Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 04 November 2003

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Daily Herald reports that a break−in at the Carpentersville, IL, water treatment facility forced crews to test water supplies and disinfect the entire filtration system. (See item 12)
- The United Press International reports that as the UK braces for an impending measles outbreak, health experts say this raises concerns the disease could spread to the U.S. (See item 14)
- vnunet.com reports antivirus firms have warned of a destructive worm that has just emerged: the W32/Mimail.c@MM, also known as Mimail.c, is a dangerous worm that bears similarities to W32MiMail@MM. (See item 20)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; 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 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. *November 03, Associated Press* — **Alleged high voltage tower saboteur arrested. A man sought by the FBI for allegedly loosening bolts on a high voltage power line tower in Northern California was arrested Sunday, November 2, when he walked into a California Highway Patrol office looking for directions. Michael Devyln Poulin said his action was intended to highlight domestic insecurity,** and that he had been trying to surrender. A federal arrest warrant issued last month charges Poulin with damaging an energy facility. Poulin is

accused of removing and loosening bolts from the legs of a high voltage transmission tower near Anderson, CA, on October 20. Bolts also have been loosened or removed from the legs of other transmission towers near Sacramento, CA, Benton City, WA, and the Oregon cities of Madras, McNary, Klamath Falls and The Dalles.
Source: http://www.cbsnews.com/stories/2003/10/17/attack/main578657. shtml

2. *November 03, Traverse City Record−Eagle (MI)* — **Drum from Big Rock will travel to Utah. Deconstruction of the Big Rock Point Nuclear Power Plant, located in Charlevoix, MI, is slated to continue this week with the shipment of a 200,000−pound steam drum to a disposal location in Utah. Shipment of the drum is scheduled to begin Tuesday, November 4,** but could be rescheduled in the case of bad weather, said Tim Petrosky, a spokesperson for Consumers Energy, owner of the plant. A heavy haul trailer will move the drum by road to Petoskey where it will be taken by rail to a disposal facility in Clive, UT. The rail portion of the trip is expected to take approximately 10 days, Petrosky said. **The drum, which Petrosky said is classified as low−level radioactive waste, is almost 41 feet long and has a maximum outside diameter of 10 feet. It weighs approximately 200,000 pounds.** It was used to remove moisture from steam during plant operation. Big Rock Point's reactor vessel was shipped in a similar manner last month to a disposal site in Barnwell, SC.
Source: http://www.record−eagle.com/2003/nov/03bigroc.htm

3. *November 03, Wpxi.com (PA)* — **Power plant fire forces evacuation. Several emergency crews were called to the scene of a fire at the Hatfield's Ferry Power Station in Greene County, PA.** The blaze began around 10:30 a.m. Monday, November 3. Officials describe blaze as a coal fire on sixth floor of the building. The power plant was evacuated and there have been no reports of injuries. **It is not yet known what caused the fire nor the extent of the damage.**
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=21205

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *October 31, Government Accounting Office* — **Report−GAO−04−48: Defense Acquisitions: Despite Restructuring, SBIRS High Program Remains at Risk of Cost and Schedule Overruns. In 1996, the Department of Defense (DoD) initiated the Space−Based Infrared System (SBIRS) to provide greater long−range ballistic missile detection capabilities than its current system.** The initial SBIRS architecture included "High" and "Low" orbiting space−based components and ground processing segments. **SBIRS has been technically challenging, and in October 2001, SBIRS Low was transferred from the Air Force to the Missile Defense Agency. The Air Force expected to field SBIRS High by 2004, but numerous problems have led to schedule overruns.** In the fall of 2001, DoD identified

potential cost growth of $2 billion. GAO's report (1) describes the key elements of the restructured program and (2) identifies problems and potential risks still facing the program. **GAO recommended that DoD convene a task force to assess the restructured program with an emphasis on providing concrete guidance for the program to address its underlying problems.** DoD agreed that another review of the program is warranted. Report: http://www.gao.gov/cgi−bin/getrpt?GAO−04−48
Source: http://www.gao.gov/highlights/d0448high.pdf

