

**Department of Homeland Security  
Information Analysis and Infrastructure  
Protection  
Daily Open Source Infrastructure Report  
for 06 June 2003**

Current Nationwide  
Threat Level is



[For info click here](#)

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

**Daily Overview**

- The Daily Press reports a congressional panel warned that efforts to tighten security at the nation's ports could be jeopardized by a lack of federal money and a Coast Guard that is stretched too thin. (See item [5](#))
- Reuters reports that Bugbear.B, a variant of the Bugbear worm which spread around the Internet last October, has started to infect users around the world, putting them at risk of losing confidential information. (See item [14](#))
- The Associated Press reports a man in prison for vehicle theft is suspected of planning a significant attack, possibly in Los Angeles, say authorities who uncovered an arsenal of semiautomatic assault weapons, ammunition, pipe bombs and barrels of jet fuel. (See item [19](#))
- Internet Security Systems has raised AlertCon to Level 2 due to the rapid spreading of the Bugbear virus variant. Please refer to the Internet Alert Dashboard.
- SecurityFocus has raised ThreatCon to Level 2, increased alertness. This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring and requires increased vigilance, such as a careful examination of vulnerable and exposed systems and increased monitoring of logs. Please refer to the Internet Alert Dashboard.

**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. *June 04, Platts Global Energy News* — **Russia to suspend fuel shipments to Iran. Russia will suspend shipment of fresh fuel to Iran's Bushehr reactor until Iran accepts the IAEA's Additional Protocol**, U.S. Under Secretary of State for Arms Control & International Security John Bolton said Wednesday. Testifying at a hearing of the House International Relations Committee, Bolton cited and confirmed a statement earlier in the day by British Prime Minister Tony Blair. After the hearing, Bolton said the Russian commitment would not affect that country's work on the construction of the reactor, which is ongoing. **Russia is to supply fresh fuel and take back spent fuel from Bushehr, in part to ease international concerns about Iran's nuclear program.** Under the Additional Protocol, the IAEA would have expanded inspection authority in Iran.  
Source: <http://www.platts.com/stories/nuclear1.html>
2. *June 03, Chattanooga Times/Free Press* — **Tennessee Valley Authority makes business case for restarting nuclear reactor. Falling interest rates and rising natural gas prices have strengthened the case for restarting the Tennessee Valley Authority's oldest nuclear reactor**, according to agency directors. "The business case for the recovery of Unit 1 at Browns Ferry makes even better sense today than it did when the board made its decision a year ago," TVA Chairman Glenn McCullough said last week. "We're ahead of schedule and under budget at Browns Ferry." Market changes in the past year also have weakened the need to use outside financing to pay for the \$1.8 billion project, according to the directors. **Repairing and reactivating the oldest reactor at the nuclear plant should pay for itself in only seven years, they said. But critics of the nuclear plant recovery remain unconvinced.** Keith Ashdown, vice president of policy for the Washington, D.C.-based Taxpayers for Common Sense, said the history of nuclear plants is that they cost more to build and repair than budgeted and don't always run as well as intended. TVA, which already has more than \$25 billion in debt, is having to borrow money to repair the Browns Ferry unit by 2007. But TVA officials insist the relatively low cost of operating another unit at Browns Ferry will make that cheaper than buying other power or building gas-fired plants.  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3891429](http://www.energycentral.com/sections/news/nw_article.cfm?id=3891429)
3. *June 03, Daily News Bulletin, Moscow* — **Emergency shutdown at Ukraine nuclear plant unit. There has been an emergency shutdown at the first power unit of the Rivne nuclear power station in Ukraine. The Emergencies Ministry reports that a vapor alarm went off at the station at 8:30 p.m. on Monday. During an inspection, a pipeline was discovered to be leaking steam.** An emergency shutdown of the power unit was requested for the period from 10:45 p.m. on June 2 to midnight June 5 in order to find and fix the defect. The second and third power units are operating at nominal capacity. Ten of the 13 power units at Ukraine's nuclear stations are currently in operation. Repairs are also under way on the first unit in Zaporizhzhya and the second unit at the South Ukrainian station.  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3892050](http://www.energycentral.com/sections/news/nw_article.cfm?id=3892050)

[[Return to top](#)]

## Chemical Sector

Nothing to report.

