Department of Homeland Security Daily Open Source Infrastructure Report for 24 January 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports oil prices might soar past $100 a barrel if the United Nations Security Council authorizes trade sanctions against Iran −− which the West accuses of trying to make nuclear bombs −− and Iran curbs oil exports in retaliation. (See item 1)
- The Denver Post Business reports the 2005 Global Business Security Index reports a shift in cybercrime from massive outbreaks to smaller, stealthier attacks targeted at specific organizations for extortion purposes. (See item 8)
- USA TODAY reports an antiquated warning system for the nation's pilots has led dozens of them to receive unreliable information about slippery runways and to land in dangerous conditions, according to a review of accidents and pilot reports during the past decade. (See item 17)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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. *January 22, Associated Press* — **Oil could top $100 a barrel if UN imposes sanctions on Iran over nuclear program.** A recent surge in oil prices to almost $70 a barrel on concerns about the restart of Iran's nuclear program only hints at what may lie ahead. Prices could soar

past $100 a barrel, experts say, if the UN Security Council authorizes trade sanctions against the Middle Eastern nation, which the West accuses of trying to make nuclear bombs, and Iran curbs oil exports in retaliation. A sharp global economic slowdown could follow. The United States and European nations face this dilemma as they decide whether to act. Iran, the second−largest oil producer within the Organization of the Petroleum Exporting Countries, exports roughly 2.5 million barrels per day −− one million barrels more than current excess production capacity worldwide. It also controls the strategic Strait of Hormuz, a critical shipping lane in the Middle East. "Even if Iran pulled a small amount of its oil off the market, say it pulled a half million barrels a day, I could see oil prices literally jumping over the $100 per barrel mark," said James Bartis, of the Rand Corp. But other oil analysts say prices would likely not climb much higher than $75 a barrel before strategic reserves would be released.
Source: http://www.moneysense.ca/news/company_news/shownews.jsp?content=D8F9U2780_ap#

2. *January 22, Augusta Chronicle (GA)* — **Plan for nuclear storage bolsters security.** The Department of Energy (DOE) is preparing to consolidate plutonium at the Savannah River Site in one place to strengthen its defenses against terrorism and improve its ability to monitor the radioactive material. An unspecified amount will be moved from the site's F−Area, where it was produced for decades, to a former nuclear reactor where there are additional stockpiles, according to agency documents. "This will be a more secure, hardened facility," said Perry Holcomb, a member of the SRS Citizens Advisory Board that monitors site activities. At least two independent reports show that the upgrades are needed. One by the Defense Nuclear Facilities Safety Board in 2003 stated that current storage facilities at SRS lack proper fire protection, ventilation and filtration, and the ability to remove plutonium from storage containers to ensure its stability. A report by the Government Accountability Office last year reiterated those points and encouraged the DOE's planned changes. The agency's remodeling plans would make it possible to open plutonium containers for testing and provide the ability to monitor them from the outside, the agency's proposal states. A DOE committee is investigating the consolidation of excess plutonium from around the country in one place.
Source: http://chronicle.augusta.com/stories/012306/met_6302057.shtml

3. *January 21, Associated Press* — **Nigerian militia leader behind kidnappings threatens new attacks.** An American worker held hostage in Nigeria is sick and his kidnappers will kill three fellow hostages if he dies, a militant leader threatened Saturday, January 21. Brutus Ebipadei of the Movement for the Emancipation of the Niger Delta did not say why his group would kill hostages from Britain, Bulgaria and Honduras if he died. Ebipadei said the kidnappers refused to negotiate and he reissued a threat to launch new attacks on installations in the oil−rich Niger Delta. "Our demands are not negotiable. And failure to meet those demands means we will launch attacks on all oil installations to stop Nigeria's capacity to export oil," Ebipadei said. The militants demand the release of a former regional governor and a militant leader who pushed for greater local control of revenues from the delta. Nigeria, Africa's leading oil producer, exports about 2.5 million barrels of oil a day, making it the fifth−largest source of U.S. oil. A major Shell pipeline leading was blown up the next day and more attacks followed in other areas. The attacks have cut the OPEC−member nation's crude output by nearly 10 percent. Shell has evacuated hundreds of workers since the unrest began.
Source: http://www.nctimes.com/articles/2006/01/22/news/nation/18_27_341_21_06.txt

4. *January 19, Federal Energy Regulatory Commission* — **Federal Energy Regulatory Commission reports gas supply adequate for winter.** According to a report released by the Federal Energy Regulatory Commission, gas supply appears to be adequate for this winter. Several other agencies' statistics take into account this year's warmer−than−normal winter temperatures. An Energy Information Administration's recent report indicated a net injection into U.S. storage, which is unusual for late December. This is largely due to the unseasonably warm weather, in addition to a lower level of withdrawal for every degree of cold weather this winter. Gas supply assessments show that progress continues in returning gulf production, slowing somewhat in the past month. The level of shut−in gas from the offshore, as reported by the Minerals Management Service, is now about 1.8 billion cubic feet (or Bcf) per day. Shut−in onshore Louisiana gas, which was reported as totaling as much as 2.0 Bcf/d immediately after hurricane Rita, is now down to a little less than 0.6 Bcf/d. Today, a little less than 2.4 Bcf/d is not flowing due to the hurricanes. Given weather conditions this winter, supply overall appears to be adequate for U.S. needs through the winter, though prices could still spike on cold weather and local deliveries could be affected by local factors.
   Report: http://www.ferc.gov/EventCalendar/Files/20060119153924−A−3−w eb.pdf
   Source: http://www.ferc.gov/