[Return to top]

Banking and Finance Sector

5. *November 03, ZDNet Australia* — **Scammers target Westpac customers.** The e−mail is the latest in a growing trend of phishing expeditions, where fraudsters attempt to trick users out of confidential bank account details. **A New Zealand version of the e−mail targeting Westpac customers in that country has now appeared.** The latest e−mail has another level of sophistication over previous scams. **The link included in the e−mail appears to go to a Westpac page −− although the gibberish included in the URL is an indicator it is fake −− but uses the technique of including an "@" symbol to take the user to a site hosted in Russia.** The Russian Website then opens a pop−up window requesting the users' details, and redirects itself to the legitimate Westpac bank's privacy policy page. If the customer is not paying attention, or inexperienced with the Internet, they may be fooled into thinking the pop−up was produced by Westpac.
Source: http://www.zdnet.com.au/newstech/security/story/0,2000048600 ,20280458,00.htm

[Return to top]

Transportation Sector

6. *November 03, Government Technology* — **Tanker truck shut down wirelessly in test.** California Assembly Bill 575 would require a position−locating reporting system to be installed in any truck carrying hazardous materials, and a device to enable immediate disabling of the vehicle. **Recently, a remote disabling device was tested by the California Highway Patrol (CHP), InterState Oil Company and Satellite Security Systems (S3). From S3's headquarters in San Diego −− 530 miles from the demonstration site −− satellite communications were used to disable the truck.** The event, conducted on CHP Academy grounds in Sacramento and administered by the CHP, addresses ongoing concerns about the affordability of effective security technology, stealthiness of such a security device, and how locational monitoring can be incorporated safely into law enforcement protocol. **The need to secure trucks carrying hazardous waste or petrochemical products is of paramount concern to trucking companies, California Independent Oil Marketing Association (CIOMA) members, and state and federal departments.**
Source: http://www.govtech.net/news/news.php?id=2003.11.03−75762

7. *November 03, Associated Press* — **Sky Harbor, other airports short on screeners.** Arizona's Phoenix Sky Harbor International Airport is about 13 percent short of the number of security

personnel mandated by Congress to monitor passengers at checkpoints and examine baggage before it's loaded onto planes. **According to the Transportation Security Administration (TSA), the airport is one of 89 airports nationwide that is understaffed by at least 120 screeners.** Suzanne Luber, regional spokesperson for the security administration, said a high turnover rate and a complex hiring process have contributed to the shortages. Sky Harbor has lost 130 of its 1,026 TSA screeners since June. **The shortage has raised the specter of longer checkpoint lines just weeks before the busiest season of the year. The shortage also comes amid security concerns after a Baltimore college student sneaked box cutters and other illegal objects past security screeners and aboard two passenger jets.** The shortage has had minimal effect on airport operations, Luber said, and passenger−waiting times in screening lines have been kept down to an average of 10 minutes, which is the agency's national goal.
Source: http://www.azdailysun.com/non_sec/nav_includes/story.cfm?sto ryID=76163

8. *October 31, Government Executive Magazine* — **TSA may use private security workers for late shift.** The Transportation Security Administration (TSA) plans to replace some federal passenger and baggage screeners with private security forces at New York's LaGuardia Airport starting November 1. **But federal screeners oppose the move, claiming TSA is trying to do an end−run around federal law and is putting airport security at risk.** Federal screeners at LaGuardia, who are hired and managed by TSA, were notified about a week ago that they will no longer work the late shift from 11 p.m. to 4 a.m., said Miguel Shamah, acting vice president of the Metropolitan Airport Workers Association, a group organized to represent the interests of airport workers. Instead, LaGuardia plans to use private security contractors to work the late shift, Shamah said. TSA spokesman Darrin Kayser said private security forces at LaGuardia are being hired only to patrol the airport terminals and watch exit areas, and will not conduct passenger and baggage screening. **After the September 11 terrorist attacks, Congress mandated that only a federal workforce of screeners trained by TSA could conduct passenger and baggage screening at the nation's airports.**
Source: http://www.govexec.com/dailyfed/1003/103103c1.htm