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

## **Defense Industrial Base Sector**

4. *June 04, General Accounting Office* — **Missile defense: knowledge-based practices; GAO-03-441.** The General Accounting Office (GAO) was asked to review the Missile Defense Agency's (MDA) strategy for this investment and determine what knowledge-based practices characteristic of successful programs are being adopted by MDA; what significant practices are not being adopted; and whether MDA is following the practices that it has adopted. The GAO found that MDA has not adopted some knowledge-based practices regarding long-term investment decision-making and, as a result, the missile defense program's success could be hampered. **First, MDA is not making an early determination of the full cost of a capability. Such an estimate would help decision makers more effectively evaluate which technologies to include because they offer the best capability for the funds invested. Second, DoD is not allocating a "wedge" of funds in its Future Years Defense Plan for system production and operations. Without this wedge, DoD may not have the funds needed to procure and maintain the missile defense system.** The GAO is recommending that DoD prepare life cycle cost estimates for missile defense elements before beginning integration activities and explore the option of setting aside funds to produce and operate the missile defense system over the long term.  
Source: <http://www.gao.gov/highlights/d03441high.pdf>

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

## **Banking and Finance Sector**

Nothing to report.

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

## **Transportation Sector**

5. *June 04, Daily Press (Washington, DC)* — **Lack of money may jeopardize port security. Efforts to tighten security at the nation's ports could be jeopardized by a lack of federal money and a Coast Guard that is stretched thin,** a congressional panel warned Tuesday. Seven months after Congress passed the Maritime Transportation Security Act – authorizing more manpower, equipment and planning at major ports – there still is no funding to implement it. **And in a move that upset members of Congress, the Transportation Security Administration has asked to use \$105 million that had been allocated for port security grants to cover cost overruns in aviation security.** The funding troubles are the latest wrinkle in a congressional struggle to enhance port security since the terrorist attacks of September 11, 2001. **Less than two percent of all cargo containers that enter the country each year are inspected by customs or law enforcement officials. Many fear there is no way to inspect a majority of the cargo without a major disruption in trade and severe economic losses.** The first step toward addressing the problem came last fall, with passage of the security act. The

legislation includes new requirements for vulnerability assessments and security plans to be drafted for 55 major ports.

Source: <http://www.dailypress.com/business/local/dp-18022sy0jun04.0.3097314.story?coll=dp-business-localheads>

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

## **Postal and Shipping Sector**

- 6. *June 03, U.S. Customs and Border Protection* — Britain implements U.S. container security initiative.** U.S. Customs and Border Protection (CBP) Commissioner Robert C. Bonner announced that the Container Security Initiative (CSI) will be operational at the port of Felixstowe, in England, for cargo containers destined for U.S. ports. CBP and the United Kingdom signed a declaration of principles on December 9, 2002. **As part of the CSI program, U.S. Customs and Border Protection has deployed a team of CBP officers to the port of Felixstowe to work targeting high-risk cargo containers destined for the United States.** United Kingdom Customs officials, working with CBP officers, are responsible for screening any containers identified as a potential terrorist risk. The port of Felixstowe is the 13th CSI port to become operational. **It joins the already operational CSI ports of Rotterdam, LeHavre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Hong Kong, Göteborg, Vancouver, Montreal, and Halifax.**

Source: [http://usinfo.state.gov/cgi-bin/washfile/display.pl?p=/products/washfile/latest=/products/washfile/news\\_item.shtml](http://usinfo.state.gov/cgi-bin/washfile/display.pl?p=/products/washfile/latest=/products/washfile/news_item.shtml)

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

## **Agriculture Sector**

- 7. *June 06, Reuters* — Official sees no need for U.S. cattle quarantine.** U.S. Agriculture Secretary Ann Veneman said Thursday there was no need to quarantine any American cattle herds due to concern about a case of mad cow disease in Canada. **On Wednesday, U.S. Department of Agriculture (USDA) officials announced five bulls were shipped to Montana in 1997 from a Canadian farm involved in the mad cow probe. The bulls were born in Saskatchewan in 1996 in one of the potential source herds for the cow found to have mad cow disease, or bovine spongiform encephalopathy. USDA investigators believe the five bulls were among a group of livestock sent from the Montana farm to stockyards in South Dakota and Montana but are trying to pinpoint what happened to the animals.** Veneman, speaking to reporters, refused to give any forecast on when her agency might lift or modify the near-total ban on importing Canadian beef and live cattle.

