



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 01 September 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- Government Computer News reports the New York City Transit agency has added 230 Iridium satellite service telephones to its emergency communications, and has installed a satellite repeater to enable indoor communications at its Manhattan headquarters, to help with security for the Republican National Convention. (See item [10](#))
- The Associated Press reports multiple agencies from the U.S. and Mexico are working together to track cattle, prevent agroterrorism, and ensure that a major livestock disease doesn't pass between the countries. (See item [18](#))
- Federal Computer Week reports Pennsylvania's state officials have developed an integrated network that Department of Homeland Security officials praise as a model for the kind of information sharing and collaboration that are crucial to preventing future attacks. (See item [22](#))

DHS/IAIP Update *Fast Jump*

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

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [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. *August 31, Washington Post* — **Russian queried over photos. A high-level Russian diplomat was questioned by local and federal authorities Sunday, August 29, after a 911 caller became suspicious of a man photographing a liquefied natural gas terminal on the waterfront in Calvert County, MD, state police said. According to Lt. Homer Rich, the man**

appeared to be taking pictures of the bay, various wildlife and fauna with Dominion's Cove Point gas terminal in the background. The man, whom authorities identified only as a member of the Russian Embassy who has been living in the United States for six years, was not detained, Rich said. The man's digital camera card and videotape were confiscated and will be forwarded to the State Department or the Department of Homeland Security, Rich said. If federal authorities find the items not to be a threat, they will be returned to the man, he said. "It does not appear to be that he was focusing on the power plant," Rich said, adding that the man was not trespassing when he got out of a vehicle and took the pictures and video. Calvert residents and Maryland lawmakers have raised concerns that the liquid nitrogen gas facility could become a target of terrorist attack.

Source: http://www.washingtonpost.com/wp-dyn/articles/A48052-2004Aug_30.html

2. *August 31, New York Times* — **Tar sands operations are looking attractive.** Part of Canada's energy industry is going through a spurt of frenetic development -- the production of oil by sucking the viscous tar out of the sandy soil around Fort McMurray, Alberta. It is not easy and it is not cheap, but both sides of the equation have now changed. North America's crude oil resources have been thoroughly explored, and in the rest of the world, most of the best places to drill for new oil are off limits or are already pumping every barrel they can. So, with global demand driving energy prices up to record levels over the last few years and fresh supplies of crude oil so hard to find, more than a dozen other energy companies are pursuing projects in Fort McMurray. Their output is already crucial to the United States' energy supply. **While the United States deepens its reliance on Canadian energy -- Canada is already the country's largest supplier of both oil and natural gas -- the frenzy of tar sands development in Alberta highlights an uncomfortable fact about the search for unconventional sources of oil to replace dwindling conventional supplies: it depends on petroleum prices staying high for decades to come.**

Source: <http://www.nytimes.com/2004/08/31/business/31tar.html>

3. *August 31, Reuters* — **Florida Gas issues overage alert day due to heat.** Florida Gas Transmission issued its second consecutive overage alert day on Tuesday, August 31, due to continued high temperatures in the state, the company said in a posting on its Website. Because high natural gas demand for cooling had reduced line pressure in the system, the company issued an overage alert at 20 percent tolerance, meaning that shippers must stay within 20 percent of their scheduled volumes. **Alerts, also called critical days, require natural gas shippers to carefully adhere to scheduled quantities to maintain system integrity.** An overage alert signals that taking excess quantities off line would be harmful. The 5,000-mile Florida Gas Transmission pipeline extends from south Texas to south Florida, with a mainline capacity of 2.1 billion cubic feet per day.

Source: http://biz.yahoo.com/rc/040831/energy_natgas_florida_1.html

4. *August 31, Dominion Virginia Power* — **Gaston knocks out power in Virginia.** Dominion Virginia Power crews and contractors from Northern Virginia and Hampton Roads are in the Richmond, VA, metropolitan area on Tuesday, August 31, restoring power to thousands of customers affected by Tropical Storm Gaston. **As of 10 a.m. Tuesday, about 60,000 customers in Richmond, East Richmond and Midlothian service areas of Dominion were without power.** Power is expected to be restored to most of these later in the day, with the remainder back on by Wednesday, September 1. About 10 to 14 inches of rain fell Monday,

August 30 in central Virginia. **Two of Dominion's major electric substations were flooded and severely damaged.** Much of Tuesday's work focused on restoring some level of service to those substations and reconfiguring other circuits to deliver power. However, because some buildings were destroyed, not all power will be restored until electrical inspectors give their approval.

Source: <http://www.dom.com/news/storm.jsp>

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

Chemical Industry and Hazardous Materials Sector

5. *August 31, Associated Press* — **Fire at ag fertilizer facility. Experts will try to determine what started the Tuesday, August 31, fire at a fertilizer distribution site in rural Greenville, TX.** Nobody was hurt. Hazardous materials crews remained at the El Dorado Chemical ag center to monitor the smoldering chemicals. A school in Floyd, about ten miles west of the scene, was evacuated — as a precaution. Company spokesperson John Carver says four people work at the Greenville site, but nobody was present when the fire broke out just before dawn. Carver told The Associated Press that there was no explosion. He says the unit blends and distributes bulk fertilizer to farmers in the area, with no manufacturing done at the facility. Greenville is about 45 miles northeast of Dallas.