[Return to top]

Postal and Shipping Sector

9. *November 02, Associated Press* — **Clemson shuts post office after substance found. A Clemson, SC, postal facility was shutdown for about 30 minutes Saturday when an unknown white powder was discovered.** Clemson Police Chief Jimmy Dixon said authorities did not yet know what the powder was. "There was a letter that came through that had white powder in it," he said. "It looked like white baby powder." The State Law Enforcement Division, the FBI, and postal authorities were called, Dixon said. **Dixon said he collected the Clemson sample himself and had his department enact its "terrorism" mode to contain the substance. The substance was taken to the FBI, which is expected to perform tests. It was unclear how long it will take before the results are known.**
Source: http://www.thestate.com/mld/thestate/news/local/7166718.htm

[Return to top]

Agriculture Sector

10. *November 03, Associated Press* — **Sales of cloned cattle multiply. Cattle are quietly being cloned and sold for high prices as the livestock industry anticipates government approval for letting their offspring into the food chain.** The Food and Drug Administration (FDA) is still trying to decide if cloned farm animals will require government approval before being sold as food. That decision is expected to take another year. There already are as many as 300 cloned bulls in existence, said Lisa Dryer of Biotechnology Industry Organization, a Washington lobbying group. And a Texas−based biotech firm, ViaGen, said Friday that a cow cloned from a prodigious producing animal was auctioned for $170,000 in Missouri. **ViaGen President Scott Davis said "thousands and thousands" of units of frozen semen from hundreds of cloned bulls are being stockpiled around the country, ready for sale to cattle breeders when the FDA issues its new guidelines.** Some members of Texas' cattle circles have reservations about whether cloning is commercially practical. The cost of a cloned calf currently is estimated at $19,000, and some cloned animals develop health problems.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/business/2198080

11. *November 01, Agriculture Online* — **Trace−back system plan. State animal health officials, livestock industry groups, and the federal government are working together to finalize a U.S. Animal Identification Plan (USAIP), with a goal of creating a trace−back system that can identify all animals and premises potentially exposed to an animal with a foreign animal disease within 48 hours.** The 48−hour trace−back goal requires records of an animal's origin and movement to other locations for its entire life. **Current goals are to start implementing the plan with identification of livestock premises next summer, and have individual identification for cattle in commerce as well as other food animals and livestock in commerce identified by July 2006.** The plan, currently includes all domestic cattle, bison, swine, sheep, goats, deer and elk, horses, poultry, game birds, aquaculture, and other animals, whether they are intended for breeding stock, consumption, or personal use. Reasons for wanting to introduce a trace−back system include enhancing disease control and eradication capabilities and enhanced ability to respond to bio−security threats. **It also would help the industry meet consumer demands for source−verified products, and mitigate threats to the bio−security of the food supply.**
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=topStoryDetail__ANewsindex_html___50811___1

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

12. *November 03, Daily Herald (Chicago)* — **Water plant break−in.** A break−in at the Carpentersville, IL, water treatment facility forced crews to test water supplies and disinfect the

entire filtration system. **Public works and police officials say the culprits were two children under the age of 15. The duo sprayed fire extinguishers and created some "general mischief," police chief Bob Lowen said. There wasn't any reason to think they'd contaminated the water supply, he said.** An operator doing an inspection of the plant noticed the children shortly before 7 a.m. Sunday. **The treatment facility's filtration room is the only room in the plant that would allow contamination of the public drinking water supply, but Public Works Director Bob Cole said no water was being produced at the time and, consequently, the filters were empty.** As a precaution, crews on Sunday made certain any water running through the system was bypassing the filters. They planned to do tests of the water supplies Monday. In addition, the filters will be cleaned and disinfected, likely coming back online Tuesday or Wednesday. **In the aftermath of the September 11 attacks, the facility began using a key−card system to beef up security at its primary doors, but the door the kids apparently used to gain access had only a normal lock.**
Source: http://www.dailyherald.com/search/main_story.asp?intID=37928 112