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *January 23, Federal Computer Week* — **Panel seeks changes to DoD acquisition system.** The Department of Defense (DoD) is reviewing eight major recommendations from an independent panel on how to fix the military's acquisition system. The panel's recommendations, issued in December 2005, cover every aspect of acquisition policy. The Defense Acquisition Performance Assessment (DAPA) Project, a panel of nine military, industry and education officials, was formed last summer to advise DoD on acquisition changes that could help speed delivery of weapon systems to the battlefield. The panel's most significant recommendation involves the creation of new organizations, called service systems commands, in the Army, Navy and Air Force. A four−star general or flag officer would lead the new organizations and report to the services' acquisition secretaries and top officers. Another recommendation calls for DoD's top acquisition official to budget and manage a modernization account. Paul Kern, a panel member and retired Army four−star general, said stable defense programs require industry to submit more realistic contract bids. Kern also said industry needs to reinvest more of its DoD sales revenue in research and development to preserve the military's technological superiority. DoD will publish the DAPA Project's final report later this month. The department will likely implement the recommendations in six−month intervals, Kern said.
   Source: http://www.fcw.com/article92056−01−23−06−Print

6. *January 20, Aviation Week* — **Net−centric defense leaders spell out needs from industry.** A

star−laden panel of U.S. military leaders responsible for network−centric systems told industry contenders Thursday, January 19, to focus their product pitches on protecting networks, helping with limited spectrum allocation and assisting information sharing across disparate networks for the U.S. military, nongovernmental organizations and allied nations. The panel, which appeared at the Institute for Defense and Government Advancement's annual Network Centric Warfare conference in Washington, DC, indicated no revolution was likely in how the Department of Defense tries to implement a net−centric environment across the military arena, especially because of budget constraints, so companies proposing "paradigm shift" products will have a harder time. In response to an audience question from a small−business entrepreneur, Navy Rear Adm. Elizabeth Hight, principal director for Global Information Grid operations at the Defense Information Systems Agency (DISA), said DISA would continue to try to adopt existing systems across the domain before buying new ones. Next, military services and agencies are supposed to buy existing information technology on the commercial market, rather than contract for wholly new IT.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/NETC01206.xml

7. *January 19, Aviation Week* — **To maintain interoperability, Air Force standards must be enforced in industry contracts.** A series of flight demonstrations at Eglin Air Force Base, FL, has helped confirm the idea that it will be possible to integrate air−to−ground weapons into network−centric operations, according to the U.S. Air Force. More than 140 bomb runs in 12 typical types of missions showed that various weapons can use standard methods to confirm their status after release from an aircraft, report it to networks, and provide information on their impact, just as testers planned, the Air Force said Tuesday, January 17. The demonstrations were carried out under the Weapons Data Link Network (WDLN) advanced concept technology demonstration (ACTD). The goal of the effort, which has been achieved, is to define a standard way for aircrew, ground controllers and air operations centers to have two−way communications with network−enabled weapons after they're already in flight, the Air Force said. Lynda Rutledge of Eglin's Air Armament Center said there will be some challenges. For one thing, if interoperability is to be maintained, standards must be strictly observed, meaning they must be enforced in contracts with industry, and that configuration control is vital.
Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/EGLIN01196.xml

[Return to top]

Banking and Finance Sector

8. *January 23, Denver Post Business (CO)* — **Hackers' attacks more calculating.** IBM's annual security index shows fewer mass attacks, but a rise in stealth attacks that are useful for extortion. Attacks on computer systems are down, but more skillfully planned, according to a report released Monday, January 23, by IBM. The year−end 2005 Global Business Security Index reports a shift in cybercrime from massive outbreaks to smaller, stealthier attacks targeted at specific organizations for extortion purposes. David Mackey, head of the team compiling the report, said "In 2005, we saw almost a complete dropoff with mass outbreaks...What has sprung up is an underground economy for credit card information or

extortion." Trends in 2006 are likely to include an increased use of "botnets" to undertake malicious online activity. Attacks on large corporations from insiders also pose greater risks. Mackey said software that can attack cell phones and PDAs, specifically phones using Bluetooth technology, are at risk in 2006, as attackers develop more sophisticated software. In 2005, one in every 36 e−mails contained a virus or Trojan horse, compared to 2004, when one in every 16 e−mails contained malicious software. Phishing threats are on the rise, with one in every 304 e−mails being a hoax, compared to one in every 943 in 2004.
Source: http://www.denverpost.com/portlet/article/html/fragments/print_article.jsp?article=3426261

9. *January 23, MarketWatch* — **UK banks keeping up with scammers.** UK banks are responding to scamming attacks by devoting more staff to fighting fraud, teaching staff through training courses how to spot fraud, said Ken Farrow, head of anti−fraud operations at Lloyds TSB (LYG). Barclays PLC (BCS), which has larger credit−card operations, has increased its anti−fraud staff to 550 from about 400 two years ago. "Sleeper" fraud, a practice in which scammers either create a fake identity or use another person's to open a new account with a bank, is on the rise. For several months scammers use the account as any normal customer would and build a good credit rating. Then they take out a loan or charge their credit cards to the max and disappear. Sleeper fraud in which the used identity is that of someone who has died rose by 60 percent last year to about 112,000 cases, the fastest rate of any type of identity fraud in the country, according to CIFAS, the UK's bank fraud protection service. A relatively new type of fraud that is particularly worrying involves a gang of impostors getting jobs within a bank and stealing information after establishing the trust of other employees.
Source: http://www.marketwatch.com/tools/quotes/newsarticle.asp?guid=%7BE39D0E44−8F2A−4153−8785−235116A64E67%7D&dist=rss&siteid= mktw

10. *January 21, Associated Press* — **National Guard officers' personal information stolen.** A briefcase containing personal information about hundreds of California National Guard officers was stolen from an employee's vehicle, officials said. National Guard spokesperson Maj. Jon Siepmann declined to say where in California the Saturday, January 7 break−in occurred because the thief may not realize the importance of what was stolen. Siepmann said, "Somebody broke into a car and stole a briefcase...It's not apparent that they had any idea what was in the briefcase." The names were included, along with the Social Security numbers and dates of birth of the officers, according to a memo distributed Wednesday, January 18, by Maj. Gen. Jeffrey L. Gidley. The memo was sent to warn Guard officers that their personal information could be used and to be on the alert for possible identity theft.
Source: http://www.nctimes.com/articles/2006/01/22/military/21_17_20_1_21_06.txt

