit security plans and gain approval of them from the Coast Guard will meet a July 1 deadline for improving security at the nation's ports and waterways.** "I think on July 1 we'll be in pretty darn good shape," Rear Adm. Larry Hereth, the Coast Guard's director of port security, told the House Transportation and Infrastructure Coast Guard Subcommittee during a hearing on implementing a 2004 maritime security law. Hereth said he is "more confident on the vessel side" than on the facilities side that most will meet the deadline for gaining approval and implementing their security plans. Of the 3,200 port facilities covered by the law, Hereth said that nearly 1,300 have submitted and had their security plans approved by the Coast Guard. About 1,800 other facilities have submitted their plans and are awaiting approval, while about 75 have failed to submit plans at all.

Source: <http://www.govexec.com/dailyfed/604/060904tdpm1.htm>

[[Return to top](#)]

## **Postal and Shipping Sector**

18. *June 10, Government Computing News* — **Postal service upgrading address recognition systems.** The U.S. Postal Service has contracted with a company to introduce address recognition capability earlier in the mail processing cycle to help speed mail delivery. **Under a \$33 million contract, the company will upgrade remote computer reader machines at 350 U.S. postal centers to provide greater sort capability on 1,086 advanced facer canceller systems. The machines position envelopes so postage can be canceled and envelopes can be marked with an identification tag that enables further processing.** The improvements "allow us to be more efficient and serve our customers better because we're consolidating high-speed mail sorting technology and eliminating several mail processing functions," said Tom Day, vice president of engineering for the U.S. Postal Service. The upgrade uses enhanced optical character recognition technology.

Source: [http://gcn.com/vol1\\_no1/daily-updates/26170-1.html](http://gcn.com/vol1_no1/daily-updates/26170-1.html)

[[Return to top](#)]

## **Agriculture Sector**

19. *June 11, Republican (ME)* — **Salmon virus poses a threat. Wild Atlantic salmon in the Merrimack River in Massachusetts and the Penobscot River in Maine have tested positive**

**for a deadly virus that could threaten salmon runs there and in the Connecticut River.**

The disease, called infectious salmon anemia virus, first appeared in Canada's ocean pen salmon farms in 1996. Since then, it has killed or caused to be destroyed millions of farmed salmon in Canada and Maine as it has moved south. However, no Connecticut River salmon have so far shown evidence of the disease, according to the U.S. Fish and Wildlife Service. Using a new test that has only recently become available, service biologists tested stored blood samples from 304 salmon that returned to the Connecticut River between 1996 and 2001 and found no evidence any of the fish were exposed to the virus. However, 10 salmon that returned to the Merrimack River and four from the Penobscot River showed evidence of exposure. "There is the threat of it occurring in the Connecticut River. However, our goal is to keep it out of the river and out of the national fish hatchery system," said Daniel M. Kuzmeskus, chief of the Northeast Division of Hatcheries for the wildlife service.

Source: <http://www.masslive.com/hampfrank/republican/index.ssf?/base/news-7/108694026861990.xml>

20. *June 11, Associated Press* — **Kansas launches effort to help animals during disasters.** While most rescue efforts after a large-scale disaster focus on humans, officials from several Kansas agencies want to extend the same kind of emergency help to animals. **The Kansas Animal Disaster Preparedness plan is designed to prepare a statewide network of agencies and volunteers who will fan out to rescue, feed, and bury animals. The team will respond to natural disasters, bioterrorism, and widespread animal diseases, such as foot-and-mouth.**

It's based on a program started in North Carolina after Hurricane Floyd struck in 1999, killing millions of poultry, cattle, swine, and pets. More than 120 veterinarians and state officials met leaders of the North Carolina State Animal Response Team, which leads animal rescue efforts in that state. While many of the details of Kansas' plan are not final, it generally expands plans the state already has for dealing with foreign animal diseases, said Sheila Dodson, a veterinarian from Shawnee who serves on a steering committee developing the Kansas response.