[Return to top]

Public Health Sector

13. *November 03, Guardian* — **Spain shuts border to virus infected ship. The arrival of a British cruise ship hit by a contagious stomach infection in Gibraltar Monday provoked a diplomatic row as Spain closed its border with the territory.** Spain said the closure was a provisional measure aimed at protecting its citizens. **The Aurora left Greek waters on Friday without landing after more than 430 passengers fell ill with norovirus, which causes sickness and diarrhea.** It arrived Monday morning as scheduled in Gibraltar after a weekend of discussions between the British and Spanish governments. The border between Spain and Gibraltar has been open since 1985. The most recent shutdown had left more than 500 Spanish employees of Gibraltarian businesses stuck at the border. Peter Caruana, Gibraltar's chief minister, said the decision to close the border was a "flagrant interference" with EU citizens' rights to freedom of movement. **Spain's health ministry said the measure was precautionary and would remain in effect until there was more information about the condition of the infected passengers.**
Source: http://www.guardian.co.uk/gibraltar/story/0,11525,1076791,00 .html

14. *October 31, United Press International* — **UK measles outbreaks pose risk to U.S. As the UK braces for an impending measles outbreak, health experts say this raises concerns the disease could spread to the U.S., particularly considering immunization rates in some states have fallen to dangerously low levels. The drop in measles vaccinations also heightens fears of outbreaks of two other diseases: rubella and mumps.** This is because the measles vaccine generally is administered in conjunction with mumps and rubella inoculations in a single shot. **Of the three diseases, measles carries the most concern because it is a highly contagious disease with a death rate of one or two children for every 1,000 infected.** Health officials are also worried about the ongoing outbreak in the Marshall Islands and recent epidemics in Asia and Italy. **Health officials think a vaccine coverage rate of about 95 percent is necessary to prevent outbreaks and anything below 90 could allow outbreaks to flourish.** In the U.S., vaccine coverage is about 91.6 percent.
Source: http://www.upi.com/view.cfm?StoryID=20031031−044151−8440r

[Return to top]

Government Sector

15. *November 03, Federal Computer Week* — **US−VISIT team works even before launch.** With all eyes on the massive border entry/exit system, Homeland Security Department officials are developing an equally robust plan to manage the process. **Officials are working to build a strong management structure even before the first pieces of the U.S. Visitor and Immigrant Status Indicator Technology (US−VISIT) system are released.** "What we need to do to be ready is to leverage what we have today and build up the talent so we have that management capability," said US− VISIT Director Jim Williams. **Last summer, DHS Secretary Tom Ridge approved the structure for a program management office with a staff of 115. Williams said he is in the process of staffing the office, which will be supported by 177 contractors.** By December 31, officials expect to have US−VISIT in place at all seaports and airports, with the use of biometrics.
Source: http://www.fcw.com/fcw/articles/2003/1103/mgt−usvisit−11−03− 03.asp

16. *November 03, PRNewswire* — **Deepwater Team delivers communications system upgrade to U.S. Coast Guard.** The Coast Guard Cutter Northland is at sea with the first phase of communications systems upgrades for 270−foot medium endurance cutters as part of the Integrated Deepwater System (IDS). Northland is the first cutter to receive this upgrade, which immediately provides improved performance within existing communications systems and allows additional access to a variety of intelligence and data sources, previously unavailable to these cutters. **Among its enhanced capabilities, Northland will have access to classified and unclassified data communications through international maritime Satellite B services connectivity to the U.S. Department of Defense's Secret Internet Protocol Network (SIPRNET). Additional future enhancements include doubling the data bandwidth and improving variable bandwidth efficiency, improvements that will enable cutters to exchange and process information more rapidly.** The Northland's initial upgrade was accomplished through the joint efforts of the Integrated Coast Guard Systems (ICGS) team, the United States Coast Guard (USCG) and the crew of CGC Northland. It is the first in a series of enhancements planned for 270−foot cutters under the Coast Guard's Deepwater modernization program.
Source: http://biz.yahoo.com/prnews/031103/phm013_1.html