[Return to top]

Transportation and Border Security Sector

11. *January 23, Department of Transportation* — **More freight moves over transportation system than previously reported.** More freight moves on the nation's transportation system than previously reported and almost one out of 10 tons of freight shipments is related to international trade, according to “Freight in America,” a new report from the Department of Transportation’s Bureau of Transportation Statistics (BTS). Working jointly on the

calculations, BTS, a part of the Research and Innovative Technology Administration, and the Department's Federal Highway Administration estimate that over 19 billion tons of freight, valued at $13 trillion, was carried over 4.4 trillion ton−miles in 2002. These new estimates include previously uncovered sectors such as construction, retail, services, and municipal solid waste. In other trends, the BTS report finds that growing demand for more efficient and faster delivery of high−value, low−weight products is changing the structure of the freight industry, creating new alliances among shippers, carriers, and logistics providers. At the same time, enormous volumes of bulk commodities −− whether grains, lumber, ores, coal, or oil −− continue to move into, out of, and within the United States.
Report: http://www.bts.gov/
Source: http://www.dot.gov/affairs/bts0406.htm

12. *January 23, Business Travel News* — **Port Authority to improve passenger flow.** The board of commissioners of the Port Authority of New York and New Jersey, which operates John F. Kennedy International Airport (JFK), LaGuardia Airport, and Newark Liberty International Airport, recently approved a $5 billion budget for 2006 that includes major investments in those three facilities, focused on getting passengers into and through the airport more quickly. Specifically, the 2006 budget funds the construction of a new terminal at JFK and renovations and improvements at Terminal B at Newark Liberty. There is planning money included in the budget to look at potential future upgrades at Newark and LaGuardia. Also, the long−term plan calls improved rail connections for all three New York−area airports, for the purchase of additional trains and cars for the AirTrains serving Newark and JFK, and "a one−seat ride from JFK to Midtown Manhattan." It also calls for a $520 million investment to extend PATH service from Newark's Penn Station to Newark Liberty Airport.
Source: http://www.btnmag.com/businesstravelnews/headlines/frontpage_display.jsp?vnu_content_id=1001882598

13. *January 23, Associated Press* — **Approval expected for Gary/Chicago airport funds.** The Department of Transportation is expected to approve $57.8 million to expand and improve the Gary/Chicago International Airport. The approval could bring more than 300 new jobs to the area and help the airport stake its claim as the third major airport in the Chicago area, officials said in a news release last week. The expansion would enable larger jets to land at the airport and increase the size of the runway's safety zones. The Gary airport is one of 300 airports nationwide that does not meet the latest runway safety standards. Officials for years have discussed whether a third Chicago area airport was needed to help relieve congestion at O'Hare and Midway airports. Gary has requested about $90 million over the next 10 years to extend runways and terminals for a predicted threefold increase in passengers by 2012. Officials have also been trying to attract airlines. Recently, airport officials were disappointed when Hooters Air temporarily stopped service from the airport. Service is expected to resume in March. Currently, no carrier is providing scheduled passenger service from Gary.
Source: http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20060123/News01/601230325/CAT=News01

14. *January 23, Logistics Management* — **Tulsa's Port of Catoosa returning to normal shipping levels.** Port of Catoosa officials said shipping activity is approaching normal levels after Hurricane Katrina pounded New Orleans last year. The hurricane not only lashed New Orleans' harbor −− where most of the Port of Catoosa's inbound goods originate −− but it also increased

energy and barge transportation costs, said Steve Kissee, chairman of the City of Tulsa−Roger County Port Authority. Shipping tonnage totaled 1.8 million tons in 2005, down from 2.2 million tons of cargo in 2004. "As the ports of New Orleans and Baton Rouge make necessary repairs to their infrastructures, shipping is returning to normal. We now have a substantial fleet of barges in our harbor. With new waterway users coming on line, we foresee a much better shipping year in 2006," said Kissee. In December, shipments of inbound steel and pipe, molasses, dry fertilizer and caustic soda were up, the port authority said. Outbound shipments of project cargo, soy products, liquid fertilizer and miscellaneous grain were down, and outbound gypsum and wheat were up.
Source: http://www.logisticsmgmt.com/index.asp?layout=articleXml&xml Id=347359341

15. *January 23, Associated Press* — **Nearing end of bankruptcy, ATA expands service.** ATA Airlines will add service to four cities and increase flights to Hawaii, the first sign of the airline's business plan once it emerges from federal bankruptcy protection in the coming weeks. Monday, January 23's announcement comes after months of gate closures and layoffs and signals a return to the airline's roots as a carrier focused on travel to popular vacation destinations. "With this announcement, we return to one of the core strengths on which ATA was built −− leisure travel −− while growing in a market that has been historically successful for our company," chief executive John Denison said in a statement. Starting in April, the Indianapolis−based carrier will begin flying from Houston's William P. Hobby Airport to New York. The airline will also begin flying from Hilo International Airport in Hawaii, Oakland International Airport and Ontario International Airport, near Los Angeles. ATA, and its parent company ATA Holdings, are expected to emerge from Chapter 11 bankruptcy protection in late February. ATA was founded in 1973, flying charter trips to leisure destinations. After becoming a passenger carrier in the 1980s, the airline grew to be the nation's 10th largest carrier before filing for bankruptcy in October 2004.
Source: http://www.usatoday.com/travel/news/2006−01−23−ata−grows_x.h tm