Source: <http://www.ljworld.com/section/stateregional/story/172714>

21. *June 11, New Scientist* — **Genome of Sudden Oak Death bug cracked. The genome of the fungal pathogen that causes Sudden Oak Death has been sequenced by U.S. scientists.** Brett Tyler, of the Virginia Bio-informatics Institute, and Dan Rokhsar and colleagues at the Joint Genome Institute in California, revealed the 65 million-long sequence of DNA base pairs that make up *Phytophthora ramorum's* 15,000 genes on Thursday, June 10. **It is the first member of the *Phytophthora* family to be sequenced. The researchers hope that the map of *P. ramorum's* genetic code will pinpoint genes and their proteins that will allow them to detect, track, and treat the disease.** The completion of the sequence coincides with heightened worries over the spread of the Sudden Oak Death in the U.S. following the discovery in March that an infected California nursery had spread the disease nationwide through plant shipments. Plant pathologists now fear that the East coast Appalachian forests could be infected.

Source: <http://www.newscientist.com/news/news.jsp?id=ns99995102>

22. *June 11, Lexington Herald Leader (KY)* — **Early blue mold hits Kentucky. Blue mold, the scourge of tobacco growers, is producing its spores in Central Kentucky, according to warnings issued by the University of Kentucky College of Agriculture.** The disease has

been confirmed in Fayette, Jessamine, Bourbon, Garrard, Logan, Hart, Green, Taylor, Adair, and Bracken counties. Blue mold watches — where conditions are favorable for a spread of the disease — are in place for many surrounding counties. **Blue mold has already rendered entire greenhouses of tobacco useless and has the potential to severely damage field crops, said UK plant pathologist William Nesmith.** "If we can't get a handle on the situation here, we could lose 25 to 35 percent of our crops," said Robert Amburgey, Jessamine County agricultural extension agent. Tobacco farming is a \$9 million industry in Jessamine County. Source: <http://www.kentucky.com/mld/kentucky/business/8895906.htm>

23. *June 11, San Francisco Chronicle* — **Insect threat to wine country.** Insects that spread a disease lethal to grapevines have been found in Vacaville, CA, striking fear into the heart of California's premium wine-producing region in nearby Napa Valley. **A colony of glassy-winged sharpshooters — half-inch-long insects that subsist on the fluids of various plants, including vines and fruit trees — were discovered by Solano, CA, agricultural agents early this week.** The sharpshooters spread Pierce's disease — an incurable malady that devastates grapevines by clogging xylem, the plant tissue that transports water and nutrients. "It's very significant. It's just way too close to the Napa Valley," said Greg Clark, the assistant agricultural commissioner for Napa County. **Until now, sharpshooter infestations have been concentrated in Southern California, where Pierce's disease has decimated vineyards. In the north, infestations have been limited to a few isolated spots. The latest discovery is by far the closest to Napa and Sonoma.** It's too early to know how difficult it will be to contain the infestation. If it hasn't spread much beyond the area where it was discovered, officials said it should be relatively easy to eliminate. But if it has spread more widely, it'll be a much tougher problem.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/06/11/SHARPSHOOTERS.TMP>

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

## **Food Sector**

24. *June 11,* — **Bad dumplings scandal swells.** The Korea Food and Drug Administration (KFDA) Thursday, June 10, released a list of companies guilty of supplying mandu, or Korean dumplings, containing spoiled radish, which has spurred public distrust over food standards. **The scandal has even migrated abroad, prompting Japan to impose a temporary ban on mandu imports.** The state-run agency identified 12 companies that have used below-standard radishes to make dumplings between last year and February this year. The companies must destroy their remaining inventories. The KFDA said the relevant companies received the sordid vegetable from a local source, which takes up 70 percent of the local market as a supplier of the item. **The company imported the radishes, which were headed for the dump, from China and were reportedly cleansed under unsanitary conditions.** The issue surfaced Monday, June 7, when the KFDA announced that it was recalling mandu brands that were more fit for the waste dump rather than consumption.

Source: [http://www.koreaherald.co.kr/SITE/data/html\\_dir/2004/06/11/2\\_00406110022.asp](http://www.koreaherald.co.kr/SITE/data/html_dir/2004/06/11/2_00406110022.asp)

25. *June 09, Food and Drug Administration* — **Whole almonds recalled.** Apple Valley Natural Foods is conducting a voluntary recall on its distribution of raw whole almonds packaged

**as Almonds–Whole Raw Natural due to the possibility of contamination with Salmonella Enteritidis.** The recalled almonds are packed in one pound packages under the Apple Valley Vegetarian Foods Emporium label. Salmonella is an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. In rare circumstances, infection with Salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis. Apple Valley Natural Foods distributes this product in Michigan and Illinois. This recall is in follow-up to a voluntary recall announced in mid-May by Paramount Farms of California of whole and diced raw almonds based on over 20 possible cases of illnesses associated with the almonds.