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNewsD=2884397>

- 8. *June 05, Successful Farming* — Country of origin labeling will cost producers \$10 per head.** Leaders of the National Pork Producers Council repeated their opposition to mandatory country of origin labeling (COOL) at the opening of the World Pork Expo in Des Moines, Iowa, Thursday. Their opposition is based in part on an economic study showing that the cost of proving domestic origin of U.S. hogs would be about \$10 a head

**for producers.** Country of origin labeling advocates argue that costs will be much lower and that domestic traceability isn't needed under the law. It bars the U.S. Department of Agriculture (USDA) from requiring a traceback system, but Caspers said he expects the industry to require it, and the system may differ from packer to packer. **Mandatory labeling of pork at the grocery store is supposed to start in the fall of 2004, under the 2002 Farm Bill.**

Source: [http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail\\_ANewsindex.html\\_50033\\_1](http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail_ANewsindex.html_50033_1)

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

## **Food Sector**

Nothing to report.

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

## **Water Sector**

Nothing to report.

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

## **Public Health Sector**

9. *June 05, Associated Press* — **WHO says SARS outbreak over its peak. The Severe Acute Respiratory Syndrome (SARS) outbreak is "over its peak" around the world, including in the hardest-hit country China, a World Health Organization (WHO) official said Thursday.** A renewed outbreak in Toronto shows, however, that the world must still remain vigilant against the illness, said Henk Bekedam, the WHO representative in China. "I think the challenge now is to eliminate (SARS) as a public health threat," he said at a news conference. **His comments came as China for a second consecutive day reported no new cases of SARS on its mainland. In Hong Kong, Chief Executive Tung Chee-hwa welcomed the lifting of a travel advisory by the U.S. Centers for Disease Control and Prevention as proof the territory is recovering from the virus.** WHO lifted its own advisory for Hong Kong, imposed in April, nearly two weeks ago. Hong Kong reported no new cases or deaths Thursday. **With Taiwan reporting just one new case, the three areas of the world worst-hit by SARS appeared on the road to recovery.**

Source: [http://abcnews.go.com/wire/World/ap20030605\\_450.html](http://abcnews.go.com/wire/World/ap20030605_450.html)

10. *June 05, Better Humans* — **Smart flu vaccines could prevent pandemic.** Scientists have found that a key weakness in the flu virus could lead to a new class of vaccines that helps prevent a looming pandemic. **Researchers from the University of Melbourne and St. Jude Children's Research Hospital in Memphis, TN report that they have found a chink in the flu virus's armor that could prove key to preventing a predicted pandemic.** The danger of the flu virus is that it constantly changes to elude the body's immune defenses. Vaccinations prime the body by getting it to develop antibodies against related flu strains. "If another pandemic arose, it is unlikely a vaccine will be available in time to effectively combat such a strain," says Steve Turner, a University of Melbourne researcher. **Turner and his team hope**

to create a vaccine that gets killer T–cells to respond to proteins found inside the flu virus, as opposed to those on its surface. The proteins inside the flu virus rarely mutate, so such a vaccine would be more effective.

Source: <http://www.betterhumans.com/News/news.aspx?articleID=2003-06-05-1>

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

## Government Sector

### 11. *June 04, Government Executive* — **Online security clearance forms on track for June debut.**

As promised in March, federal workers will be able to file security clearance forms electronically by the end of June, an Office of Personnel official said Wednesday. **The e-clearance project, one of 24 electronic government initiatives supported by the president's management agenda, is running on schedule, according to Norm Enger, project manager for human resources-related electronic government projects at OPM. Electronic filing is one component of the three-part e-clearance project.** Enger could not provide an exact date for when the electronic filing system would be ready, but said it would be done by June 30 at the latest. When the new automated clearance system is in place, federal workers will be able to complete and file SF-86 forms online. Employees use SF-86 forms to apply for government security clearances.

Source: <http://www.govexec.com/dailyfed/0603/060403a1.htm>

### 12. *June 04, Federal Computer Week* — **Congressman speaks up for E911.** A congressman today called for the creation of an Enhanced 911 office within the Homeland Security Department and a major block grant program to help state and local governments complete their E911 systems. **Rep. Fred Upton (R-MI) said such an office would provide "crucial, unified federal leadership and coordination." The push is based on one of the recommendations in a report sanctioned by the Federal Communications Commission.** Upton was speaking during a hearing on the progress of wireless E911 implementation before the House Energy and Commerce Committee's Telecommunications and the Internet Subcommittee. Upton is chairman of the subcommittee.