16. *January 23, Associated Press* — **Serbia−Montenegro train falls into ravine.** A packed passenger train derailed Monday, January 23, and plunged into a steep river canyon in a forest outside the Montenegrin capital, killing at least 10 people and injuring more than 100, police and witnesses said. The train derailed near Bioce, a village about nine miles northeast of Podgorica, shortly after 4 p.m. local time, as it emerged from a tunnel above the Moraca River, police said. Police, medical workers and volunteers were pulling bodies from the 328−foot ravine. At least 106 injured passengers, including 10 children, were taken to the main hospital in Podgorica, said its head, Miodrag Djurovic. He appealed for blood donors. Interior Minister Jusuf Kalomperovic said initial reports indicated the train's brakes may have failed.
Source: http://www.forbes.com/entrepreneurs/feeds/ap/2006/01/23/ap24 69616.html

17. *January 22, USA TODAY* — **Runway reports often unreliable.** An antiquated warning system for the nation's pilots has led dozens of them to receive unreliable information about slippery runways and to land in dangerous conditions, according to a USA TODAY review of accidents and pilot reports during the past decade. In at least 42 cases since 1995, pilots of commercial and corporate aircraft reported skidding off runways after receiving reports that the runways were safe. The reports shed light on the weaknesses of a warning system in which pilots rely on other pilots who have landed recently on slick runways to report conditions on a scale that ranks braking from "good" to "nil." The reports, relayed by air traffic controllers, are subjective,

and the braking abilities of different types of planes vary. Among the issues being investigated are the condition of the runway and the information passed to pilots by controllers, says Keith Holloway, a spokesperson for the National Transportation Safety Board (NTSB). Pilots and investigators have long complained that pilots aren't given enough information about slippery runways, accident records show. The NTSB has issued recommendations for a better system since 1982, when two passengers died at Boston's Logan International Airport when a World Airways DC−10 skidded off the end of an icy runway and broke apart.
Source: http://www.usatoday.com/travel/news/2006−01−22−runway−warnin gs_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *January 23, Indiana Ag Connection* — **Tree−killing beetle found in central Indiana.** The beetle that has killed or damaged millions of ash trees has been found in suburban Indianapolis, IN, far beyond its previously known range. The emerald ash borers (EAB) were found by city tree−trimming crews a couple weeks ago, but an expert said the infestation could be seven years old. Indiana Department of Natural Resources officials on Friday, January 20, ordered restrictions on the movement of ash products in Hamilton County, which includes Carmel, and neighboring Marion County, which includes Indianapolis, in an attempt to slow the beetle's spread. Officials said they did not know how far the beetles might have ranged from the Carmel site, but another possible infestation in neighboring Fishers was being investigated. The beetle was first noticed in Michigan during 2002 and has blanketed most of Lower Michigan and appeared in northern parts of Indiana and Ohio and southern Ontario, Canada. Jodie Ellis, Purdue University's exotic insects education coordinator, said the beetle−infested trees in Carmel had been traced to nursery stock that originated in Michigan. EAB has killed or infested 15 million trees in Michigan, with some 200,000 more trees destroyed in Ohio. More than 100,000 ash trees have been cut and burned in Indiana since April 2004.
EAB information: http://www.emeraldashborer.info/
Source: http://www.indianaagconnection.com/story−state.cfm?Id=43&yr= 2006

19. *January 23, Associated Press* — **Pimlico under quarantine for equine virus.** Pimlico Race Course, in Baltimore, MD, is under quarantine because of an outbreak of the equine herpes virus at the track. Since January 1, 11 horses have shown signs of the virus, prompting the Maryland Department of Agriculture to place an "investigational animal hold order" on three barns. Two horses were euthanized and tested positive for the virus. Equine herpesvirus−1, also known as "rhino," causes upper respiratory infection and can cause neurological disease. There is no reliable method to prevent the neurological form of EHV−1 infection. "This is a precautionary measure," said Lou Raffetto, chief operating officer for the Maryland Jockey Club. "It is in our best interest to restrict the movement in and out of Pimlico until we see the outcome of the tests on the horse in Barn A." A ninth horse in Barn A showed signs of the virus

on Thursday, January 19. Eight horses from Barns 5 and 6 are currently in isolation in the detention barn.
Equine Herpes virus information:
http://www.vet.uga.edu/vpp/IVM/ENG/ERD/EHV−4and1.html
Source: http://www.thewbalchannel.com/news/6359311/detail.html

20. *January 23, Japan Economic Newswire* — **Japan's 22nd mad cow disease case confirmed in Hokkaido.** A five−year and four−month−old cow that died last week on a Hokkaido farm had mad cow disease −− the 22nd case in Japan, the Ministry of Agriculture, Forestry and Fisheries said Monday, January 23. The cow was born in September 2000, before the 2001 implementation of a ban on meat−and−bone meal suspected of being a cause of the disease, formally called bovine spongiform encephalopathy (BSE). The Hokkaido prefectural government will investigate the route of the BSE infection analyzing feeds, the ministry said.
Source: http://www.tmcnet.com/usubmit/−japans−22nd−mad−cow−disease−case−confirmed−hokkaido−/2006/01/23/1306590.htm

21. *January 23, Associated Press* — **Canada reports positive test for mad cow disease.** A cow from an Alberta farm has tested positive for mad cow disease, officials said Monday, January 23. Brian Evans, Canada's chief veterinary officer, said it was found in an animal approximately six years old. Evans said it did not enter the human food or animal−feed systems. Mad cow disease is the common name for bovine spongiform encephalopathy (BSE). The result was a new setback for Canadian ranchers who were hit hard after the U.S. banned cattle imports in May 2003 following the country's first case of mad cow disease. The U.S. border reopened to young Canadian cattle in July 2005. "This case, of course, is unwelcome but it's not unexpected," Evans said, adding the cow's "age and geographic location are consistent with Canada's three previous BSE cases." Canadian beef recently also returned to some supermarket shelves in Tokyo following the lifting of a two−year ban on imports. Japanese officials agreed to allow beef from North America back into the marketplace −− provided it came from animals under 21 months. Entry into Japan is considered key to the long−term recovery plan of Canada's battered beef industry. The scare has cost the industry $5.7 billion.
Source: http://www.chron.com/disp/story.mpl/ap/world/3605914.html