Source: [http://www.fda.gov/oc/po/firmrecalls/applevalley06\\_04.html](http://www.fda.gov/oc/po/firmrecalls/applevalley06_04.html)

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

## **Water Sector**

**26. *June 09, Tahoe Daily Tribune (CA)* — Surveyors use seismic waves to study MTBE contamination.** Results due this summer from a seismic survey will hopefully lead to a better understanding of how methyl tertiary butyl ether (MTBE) contaminated water moves underground at South Shore. **The information from the survey, conducted last week, may allow the South Tahoe, CA, Public Utility District to better contain and treat water contaminated by MTBE.** It is a gasoline additive that has shut down 13 public water wells since it was discovered it had leaked underground at South Shore in 1997. The district had the pump removed from its Martin Avenue well so that surveyors could send seismic waves 205 feet down its foot-wide shaft. The seismic waves were measured by receivers dropped to a variety of levels within the well.

Source: <http://www.tahodailytribune.com/apps/pbcs.dll/article?AID=/20040609/News/106090009/-1/NEWS>

**27. *June 08, Scotsman (United Kingdom)* — Filtration protects patients from pathogens in hospital water.** A study, conducted at the Veterans Administration Pittsburgh, PA, found that the 0.2-micron Pall-Aquasafe(TM) Water Filter completely eliminated Legionella pneumophila and Mycobacterium spp and achieved a greater than 99 percent reduction in heterotrophic bacteria in the water samples. Each year over two million Americans acquire an infection while at a hospital, and tap water is a significant contributor. Serious infections of the lung (pneumonia) and blood (bacteremia), can be caused by a host of bacteria, such as Legionella, Pseudomonas, and fungi, such as Aspergillus. These microorganisms can contaminate faucets, taps, and showers in hospitals. Although these organisms are normal inhabitants of water systems and do not harm healthy individuals, they can be especially dangerous to patients with compromised immune systems. Mortality for hospital-acquired Legionnaires disease and Pseudomonas aeruginosa bacteremia approaches 40 percent.

Source: <http://news.scotsman.com/latest.cfm?id=3035316>

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

## **Public Health Sector**

28. *June 11, Global Security Newswire* — **Progress on biological defenses.** The U.S. has made progress in developing several new treatments and vaccines against a variety of biological weapons agents, with some set to be introduced into U.S. defenses by the end of 2005, Anthony Fauci, the head of the U.S. National Institute of Allergy and Infectious Diseases told Global Security Newswire. **A new smallpox vaccine that poses less risk from side effects than the current inoculation has entered Phase 1 safety trials after having been found to provide protection in monkeys and mice, Fauci said.** The new vaccine, which is being jointly developed by the National Institutes of Health and several pharmaceutical companies, could be introduced into the national pharmaceutical stockpile by the end of next year. Progress has also been made in developing a more advanced vaccine against anthrax, Fauci said. He said that a contract is likely to be awarded by the end of the summer to produce 75 million doses of the new vaccine. **In addition, a new Ebola vaccine is set to undergo Phase 1 safety trials, Fauci said.** He also said the Bush administration is seeking to develop at least two treatments against every Level A pathogen as classified by the U.S. Centers for Disease Control and Prevention. **Such agents include smallpox, anthrax, botulism toxin, tularemia, and hemorrhagic viruses.**

Source: <http://www.govexec.com/dailyfed/0604/061004gsn1.htm>

29. *June 11, Agence France Presse* — **Hong Kong hospital alert as rare disease kills maid.** Hong Kong is in the throes of another health scare, with hospital bosses raising the alert on a rare disease that has claimed only its second ever victim in the former British colony. **The Hospital Authority chief has ordered all suspected cases of Japanese encephalitis to be reported to a special unit following the death Thursday, June 10, of an Indonesian woman from the disease.** The alert comes weeks after Hong Kong lowered its risk assessment of the killer avian flu and Severe Acute Respiratory Syndrome (SARS). Under the emergency arrangements, doctors who diagnose patients with any form of encephalitis must report the case to the city's Center for Health Protection special unit. **The death of the 29-year old maid was classified a local infection as she had not left Hong Kong in the past two years, an authority spokesperson said.**

Source: [http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20040611/hl\\_afp/health\\_hongkong\\_alert\\_04061108\\_3951](http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20040611/hl_afp/health_hongkong_alert_04061108_3951)