Source: <http://www.fcw.com/geb/articles/2003/0602/web-e911-06-04-03.asp>

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

## Emergency Services Sector

### 13. *June 04, U.S. Department of Homeland Security* — **Helping Massachusetts' first responders.**

On Wednesday, June 4, Secretary of Homeland Security Tom Ridge traveled to Boston, Massachusetts to meet with Governor Romney and announce the recent award of \$31,020,000 to the State of Massachusetts to enhance the capabilities of the state and local first responder groups. **These funds can be used for equipment, training, planning and exercises for first responders. In addition, a portion of the funds is available to help offset the costs associated with enhanced security measures deployed under the heightened threat period during the conflict in Iraq.**

Source: [http://www.dhs.gov/dhspublic/interapp/press\\_release/press\\_re lease\\_0169.xml](http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0169.xml)

## **Information and Telecommunications Sector**

14. *June 05, Reuters* — **Variant of Bugbear virus spreading on PCs.** A variant of the Bugbear worm, which spread around the Internet last October, opening back doors on computers and logging keystrokes, has started to infect users around the world, putting them at risk of losing confidential information. According to Mikael Albrecht of computer security company F-Secure, **the worm includes a large list of domains belonging mostly to banks. "The list...includes banks from all over the world; Europe, US, Asia and Africa. Bugbear.B changes system settings if activated in one of these banks,"** he said. The worm variant is better at using addresses in a user's e-mail program than the original, sending itself to those addresses using the infected user's identity, said David Emm of anti-virus company Network Associates Inc. **Once activated, Bugbear.B tries to disable some security programs and starts to snoop on an infected system.** Bugbear.B takes advantage of **a known vulnerability in Microsoft Corp.'s Internet Explorer and can be run automatically simply by reading the e-mail and not opening the attachment.** Users are advised to keep their anti-virus software updated.

Source: <http://www.nytimes.com/reuters/technology/tech-tech-virus-bugbear.html>

15. *June 05, eSecurity Planet* — **Draft vulnerabilities warning guidelines released.** The **Organization for Internet Safety (OIS) is proposing the use of binding arbitration to resolve conflicts and deadlocks between vendors and researchers.** The OIS, a consortium of software vendors, security researchers and consultancies, issued a preliminary draft of best practices for reporting and responding to security vulnerabilities. **"The Finder and Vendor must work together to develop a target timeframe that balances the risk posed by a particular vulnerability versus the engineering challenges associated with thoroughly investigating and effectively remedying it,"** the group said. Within that agreed-upon timeframe, **the OIS proposes that predictable and regular communications occur between the Finder and Vendor.** Once the investigation is complete and a remedy has been delivered, the Finder and Vendor observe a 30-day grace period during which they provide such details only to people and organizations that play a critical role in advancing the security of users, critical infrastructures, and the Internet. Upon the expiration of the grace period, these details can be shared more broadly," the group said.

Source: <http://www.esecurityplanet.com/trends/article.php/2217751>

16. *June 05, Federal Computer Week* — **Bush proposes spectrum management plan. President Bush announced Thursday an initiative to improve the efficiency and management of radio frequency spectrum to keep pace with the expanding technologies.** The spectrum policy initiative is intended balance the often competing interests of promoting economic growth, ensuring national security, and satisfying public safety, research and transportation infrastructure needs, according to White House officials. **"The existing legal and policy framework for spectrum management has not kept pace with the dramatic changes in technology and spectrum use."** The initiative, chaired by the Commerce Department, includes two actions: the development of an interagency federal spectrum task force and the convening of a series of public meetings. **There are more than 140 million wireless phone customers,**

**and businesses are increasing the installation of Wi-Fi systems for wireless computing,** White House officials said. **The government uses spectrum for radars, communications, geolocation and space operations.** The Presidential Memo on Spectrum Policy is on the White House Website: <http://www.whitehouse.gov/news/releases/2003/06/20030605-4.html>. Source: <http://fcw.com/fcw/articles/2003/0602/web-spectrum-06-05-03.asp>

17. *June 04, National Journal* — **Security officials urge more research into supercomputing. The nation's investment in supercomputing research and development has played a crucial role in national security, but more investment is needed to resolve numerous computational problems,** a key National Security Agency (NSA) official said on Wednesday. George Cotter, chief of NSA's Office of Corporate Assessments, told attendees of an Army High-Performance Computing Research Center luncheon that **the conclusion of a congressionally mandated study on high-end computing R&D determined a need for faster computing to enable the military to create better weapons, aircraft and ships, as well as to improve the nation's ability to monitor its nuclear-weapons stockpile.** Faster computers also are needed to analyze intelligence data and build better mapping capabilities for the military, he said. The center has received \$4 million in research funding annually over the past two years from the Army as the Pentagon decided to increase its focus on using supercomputing for military purposes. The program was initiated in 1990. Source: <http://www.govexec.com/dailyfed/0603/060403td1.htm>