22. *January 22, Charleston Gazette (WV)* — **Computer mapping makes biologists' jobs easier.** As the West Virginia Division of Natural Resources' (DNR) Geographic Information System specialist, Mike Dougherty is helping biologists to know with pinpoint precision where on the state's landscape problems have cropped up and where solutions are needed. "In years past, biologists made management decisions based on a bunch of pins stuck in a topographic map," said Dougherty. "Now, using computers, we can overlay maps with all sorts of information and get a much better picture of what's going on." As an example, Dougherty cited the DNR's ongoing study of chronic wasting disease (CWD). "If that had happened 20 years ago, the teams that went out and shot deer to sample for CWD would have plotted each animal's location on a grid drawn over a county highway map," Dougherty said. "That system required a certain amount of guesswork as to the animals' location. "Now the teams carry Global Positioning System receivers, which record the location of each animal with less−than−a−meter accuracy. We store those locations in a database make computer−generated maps with them. On those maps, we can overlay information we already have −− such as habitat, land use, roads, rivers, and ridges." Recent projects include mapping of the state's wildlife management areas

and catch−and−release trout streams.
Source: http://www.tmcnet.com/usubmit/2006/01/22/1304291.htm

[Return to top]

Food Sector

23. *January 23, Associated Press* — **Japan to inspect all U.S. beef imports.** Japan has ordered inspections of all U.S. beef imported over the past month, calling for a full explanation of a U.S. violation of the countries' beef pact. Japan halted U.S. beef imports last week after inspectors found spinal bone in an American veal shipment, renewing fears of mad cow disease. The halt came only a month after Tokyo partially lifted its two−year−old ban on U.S. beef. Deputy Secretary of State Robert Zoellick called the prohibited bone material an unacceptable mistake and expressed "sincere regret" in a meeting with Agriculture Minister Shoichi Nakagawa on Sunday, January 22. A delegation of U.S. agriculture officials headed to Japan on Monday, January 23. Chief Cabinet Secretary Shinzo Abe said no U.s. beef would be allowed into Japan until Washington explains to Tokyo's satisfaction how the violation happened and what the U.S. will do to prevent a recurrence. Japan banned American beef imports in 2003 after the first detection of mad cow disease in the U.S. herd. Last month Japan resumed imports. Japan was previously the most lucrative overseas market for U.S. beef, buying some $1.4 billion worth in 2003. Japan's decision to halt imports again spurred supermarkets and restaurants to pull American beef from menus and shelves.
Source: http://www.bradenton.com/mld/bradenton/business/13688882.htm

[Return to top]

Water Sector

24. *January 23, Medford News (OR)* — **New software tool to protect drinking water.** Hundreds of thousands of bodies of surface water help supply the U.S. with its drinking water. If a chemical or biological contaminant were accidentally or intentionally introduced into a drinking water source, knowing what threat it posed to the public would be essential. Incident commanders need timely and accurate information to guide their decisions on deploying first responders," said Douglas Ryan, manager of the Pacific Northwest Research Station's Aquatic and Land Interactions Program. "This information often can be drawn from sources that already exist, but they are scattered and usually not quickly available in emergencies." Ryan organized an interagency effort to develop ICWater, an incident command tool designed to help protect drinking water in an emergency. ICWater is a computer−based tool that integrates multiple information sources and data from incident commanders at the scene of a surface water contamination. It produces maps, tables, and charts that tell incident commanders if drinking water intakes are in the contaminant's path, and when and in what concentration the contaminant will reach the intakes. ICWater is currently used by water utilities and state hazardous materials response teams in Oregon and Washington, the National Oceanic and Atmospheric Administration (NOAA), and the U.S. Environmental Protection Agency in the Ohio Valley.
Source: http://www.medfordnews.com/articles/index.cfm?artOID=327090& cp=10996

[Return to top]

Public Health Sector

25. *January 23, Agence France−Presse* — **Woman becomes China's 10th human bird flu case.** China's health ministry has announced the country's 10th human bird flu case, a 29−year−old woman who was in critical condition after contracting the virus. The woman, from Jinhua Town of Chengdu City, is hospitalized in Chengdu, in southwest China's Sichuan province. She showed symptoms of fever and pneumonia on January 12 and was found to be infected with the H5N1 strain of bird flu five days later in tests carried out by the Sichuan provincial center for disease control and prevention. The ministry did not say if there was an outbreak of the disease in poultry where she lived. China has so far reported more than 30 outbreaks of bird flu among animals since the beginning of last year, with most appearing since October 2005.
Source: http://news.yahoo.com/s/afp/20060123/hl_afp/healthfluchina_0 60123155541

26. *January 22, Howard Hughes Medical Institute* — **Malaria parasites develop in lymph nodes.** In the first quantitative, real−time imaging study of the travels of the malaria parasite Plasmodium through mammalian tissue, researchers found the parasites developing in an unexpected place: the lymph nodes. The parasites' presence in the lymph nodes almost certainly has implications for the mammalian immune response, said Robert Ménard, who led the study. “Parasite development in lymph nodes could be one reason there is so much tolerance to these parasites.” When a mosquito infected with Plasmodium bites a mammal, the immature parasites travel to the animal's liver, which, until now, scientists thought was the only place they could develop. Once they have developed, the parasites burst out of the liver cells and infect red blood cells, beginning the onset of malaria. No one had measured directly how many parasites a mosquito bite transmits or where else in a mammal's body they travel, said Ménard. To find out, he and his colleagues infected mosquitoes with fluorescently tagged Plasmodium parasites, and then allowed the mosquitoes to bite a mouse. From each bite, they found an average of 20 parasites in the animal's skin. After leaving the skin, the parasites invaded blood vessels. About 25 percent of the parasites were drained by lymphatic vessels and ended up in lymph nodes.
Source: http://www.hhmi.org/news/menard20060122.html