30. *June 10, Associated Press* — **Researchers exposed to anthrax. At least five workers developing an anthrax vaccine at a children's hospital research lab in Oakland, CA, were accidentally exposed to the bacterium because of a shipping mistake, officials reported Thursday, June 10.** Officials with the Children's Hospital Oakland Research Institute said none of the researchers has shown symptoms of infection since the first exposure about two weeks ago, but each is being treated with precautionary antibiotics. The researchers believed they were working with syringes full of a dead version of anthrax, hospital spokesperson Bev Mikalonis said. Instead, they were shipped live anthrax by a lab of the Southern Research Institute in Frederick, MD, Mikalonis said. Anthrax produces severe flu-like symptoms in most of its victims. If inhaled, ingested or otherwise introduced into the body, it can kill. **Other workers may also have been exposed while the researchers handled the live anthrax, Mikalonis said, a possibility that federal, state, and local officials are investigating.** Though the five workers were exposed, state health officials and the hospital don't believe anyone was infected because the researchers took proper safety precautions.

Source: [http://news.yahoo.com/news?tmpl=story&cid=541&u=/ap/20040611/ap\\_on\\_he\\_me/anthrax\\_exposure\\_1&printer=1](http://news.yahoo.com/news?tmpl=story&cid=541&u=/ap/20040611/ap_on_he_me/anthrax_exposure_1&printer=1)

31. *June 10, Voice of America* — **First SARS human vaccine trial. World Health Organization (WHO) officials say a Chinese lab has begun clinical tests of a Severe Acute Respiratory Syndrome (SARS) vaccine, but it may take at least five years before the product is available to the public.** Director of WHO's vaccine research unit, Marie-Paule Kieny, told reporters four patients who received their shots two weeks ago at a Chinese laboratory are reported in good health. They are the first of 36 volunteers to test the vaccine. The inventor of the measles vaccine, Stanley Plotkin, cautions that in spite of encouraging results, it will take at least five years before a vaccine is approved for sale.

Source: <http://www.voanews.com/article.cfm?objectID=D0F8AAE6-0184-4E58-B091D9DD9AAB2F8C>

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

## Government Sector

32. *June 10, Federal Computer Week* — **House panel seeks homeland spending boost. The House Appropriations Committee has approved a \$32 billion Homeland Security Department spending plan for fiscal 2005 that includes increases for several agencies involved in technology research and development.** The bill, which was approved after a full committee markup June 9, is \$2.8 billion more than the department's fiscal 2004 appropriations and \$896 million higher than what the Bush administration's requested. In a prepared statement, Rep. Hal Rogers (R-KY), chairman of the committee's Homeland Security Subcommittee, said while a significant amount has been accomplished, there's more that needs to be done. "It is important that we provide the money and the tools to continue progress in areas such as container security, critical infrastructure protection and border security," he said. "We must also provide DHS with the tools and resources to respond to the ever-changing threat environment. The bill before us today does just that. It supports ongoing work and includes initiatives to move us closer to our goals of prevention, preparedness and response."

Source: <http://fcw.com/fcw/articles/2004/0607/web-dhs-06-10-04.asp>

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

## Emergency Services Sector

33. *June 10, The Trucker* — **Objections delay Hazmat rule effective date. A rule that would allow other government agencies to regulate portions of hazardous materials transport was set to become effective October 1, but will now be delayed until January 1, 2005, according to a Federal Register notice.** The Research and Special Programs Administration (RSPA), part of the Department of Transportation, published the notice of delay in the May 28 Federal Register. The Final Rule was originally published October 30, 2003, and was issued to clarify the applicability of the Hazardous Materials Regulations (HMR) to specific functions and activities, including hazmat loading and unloading operations and storage of hazmat during transportation, according to the May 28 notice. RSPA stated that it received 14 appeals of the

Final Rule concerning a number of issues related to the consistency of the rule with federal hazmat transportation law; state and local regulation of hazmat facilities; the relationship of the HMR to regulations by other agencies; and some of the specific definitions in the Final Rule. RSPA stated that the issues raised by appellants were detailed and complex, causing the agency to delay the effective date to provide it with sufficient time to fully address the issues raised. Source: [http://www.thetrucker.com/stories/06\\_04/0610\\_hazmat\\_reg.html](http://www.thetrucker.com/stories/06_04/0610_hazmat_reg.html)