[Return to top]

Emergency Services Sector

17. *November 03, Department of Homeland Security* — **Mass casualty exercise to take place in Erie.** More than 250 responders from 50 different federal, state and local agencies will test Lake Erie, PA, contingency plans in a two−day mass casualty and pollution exercise beginning November 5 at the Erie Port Authority Cruise Ship Visitors Terminal. **The exercise, centered around a simulated collision between a cruise ship and an ore carrier, is designed to focus on a broad range of themes including search and rescue, emergency medical care,**

immigration, law enforcement and environmental response. Participants will run through actual drills such as medical triage, helicopter rescue operations and deployment of pollution equipment, as if the exercise was an actual event. Exercise coordinators will monitor operational and planning methods along with logistics, finance and multi−agency coordination. Agencies will also test new technology and procedures such as the Coast Guard's new On Water Recovery System for mass rescue and Side Looking Rader (SLAR) for pollution detection.
Source: http://piersystem.com/external/index.cfm?cid=443&fuseaction=EXTERNAL.docview&pressID=24269

18. *November 01, Associated Press* — **Britain stages anti−terror exercise drill. The British army joined emergency services Saturday, November 1, in responding to a simulated terrorist attack on a chemical tanker truck, said to be one of the largest anti−terrorist preparedness exercises ever conducted in the country.** The army said about 800 soldiers, firefighters, police officers and paramedics participated in the drill, which simulated the explosion of a chemical−carrying tanker at an airfield near Abingdon, about 95 miles west of London. **The army said it was an unprecedented exercise in terms of the scale and the numbers involved.** About 200 soldiers established a center to cope with a large−scale evacuation, while 150 firefighters and paramedics sealed off the area and began decontaminating 400 soldiers and cadets posing as civilian casualties. Police also were involved.
Source: http://www.washingtonpost.com/wp−dyn/articles/A50902−2003Nov 1.html

[Return to top]

Information and Telecommunications Sector

19. *November 03, Federal Computer Week* — **NIST releases security controls proposal. The National Institute for Standards and Technology (NIST) released the first draft of a publication describing mandated security controls for federal information systems on Monday, November 3.** NIST officials want agencies to experiment with the initial public draft, "Special Publication 800−53: Recommended Security Controls for Federal Information Systems." **It outlines electronic and physical controls for systems categorized under three levels of potential impacts, such as what would happen if someone steals information from a federal system and modifies the data or disrupts a government service.** NIST's Computer Security Division plans to use agencies' comments from the initial draft and an open workshop in March to develop final security controls that would become the new "FIPS 200: Minimum Security Controls for Federal Information Systems." FIPS 200 is required under the Federal Information Security Management Act of 2002. NIST expects to publish FIPS 200 in the fall of 2005, when its controls will become mandatory for all federal agencies.
Source: http://www.fcw.com/fcw/articles/2003/1103/web−nist−11−03−03. asp

20. *November 03, vnunet.com* — **Destructive MiMail variant hits Web. Antivirus firms have warned of a destructive worm that has just emerged in the wild. The W32/Mimail.c@MM, also known as Mimail.c, is a dangerous worm that bears similarities to W32MiMail@MM. Mimail.c contains its own SMTP engine for constructing messages, and mails itself as a zip or upx attachment. After being executed, Mimail.c e−mails itself**

out as an attachment with the filename 'Photos.zip'. Target e−mail addresses are harvested from the victim's machine and are written to the file eml.tmp in WinDir. Users should immediately delete any email containing the following 1) Subject: Re[2]: our private photos [plus additional spaces then random characters] 2) Attachment: 'photos.zip' (12,958 bytes) which contains 'photos.jpg.exe' (12,832 bytes). Also, in a bid to make the virus e−mails less conspicuous, the 'From' address of infected outgoing messages may be spoofed with james@(target domain.com) − for example, james@abc.com.
Source: http://www.vnunet.com/News/1146971