18. *June 01, Information Security* — **Cyber Corps' failing grades. Federal administrators are overhauling Cyber Corps because conflicting policies and management structures are making it increasingly difficult to place graduates of the infosec training program in government jobs.** University coordinators say getting the first 50 Cyber Corps graduates into federal jobs proved extremely difficult. **Federal agencies were unwilling to hire inexperienced security admins when more senior infosec positions went unfilled.** Complicating the situation is **the Office of Personnel Management (OPM), which is responsible for placing students but has little authority to compel placements.** Officials are still working on details, but it has already been decided to reorganize Cyber Corps based on the Department of Defense's Information Assurance Scholarship Program. The government launched Cyber Corps in 2001 under the scholarship for service model. Students receive tuition and a stipend in exchange for serving in a summer internship and working at a government agency for up to two years. **Cyber Corps has distributed nearly \$30 million to upgrade university infosec programs and fund scholarships for 200 students at 13 universities certified as Centers for Academic Excellence by the National Security Agency.** Source: <http://www.infosecuritymag.com/2003/jun/cybercorps.shtml>

## Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a>	 Security Focus ThreatCon: 2 out of 4 <a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a>
Current Virus and Port Attacks	
<b>Virus:</b>	#1 Virus in the United States: <b>BAT_SPYBOT.A</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
<b>Top 10 Target Ports</b>	137 (netbios-ns), 80 (www), 1434 (ms-sql-m), 445 (microsoft-ds), 113 (ident), 139 (netbios-ssn), 53 (domain), 0 (---), 25 (smtp), 41170 (---) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center

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

## General Sector

19. *June 05, Associated Press* — **Inmate suspected of planning Los Angeles attack.** A man in prison for vehicle theft is suspected of planning a significant attack, say authorities who uncovered an arsenal of semiautomatic assault weapons, ammunition, pipe bombs and barrels of jet fuel. **Authorities have not been able to identify any targets, and the man has refused to talk to investigators, said sheriff's Sgt. John Demooy. "He was definitely planning on targeting a structure, location, individuals, and would have created significant damage," Demooy said.** The Bureau of Alcohol, Tobacco and Firearms is investigating John Noster, 38, for firearms and explosives violations and plans to present its findings to prosecutors, said spokeswoman Latese Baker.

Source: <http://www.newsday.com/news/nationworld/nation/wire/sns-ap-explosives-probe.0.6424231.story?coll=sns-ap-nation-headlines>

20. *June 05, Global Security Newswire* — **New Zealand: Auckland man building cruise missile inside garage.** In May 2002, Auckland-based Internet technology journalist Bruce Simpson wrote an article claiming that an effective cruise missile could be built using readily available and inexpensive materials. He received extensive feedback, some from doubters who said he underestimated the difficulty of such a project. **Simpson decided to prove the skeptics wrong by building a cruise missile in his garage for less than \$5,000. He is publishing his work on a Web site ( <http://www.aardvark.co.nz/pjet/cruise.shtml> ) and says the project is progressing well. The missile is on budget and only six weeks away from testing, although Simpson will need cooperation and clearance from the New Zealand Air Force before a test flight, he said.** Simpson is attempting to build a missile that can travel at least 100 miles, carry a payload of 22 pounds and be launched from the bed of a pickup truck. The components, including the Global Positioning System and the missile's fiberglass body, were bought from commercial retailers. The parts that came from outside New Zealand were shipped and passed through customs without incident or question.

Source: [http://www.nti.org/d\\_newswire/issues/newswires/2003\\_6\\_4.html#10](http://www.nti.org/d_newswire/issues/newswires/2003_6_4.html#10)

21. *June 05, New York Times* — **Suicide bomber kills at least 17 on bus near Chechnya.** A woman blew up a bus carrying airmen and military personnel early Thursday as it paused at a railroad crossing west of Russia's separatist Chechnya province, killing herself and at least 17 others and wounding perhaps 16 more. **It was the third suicide bombing in the region in just over three weeks, as well as the third in which a woman was either the bomber or a participant. Some of the wounded were in grave condition and were not expected to survive, doctors said.** The Russian police had made no arrests by late on Thursday. They said they believed the bombing was the work of Islamic extremists who have been waging an increasingly violent guerrilla war against the Russian military and Chechnya's Kremlin-backed government.

Source: <http://www.nytimes.com/2003/06/05/international/europe/05CND-RUSS.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 Assessments, 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](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 202-324-1129

Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) 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](mailto: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.