34. *June 10, Associated Press* — **Boston, New York police take notes on G–8.** Police from New York City and Boston have taken note of the tiny number of protesters who showed up at the G–8 summit here — and they're taking notes. **The police officials are in Georgia monitoring the tight, omnipresent security surrounding the Group of Eight summit to see what they can learn for this summer's national political conventions.** It's not clear how easily those lessons can be adapted to July's Democratic convention in Boston or August's Republican convention in New York. Sea Island is a remote barrier island, easily sequestered from the mainland. Still, activists fear that the massive security presence surrounding the summit will be a model for future events. Everywhere protesters went, they were joined by officers and soldiers, often with military helicopters overhead and sometimes with gunboats in the background. Security personnel — some with military Humvees — were stationed along roads. Caravans of state troopers drove around from morning to night with their lights on and sirens blaring. Source: [http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718&e=10&u=/ap/20040610/ap\\_on\\_re\\_us/summit\\_convention\\_lessons](http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718&e=10&u=/ap/20040610/ap_on_re_us/summit_convention_lessons)

35. *June 10, Associated Press* — **Baltimore plans 24–hour surveillance.** Authorities in the Baltimore region are trying to build a network of around–the–clock surveillance cameras to target crimes from terrorism to drug dealing, the state's homeland security chief said. "We're at war," said Dennis R. Schrader, director of homeland security for Gov. Robert Ehrlich. Dozens of surveillance cameras are already in place to deter crime throughout downtown Baltimore, but those images are generally taped and reviewed only occasionally. The new images will be monitored by about a dozen retired police officers or criminal justice college students, said Elliot Schlanger, Baltimore's chief information officer. The closed–circuit video surveillance of public areas will begin in the Inner Harbor by summer's end. **A \$2 million federal grant accepted by the city Wednesday, June 9, will expand the cameras by November into downtown's west side, which includes rail lines, government buildings and cultural institutions. The city system could connect with an existing state system of closed–circuit cameras that monitor highways.** Surrounding counties would also eventually plug into the city's hub, and Baltimore would also work toward links with closed–circuit systems at the University of Maryland and Oriole Park at Camden Yards. Source: [http://www.newsday.com/news/nationworld/nation/sns–ap–surveillance–cameras,0,5164132.story?coll=ny–nationalnews–headline\\_s](http://www.newsday.com/news/nationworld/nation/sns–ap–surveillance–cameras,0,5164132.story?coll=ny–nationalnews–headline_s)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

36. *June 11, US–CERT* — **Technical Cyber Security Alert TA04–163A: Cross–Domain Redirect Vulnerability in Internet Explorer.** There is a cross–domain vulnerability in the

way Microsoft's Internet Explorer (IE) determines the security zone of a browser frame that is opened in one domain then redirected by a web server to a different domain. A complex set of conditions is involved, including a delayed HTTP response (3xx status code) to change the content of the frame to the new domain. **Other programs that host the WebBrowser ActiveX control or use the MSHTML rendering engine, such as Outlook and Outlook Express, may also be affected.** By convincing a victim to view an HTML document (web page, HTML email), an attacker could execute script in a different security domain than the one containing the attacker's document. By causing script to be run in the Local Machine Zone, the attacker could execute arbitrary code with the privileges of the user running IE. **Publicly available exploit code exists for this vulnerability, and US-CERT has monitored incident reports that indicate that this vulnerability is being actively exploited.** Workarounds are available on the US-CERT Website.

Source: <http://www.us-cert.gov/cas/techalerts/TA04-163A.html>

**37. June 10, FCC** — **FCC promotes the deployment of wireless broadband services by creating new rules for the 2495–2690 MHz band while protecting educational services.** The Federal Communications Commission (FCC) Thursday, June 10, adopted a Report and Order and Further Notice of Proposed Rulemaking that transforms the rules governing the Multipoint Distribution Service (MDS) and Instructional Television Fixed Service (ITFS) in the 2495–2690 MHz band. **The Order creates a new band plan for 2495–2690 MHz which eliminates the use of interleaved channels by MDS and ITFS licensees and creates distinct band segments for high power operations.** The order enames the MDS service the Broadband Radio Service (BRS), while maintaining the ITFS label for ITFS licenses and operations. **The Order also expands the original MDS-ITFS band by adding to it five megahertz of additional spectrum from below 2500 MHz,** which increases the total size of the band to 194 megahertz. In addition, the Order lifts all non-statutory eligibility restrictions on BRS spectrum, including those applicable to cable operators.