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 1433 (ms−sql−s), 80 (www), 17300 (Kuang2TheVirus), 139 (netbios−ssn), 4662 (eDonkey2000), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

21. *November 03, Los Angeles Times* — **Firefighters expect to contain largest California fire.** The region's cool, moist weather Monday dulled the wildfires that have raged in five California counties over the last week, and firefighters expect to contain the largest and deadliest fire by Monday night. **The Cedar fire, which devoured 280,293 acres and killed 15 people in San Diego County, should be contained by 6 p.m. Monday and under full control by November 16, said Cathy Fritz, of the California Department of Forestry.** The California Department of Forestry revised its estimate today of when the 56,700−acre Paradise fire, one of the two fires that ravaged San Diego County, will be contained, saying that should happen Saturday. **An evacuation order remained in effect Monday for much of the area around Lake Arrowhead and Crestline.**
Source: http://www.latimes.com/news/local/la−110303fire_lat,1,2888066.story?coll=la−headlines−california−manual

22.

November 03, Associated Press — **Brick is thrown at House office building. U.S. Capitol Police arrested a man Monday, November 3, after he threw a brick that broke a window at a House office building,** less than a week after a gun scare at the same building briefly closed the House of Representatives, police said. The man was shouting and appeared to be protesting something, "but we're not sure what it was," said Capitol Police spokesperson Jessica Gissubel. She did not immediately release the man's name. She said **the man, wearing a business suit, threw the brick twice, breaking the window of an entrance door to the Cannon Office Building on the second attempt. Four officers immediately detained him,** Gissubel said.
Source: http://www.guardian.co.uk/uslatest/story/0,1282,−3343752,00. html

23. *November 01, The Aberdeen American News (SD)* — **Terrorism tip line established. South Dakota's U.S. Attorney's Office and the state's Joint Terrorism Task Force have established a toll−free tip line to report suspicious activity that may be related to terrorism.** The number is 1−877−GUARD SD (1−877−482−7373). It can be used by people in South Dakota and surrounding areas. It is not manned at all hours and is not intended for emergency use. South Dakota's Joint Terrorism Task Force is made up of investigators from the FBI, state Department of Criminal Investigation, Minnehaha County Sheriff's Office and Sioux Falls Police Department. Other agencies contribute to the task force on a part−time basis.
Source: http://www.aberdeennews.com/mld/aberdeennews/contact_us/

24. *October 31, United States Department of State* — **Travel Warning: Somalia.** The U.S. Department of State has issued a travel warning to remind Americans of continued concerns about the security situation in Somalia. **The Department of State warns U.S. citizens against all travel to Somalia, including the self proclaimed "independent Republic of Somaliland."** Inter−clan and inter−factional fighting can flare up with little warning, and kidnapping, murder, and other threats to U.S. citizens and other foreigners can occur unpredictably in many regions. Recent attacks against foreigners in the self−declared "Republic of Somaliland" in northern Somalia have occurred, and the Sanaag and Sool Regions in eastern Somaliland, bordering on Puntland (northeastern Somalia), are subject to insecurity due to potential inter−clan fighting. **U.S. citizens are urged to use caution when sailing near the coast of Somalia. Merchant vessels, fishing boats and pleasure craft alike risk seizure and their crews being held for ransom, especially in the waters near the Horn of Africa and the Kenyan border.** There is no U.S. Embassy or other diplomatic presence in Somalia to provide up−to−date security assessments.
Source: http://travel.state.gov/somalia_warning.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−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

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:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

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. This 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.