27. *January 21, Coos Bay World (OR)* — **Hospital finds 46 percent of bacteria cases are resistant.** Methicillin Resistant Staphylococcus aureus (MRSA) is not a reportable disease in Oregon, meaning there is no statewide tracking of the number of cases. But laboratories do track those numbers in house. At Bay Area Hospital in 2004, there were 403 staph aureas cases, with 46 percent antibiotic resistant. That's a jump from seven percent in 1994. For 2005, hospital officials expect the numbers will show closer to half of all cases will have been antibiotic resistant. The Oregon Department of Human Services now is tracking all cases of hospital−acquired MRSA in three counties in the Portland area. In 2004, in that area, there were 27 cases per 100,000 people. In 15 percent of those cases, the patient died. A statewide survey of labs in 1996 found 11 percent of staph aureas cases were antibiotic resistant compared to 39 percent in 2003.
MRSA information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mrsa.htm
Source: http://www.theworldlink.com/articles/2006/01/21/news/news160 12106.txt

28. *January 19, Nature* — **Bird flu virus mutations found in Turkish sample.** Scientists studying virus samples from the human outbreak of the H5N1 strain of avian flu in Turkey have identified three mutations. The first mutation involves a substitution in one sample of an amino acid at position 223 of the haemoagglutinin receptor protein. This protein allows the flu virus to bind to the receptors on the surface of its host's cells. This mutation has been observed in a father and son in Hong Kong in 2003, and in one fatal case in Vietnam last year. It increases the virus's ability to bind to human receptors, and decreases its affinity for poultry receptors. The same sample also contained a mutation at position 153 of the haemoagglutinin protein. Maria Cheng, World Health Organization (WHO) spokesperson, said, "it is not clear what role this particular change plays." Both samples showed a substitution of glutamic acid with lycine, at position 627 of the polymerase protein, which the virus uses to replicate its genetic material. This mutation has been seen in other flu sequences from Eurasian poultry over the past year. It signals adaptation to humans, said Alan Hay, director of a WHO influenza laboratory. "There is this glutamic acid–lysine flip. Glutamic acid is associated with flu−virus replication in birds, and lycine is in primates."
Source: http://www.nature.com/nature/journal/v439/n7074/full/439248a .html

[Return to top]

Government Sector

29. *January 23, Government Accountability Office* — **GAO−06−238: Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs (Report).** Recent data breaches highlight how identity theft may occur when businesses share individuals' personal information, including Social Security Numbers (SSNs), with contractors. Because private sector entities are more likely to share consumers' personal information via contractors, members of Congress raised concerns about the protection of this information in contractual relationships. In response, the Government Accountability Office (GAO) examined (1) how entities within certain industries share SSNs with contractors; (2) the safeguards and notable industry standards in place to ensure the protection of SSNs when shared with contractors; and (3) how federal agencies regulate and monitor the sharing and safeguarding of SSNs between private entities and their contractors. GAO recommends that Congress consider possible options for addressing gaps in federal requirements for safeguarding SSNs shared with contractors. None of the seven agencies GAO talked to provided formal written responses. However, six of the seven agencies provided technical comments, which were incorporated as appropriate.
Highlights: http://www.gao.gov/highlights/d06238high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−238

30. *January 20, GovExec* — **Homeland Security unit to consolidate aviation, marine assets.** In a long−awaited move, which took effect on Tuesday, January 17, the Department of Homeland Security Department's Customs and Border Protection bureau announced that it is consolidating all marine and aviation assets into an organization known as CBP Air and Marine, The new agency will command a force of 651 CBP Air and Marine officers and 500 pilots, and will manage 200 boats and 263 aircraft, said Lucia Ross, a CBP Air and Marine spokesperson. Day to day, Border Patrol sector chiefs will command assets in their area of operations along the northern and southern borders, while directors of air operations will exercise tactical control of

marine assets in Miami, New Orleans and what is known as the Ramey Sector, which includes Puerto Rico and the Virgin Islands. Operational control of marine assets, like that of aviation assets, rests with the CBP commissioner, who ultimately will decide if assets need to be redistributed to better meet the bureau's priorities. Additionally, two new occupational specialties will be established to reflect the diverse working environments within the organization.
Source: http://www.govexec.com/story_page.cfm?articleid=33209&dcn=to daysnews

[Return to top]

Emergency Services Sector

31. *January 23, World Net Daily (OR)* — **Department of Defense to hold second nuclear exercise in South Carolina.** The Department of Defense (DoD) has scheduled a second major, three−day exercise to combat nuclear terrorism in the Charleston, SC−area. The goal is not prevention, but coping with the catastrophic results of a terrorist nuclear attack on a major U.S. port city. The military's Joint Task Force−Civil Support, headquartered at Ft. Monroe, VA, will host the three−day drill for commanders and representatives of other federal agencies that would be involved in managing the consequences of a 10−megaton nuclear blast, enough to inflict mass causalities and devastation on an American city. Like last summer's exercise, Summer Respond '05, the January 31 to February 2 drill is centered around a hypothetical blast that affects nearly half a million people across a 900−square mile section of tidewater South Carolina. The scenario assumes 10,000 fatalities and more than 30,000 injuries. Officials from the Department of Homeland Security, including the Federal Emergency Management Agency and senior Coast Guard brass will be on hand. Though the target of the attack is Charleston, no part of the exercise will actually take place there. Maj. Gen. Bruce Davis, the task force's commander, will oversee the exercise from Fort Monroe.
Source: http://worldnetdaily.com/news/article.asp?ARTICLE_ID=48454

32. *January 22, Daily Times−Call (CO)* — **Communication between Colorado county's emergency groups shaky, but likely to improve, officials say.** When Colorado emergency officials reviewed a June 8 training exercise designed to simulate a chemical weapons attack in Boulder County, CO, they cited a lack of coordination among the 17 participating agencies as the day’s most persistent problem. During this exercise, members of different SWAT teams used incompatible hand motions to signal each other during mock raids, and emergency crews used incorrect terminology when coordinating their maneuvers over police radios. Similar communication problems arose five months later, when a November 10 chemical accident in Gunbarrel sent a toxic cloud into the air. Confusion among emergency crews led to hundreds of nearby residents receiving a series of contradictory warnings by phone, officials determined. Interim county emergency management director Justin Dombrowski is organizing another exercise for April 18 that will simulate a flood in Boulder on the scale of the 1976 Big Thompson Canyon disaster, which killed 145 people. The upcoming flood training will test emergency commanders’ judgment when deciding how to tackle a massive emergency with limited manpower, he said.
Source: http://www.longmontfyi.com/Local−Story.asp?id=5798

33.