Source: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-248267\\_A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-248267_A1.pdf)

**38. June 10, FCC** — **Commission adopts spectrum sharing plan to promote the efficient use of spectrum.** The Federal Communications Commission (FCC) Thursday, June 10, adopted a spectrum sharing plan for low earth orbit satellite systems (Big LEOs) in the 1.6 GHz and 2.4 GHz bands. **The spectrum sharing plan will further the Commission's goal of efficient spectrum utilization by increasing the number of providers offering services to consumers over the same spectrum, and will promote the deployment of more innovative services to consumers.** The Commission also issued a Further Notice of Proposed Rulemaking to explore whether CDMA and TDMA MSS operators feasibly could share an additional 2.25 megahertz of spectrum at 1616.0–1618.25 MHz. Action by the Commission by Report and Order, Fourth Report and Order and Further Notice of Proposed Rulemaking (FCC 04-134).

Source: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-248343\\_A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-248343_A1.pdf)

**39. June 10, National Journal** — **DHS has no plans to update cybersecurity strategy.** The time for reviewing the federal cybersecurity strategy has not come yet despite flaws that need to be addressed, Amit Yoran, director of the Department of Homeland Security's cyber-security division, said Thursday, June 10. Yoran said at a SecureE-Biz.net conference that **new issues have arisen since the strategy was released, such as a focus on securing "control systems" for infrastructure like chemical manufacturing or power systems.** Experts are working to

improve preparedness for problems, meaning better identification of attacks and dissemination of information and security patches. The private sector is key to that success, Yoran said, and the agency is working to encourage improved software development with more secure code, and to improve evaluation methods for finding bugs and malicious code sent by developers, whether they are foreign or domestic. He said **DHS will continue to invest in that, as well as ways to counter cyber crime, test data sets and improve methods for the economic analysis of cyber attacks.** "We're looking at technology as the soft underbelly of all the nation's critical infrastructure," Yoran said.

Source: <http://www.govexec.com/dailyfed/0604/061004tdpm1.htm>

40. *June 10, eSecurity Planet* — **Multiple flaws found in open source CVS.** Security researchers have found multiple potential security flaws in one of the main tools of modern open source code management, the Concurrent Version System (CVS). One vulnerability involves a flaw that could lead to a missing NULL terminator; others relate to an error\_prog\_name string, an argument integer overflow and an out of bounds issue in serv\_notify code. **A malicious attacker could theoretically exploit that vulnerability to execute code, execute commands, read sensitive information, or cause a denial of service attack . Even an anonymous user with only read-only access could exploit the vulnerability on an un-patched server.** New versions of CVS, 1.12.9 and 1.11.7, as well as binaries for most major Linux distributions are available: <http://www.cvshome.org>.  
Source: <http://www.esecurityplanet.com/alerts/article.php/3366541>

41. *June 10, SecurityFocus* — **Report: Computer intrusion losses waning.** Computer intrusions are on the decline for the third year in a row, according to an annual survey conducted by the Computer Security Institute (CSI) and the FBI's computer crime squad. Nearly 500 computer security professionals in U.S. corporations, government agencies, financial institutions, medical institutions and universities responded to the 2004 survey, with 53 percent reporting that their organization experienced unauthorized use of computer systems during the prior 12 months—down from 56 percent in 2003. **Thirty-five percent believed they had not been breached, and 11 percent said they didn't know.** Overall financial losses totaled out to \$141 million for the 269 respondents willing to quantify their losses, down significantly from 251 respondents reporting \$202 million in losses in 2003. **Despite federal government efforts to encourage information sharing between industry and the Department of Homeland Security, the percentage of companies suffering intrusions who reported them to law enforcement dropped from 30 percent to 20 percent;** the most common reason for keeping an intrusion quiet was fear of negative publicity. The survey is available here: <http://www.gocsi.com/>  
Source: <http://securityfocus.com/news/8883>

42. *June 10, Government Computer News* — **Cybercrime getting the attention of DHS.** Cybercrime is emerging as the leading IT threat, public and private-sector security experts said Thursday, June 11, at a summit hosted by SecurE-Biz.net in Washington. Crime now ranks above the threat of cyberterrorism on the Department of Homeland Security radar screen, according to Amit Yoran, head of the DHS's cyber security directorate. John Watters, CEO of iDefense Inc., said **nations are incorporating information operations into their military strategies -- in plain terms, they are learning to hack their enemies. But it is difficult to assess the level of activity because it often is masked by the activity of traditional rogue**

**hackers.** Cyberterrorists are highly motivated, but have not yet developed the level of organization or the skills necessary to carry out serious attacks. But Watters said there is a danger that advances in exploitation of IT vulnerabilities by criminal organizations will be adopted by nations and terrorists. The development of wholesale markets for stolen data, such as credit card information, is driving organized criminal activity online.