January 22, Canton Repository (OH) — **Emergency communications improve in Ohio county.** Stark County is one of the fewer than 20 percent of Ohio counties that now have the technical ability to communicate with all first responders, local health departments and state agencies in the event of a large−scale emergency, such as a tornado or terrorist attack. In December, Stark County Sheriff Tim Swanson made countywide communications a reality by distributing hundreds of portable radios −− linked to the Sheriff Department's 800 MHz trunked radio system −− to all local police, firefighters and paramedics. The problem is that the 800 MHz system cannot be used for daily communications because there aren't enough frequencies to allow every police cruiser, fire truck. or squad car that may be out in the county at one time to communicate. Some contend this leaves many small departments vulnerable. Sheriff's Lt. Gary Shankle acknowledged the radios are not for daily use. "The main thing now is, in [large emergencies], communication capabilities are better by far," he said. "The goal is to make it for day−to−day communications." The sheriff's department and the City of Canton's police and fire departments are discussing combining frequency channels and might take daily communications a step closer to becoming a reality.
Source: http://www.cantonrep.com/index.php?ID=265082&Category=9

34. *January 21, Associated Press* — **New devices allow for direct contact among first responders in Oklahoma.** A $30 million radio system that links city, county and state emergency workers was put in full−time use Monday, January 23. The radios replaced a 20−year−old communication system that required firefighters to contact dispatchers in order to get messages delivered to police. The new system will allow emergency workers direct contact. The system was paid for with funds gathered from a half−cent public safety sales tax that voters approved in 2000.
Source: http://www.channeloklahoma.com/news/6316055/detail.html

35. *January 21, Billings Gazette (MT)* — **Montana police, deputies unite via radio.** When Yellowstone County, MT, Sheriff's Deputy Roger Bodine confronted a robbery suspect, city police officers were only blocks away and converging quickly. Bodine had intercepted the suspect after hearing reports of the robbery and shooting on his police radio, but he could not communicate that to them. The incident highlighted a longstanding flaw in the communication capabilities of the two local law enforcement agencies: Officers and deputies responding to the same emergency could not immediately talk to each other on their radios. For years, radio communication between deputies and police officers in Billings has been delayed because the two agencies use incompatible systems. The Sheriff's Office uses an ultrahigh frequency, or UHF, communication system, while the city uses an 800−megahertz system. As a result, officers and deputies could talk to each other directly only after asking a dispatcher to make the necessary connections at the communications center. The delay was problematic for both agencies, especially in emergencies. On Friday, January 20, leaders of the two agencies announced that the communication hole has been patched with the help of a $40,000 federal grant. The officers' and deputies' individual radios will soon be programmed with the new frequency.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2006/01/21/build/local/55−police−radio.inc

[Return to top]

Information Technology and Telecommunications Sector

36. *January 23, Register (United Kingdom)* — **Trojan blitz poses as credit card warning.** Businesses in the United Kingdom faced a barrage of 115,000 e−mails containing a new Trojan on Friday, January 20, before anti−virus vendors scrambled out an update, according to e−mail filtering firm BlackSpider Technologies. The Trojan downloader malware −− called Agent−ADO −− comes in the payload to a message that poses as a warning about a user's credit card limits being exceeded. BlackSpider detected the malware at 9:10 a.m. GMT Friday, January 20. But it was three−and−a−half hours before the first anti−virus vendor used by BlackSpider issued a patch, once again illustrating the shortcomings of conventional anti−virus scanners in fighting fast−moving virus outbreaks. Infected emails commonly have the subject line "ERROR:YOUR CREDIT CARD OVERDRAFT EXCEED!" and an infected attachment, a packed executable file called FILE1185 which is 5592 bytes long. Analysis of the malware is ongoing. System administrators are encouraged to set up rules to block the malware at the gateway. Virus writers commonly use networks of compromised PCs to seed infection over a short space of time but the ferocity of the latest attack is unusual.
Source: http://www.theregister.co.uk/2006/01/23/trojan_blitz/

37. *January 23, Information Week* — **Cisco security alerts serve as VoIP wake−up call.** Cisco Systems' revelation last week of two security alerts and fixes for CallManager, the processing component of its voice−over−IP (VoIP) technology, reminds us that while VoIP offers all sorts of benefits, there's no getting around its vulnerability as a software application. CallManager's vulnerability to denial of service attacks and attacks that would let users increase their access privileges seem mild compared with threats aimed at stealing customer data or blocking Website access. But as more voice communication travels over the Internet, reducing that threat becomes increasingly important. Cisco CallManager extends business telephony functions to IP phones, media−processing devices, VoIP network gateways, and multimedia applications. The denial of service and privilege−escalation vulnerabilities, for which patches are available, affect CallManager 3.2 and earlier, and some versions of CallManager 3.3, 4.0, and 4.1. Like Microsoft in the software market, Cisco is likely to be the main target of VoIP hackers because of its market−share leadership. Another danger lies in IT staff inexperience: VoIP hasn't been much of a target for hackers, and gaining the security know−how to protect those networks may not be top of mind during deployments, says Ofir Arkin, chief technology officer of network−management company Insightix Ltd.
Source: http://www.informationweek.com/security/showArticle.jhtml?ar ticleID=177102457

38. *January 23, Business Week Online* — **Targeted Trojans on the rise.** It was a stealth cyberattack: Last November 18, an e−mail with a nefarious purpose was dispatched from an Internet address in the Tianjin province of China. The targets: individual employees of the U.S. and European military and pharmaceutical, petrochemical, and legal companies, according to e−mail security firm MessageLabs. Attached was an apparently innocuous Microsoft Word document with a news story from CNN. And it was designed to look like it came from a trustworthy source. In this case, the Trojan was a particularly insidious variety known as a targeted Trojan because it was directed at a specific recipient −− intended to infect the computer networks of American companies. When opened, the Word document could have become a ticking time bomb. Buried inside was special code that would allow hackers to take remote control of each employee's PC. Then, working from inside the corporate networks, the

hackers could steal corporate secrets or use the compromised computers to send spam and viruses. According to computer−security experts, spam, phishing e−mails, viruses, and worms will grow more slick and secretive in 2006.
Source: http://www.businessweek.com/technology/content/jan2006/tc200 60123_003410.htm

39. *January 23, CNET News* — **British parliament attacked using WMF exploit.** The British Parliament was attacked late last year by hackers who tried to exploit a recent serious Microsoft Windows flaw, security experts confirmed on Friday, January 20. MessageLabs, the e−mail−filtering provider for the UK government, said that targeted e−mails were sent to various individuals within government departments in an attempt to take control of their computers. The e−mails harbored an exploit for the Windows Meta File (WMF) vulnerability. The attack occurred over the Christmas period and came from China, said Mark Toshack, manager of antivirus operations at MessageLabs, who added that the e−mails were intercepted before they reached the government's systems. The vulnerability with the way that WMF images are handled by Windows was discovered in November 2005. In a WMF attack, exploit code is hidden within a seemingly normal image that can be spread via e−mail or instant messages. The attack was individually tailored and sent to 70 people in the government, MessageLabs said. It played on people's natural curiosity by purporting to come from a government security organization. The Trojan was hidden as an attachment called "map.wmf".
Source: http://news.com.com/British+parliament+attacked+using+WMF+ex ploit/2100−7349_3−6029691.html?part=rss&tag=6029691&subj=new s

40. *January 20, Secunia* — **HP−UX ftpd denial of service vulnerability.** A vulnerability has been reported in HP−UX, which can be exploited by malicious people to cause a denial of service. The vulnerability is caused due to an unspecified error in ftpd. This can be exploited to cause the daemon to become unresponsive.
Solution: Apply updates.
http://itrc.hp.com
http://www.hp.com/go/softwaredepot
HP−UX B.11.23 (InternetSrvcs): Install PHNE_33414 or later.
HP−UX B.11.11 (InternetSrvcs): Install PHNE_33412 or later.
HP−UX B.11.04 (InternetSrvcs): Install PHNE_34077 or later.
HP−UX B.11.00 (InternetSrvcs): Install PHNE_33406 or later.
HP−UX B.11.11 (WUFTP−26): Install WUFTP−26 revision B.11.11.01.006 or later.
HP−UX B.11.00 (WUFTP−26): Install WUFTP−26 revision B.11.00.01.005 or later.
Source: http://secunia.com/advisories/18543/

41. *January 20, Tech Web* — **New worm corrupts Microsoft documents.** A new worm that already accounts for one in every 15 pieces of malicious code carries a "nuclear option" payload that corrupts data in a slew of popular file formats, a security company warned Friday, January 20. The Nyxem.e worm, said Finnish security firm F−Secure, carries code that instructs it to replace data in files with .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, or .dmp extensions with the useless string "DATA Error [47 0F 94 93 F4 K5]" on the third of the month. This list includes the native document formats for Microsoft Word, Excel, PowerPoint, and Access, as well as for Adobe PhotoShop and Acrobat. Nyxem.e is similar to the VB.bi/Blackmal/MyWife.d worm that climbed the charts earlier last week, added F−Secure. The worm arrives as an attachment to e−mail messages with a variety of subject headlines,

many of which tout porn with phrases. It also tries to delete selected security software, and can spread through shared folders as well as by hijacking addresses from infected PCs.
Source: http://www.techweb.com/showArticle.jhtml?articleID=177102371

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. Successful exploitation may allow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system with root or SYSTEM privileges. More information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Restrict access to the ports used by the NetBackup services.

Malicious Website Exploiting Sun Java Plug−in Vulnerability US−CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine. More information about these vulnerabilities can be found in the following URL:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages:
http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 25 (smtp), 49200 (−−−), 41170 (−−−), 80 (www), 55556 (−−−), 65535 (Adoreworm) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *January 23, Reuters* — **Italy on guard but no evidence of Olympic threat.** Italy sees no firm evidence of a security threat to the Winter Olympics in Turin, but is alert to possible attacks by local and foreign militant groups, Interior Minister Giuseppe Pisanu said on Monday, January 23. Italy is gearing up to national elections in April, and the Games will run from February 10−26. Pisanu added that Italy had so far spent US$110 million on security measures for the event, including the cost of some 9,000 additional policemen and other security staff, and expected the final bill to be higher. The minister said he was alert to local anti−train protesters, who could cause trouble during the Games. Environmental activists and residents of the Val di Susa valley, which connects the Olympic mountain venues, have demonstrated against a planned high−speed rail link between Italy and France that would cut through their valley. Italy has says it can deal with Olympic security alone, and has rejected an offer from NATO to provide troops. But Pisanu said NATO would supply one aircraft to help patrol the no−fly zone over the Olympic sites, which stretch from Turin to the French border.
Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=sportsNews&storyID=2006−01−23T185032Z_01_L2344354_RTRIDST_0_SPORTS−OLYMPICS−COL.XML&archived=False

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

Department of Homeland Security Disclaimer