Source: [http://www.gcn.com/vol1\\_no1/daily-updates/26173-1.html](http://www.gcn.com/vol1_no1/daily-updates/26173-1.html)

## Internet Alert Dashboard

**DHS/US-CERT Watch Synopsis**

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

**Watch Synopsis:** We continue to receive reports of Korgo Worm Infections from both Public and Private organizations. Such reports indicate that not all organizations have successfully patched their networks for the LSASS vulnerability mentioned in Microsoft Bulletin MS04-011. Most infections in organizations have been traced to Insecure partner VPN connections to external organizations or infected laptops introduced into the network without prior verification that the systems were patched and virus-free.

**Current Port Attacks**

<b>Top 10 Target Ports</b>	135 (epmap), 1434 (ms-sql-m), 1433 (ms-sql-s), 445 (microsoft-ds), 137 (netbios-ns), 9898 (dabber), 5554 (sasser-ftp), 25 (smtp), 1026 (nterm), 1027 (icq)
----------------------------	--

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

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

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

## General Sector

**43. June 10, Associated Press — Tourists flocking back to bridges, dams. Tourists are flocking back to the nation's engineering marvels the dams, bridges and other structures that had seen increased security and lightened visitor traffic since September 2001 despite the fact that they're still potential terrorist targets.** Golden Gate Bridge spokesperson Mary Currie said it is difficult to determine how many visit the Golden Gate because no admission is charged, but tourism appears to be gradually coming back after September 11 and the area's dot-com demise. **Although tourism is recovering, increased security has changed what visitors can do and see at popular sites.** Traffic across the tops of larger dams, such as Grand Coulee and Hoover, has been restricted or banned. Boats patrol waters nearby and formerly public areas have been reduced. Interior Secretary Gale Norton recently announced that portions of the Statue of Liberty, closed since the attacks, would reopen to tourists this summer

after safety and security upgrades.

Source: [http://abcnews.go.com/wire/US/ap20040610\\_1159.html](http://abcnews.go.com/wire/US/ap20040610_1159.html)

**44. June 10, Associated Press — Powell blames new data collection system for understating number of terror attacks.** The State Department's annual report on terrorism mistakenly reported a worldwide decline when both the number of incidents and the toll in victims had actually increased sharply, the State Department said Thursday, June 10. Administration officials had used the findings announced last April as evidence President Bush's campaign to counter terror was succeeding. **Secretary of State Colin Powell said Thursday, June 10, the errors were the result of new data collection procedures. "I can assure you it had nothing to do with putting out anything but the most honest, accurate information we can," he said.** Department spokesman Richard Boucher said, "We got the wrong data and did not check it enough." He added, "Our preliminary results indicate that the figures for the number of attacks and casualties will be up sharply from what was published."

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/news/archive/2004/06/10/national1346EDT0622.DTL>

**45. June 09, Fox News — UN finds banned missile engines in Jordan. United Nations (UN) weapons experts have found 20 engines used in banned Iraqi missiles in a Jordan scrapyard along with other equipment that could be used to make weapons of mass destruction, an official said Wednesday, June 9.** The discoveries were revealed to the UN Security Council by acting chief UN inspector Demetrius Perricos during a closed-door briefing. The text was obtained by The Associated Press. **The UN team was following up on an earlier discovery of a similar Al Samoud 2 engine in a scrapyard in the Dutch port of Rotterdam. Perricos said inspectors also want to check in Turkey, which has also received scrap metal from Iraq.** The UN team also discovered some processing equipment with UN tags -- which show it was being monitored -- including heat exchangers, and a solid propellant mixer bowl to make missile fuel, he said. It also discovered "a large number of other processing equipment without tags, in very good condition."

Source: <http://www.foxnews.com/story/0,2933,122311,00.html>

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

### DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source

published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 883-3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.