Source: <http://www.dfw.com/mld/startelegram/news/state/9545333.htm>

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

Defense Industrial Base Sector

6. *August 30, Government Computer News* — **DoD networks the future.** The Army's Future Combat Systems (FCS) program, the flagship of the Army's transformation effort, is still in the early stages of development and about a decade from fielding its first fully equipped Unit of Action. However, Army officials are bringing the FCS future a little closer. **Prompted by the exigencies of the war on terror and the ongoing fighting in Iraq, Army officials recently announced that the program would be accelerated to provide some FCS technology elements to the current force before the fielding of the 18 FCS systems begins in 2014. Program officials expect to begin merging elements of FCS' network technology into current-force systems in 2008 or perhaps earlier,** said retired Army Lt. General Dan Zanini, deputy program manager for the lead systems integrator team and FCS program manager for a private contractor. FCS is the embodiment of the Department of Defense's (DoD) vision of a network-centric Future Force, which will let 18 avant-garde manned and unmanned systems, all operating under the same network architecture, wage war as a single unit.

Source: http://www.gcn.com/23_25/news/27082-1.html

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

Banking and Finance Sector

- 7.

August 31, Evening Standard (UK) — **Gangs target High Street banks.** Organized criminals have infiltrated High Street banks, a City of London, England, detective has warned. Detective Chief Superintendent Ken Farrow on Tuesday, August 31, said that **a new generation of criminals was targeting retail banks across the country, gaining confidential account details by posing as temporary bank employees. Once employed, they approached members of staff and offered bribes or resorted to blackmail to elicit account numbers.** He said that "it's the pressure and competitiveness of banking that is making this happen now. It happens because some manager is trying to find people for a key launch as quickly as possible and there are difficulties vetting them. The banking industry is being swept away by short-termism." Of the 350 cases he was currently investigating, a very significant number involved insiders, he said.

Source: http://www.thisislondon.com/news/business/articles/timid8194_0?source=

8. *August 31, New York Times* — **UN seeks tighter sanctions as al Qaeda skirts money controls.** Al Qaeda no longer needs large sums of money to mount terror attacks and is consequently able to finance its actions in less detectable ways, the chairman of a United Nations (UN) sanctions-monitoring committee said Monday, August 30. "We have passed the easy stage. The easy stage was the first few years, when freezing bank accounts of individuals and organizations linked to al Qaeda was a relatively easy task. Now they have become more flexible, they are staying ahead of the sanctions, and we need obviously to be better at combating them because they have become better at defending themselves," said Ambassador Heraldo Muñoz of Chile, the chairman of a panel examining the effectiveness of arms and travel embargoes against people and organizations tied to the terror group. **Among the difficult-to-scrutinize financing sources for al Qaeda that the report listed were crime proceeds, diverted charitable donations, counterfeit currency trading in Somalia, credit card fraud in Western Europe and Asia, the drug trade in Afghanistan and Northern Africa, and an ancient financial system where money brokers in the Middle East, Pakistan, India and Southern Asia can move cash from one office to another based on trust.**

Source: <http://www.nytimes.com/2004/08/31/international/31nations.html>

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

Transportation Sector

9. *August 31, Washington Times* — **Amtrak cancels mail on passenger trains. Amtrak plans to stop carrying mail in October as it refocuses on its core business of transporting passengers.** "The profit margin is small and we feel that making these changes will improve our bottom line, make the trains more efficient," Amtrak spokesperson Cliff Black said on August 30. The U.S. Postal Service has used passenger trains to carry mail since 1831, when some of the first regular passenger rail service started in the United States. Black said "interference with passenger train operations" compelled Amtrak's management to curtail the contract. **The interference includes delays from coupling and uncoupling freight rail cars to passenger trains. Amtrak also has to divert some of its resources to maintenance of the rail cars.** Steve Kulm, Federal Railroad Administration spokesperson said, "The more they focus on their core business of moving people, the better off they're going to be." Ending mail service on Amtrak is likely to shift more bulk mail to freight railroads, long-haul trucks and

airline service.

Source: <http://washingtontimes.com/business/20040830-093538-8027r.htm>

10. *August 31, Government Computer News* — **NYC Transit enhances satellite communications capabilities.** The New York City Transit (NYCT) agency has added 230 Iridium satellite service telephones to beef up its emergency communications and has installed a satellite repeater to enable indoor communications at its Manhattan headquarters. **This was installed last week in anticipation of the Republican National Convention. If telephone or power systems are knocked out, satellite service will remain available.** NYCT is the largest agency within the regional Metropolitan Transportation Authority and operates the city's bus and subway systems. It carries 2.2 billion riders a year, has 48,000 employees and has been tasked with securing the transit system during the convention. The convention has been designated a national special security event, making Department of Homeland Security funding available for security technology.

Source: http://gcn.com/vol1_no1/daily-updates/27120-1.html

11. *August 31, Associated Press* — **NTSB wants alert systems for towboats.** Federal safety officials on Tuesday, August 31, said that an alert system could have warned a towboat crew that their pilot had fainted and prevented the deadly collapse of the Interstate 40 bridge near Webbers Fall, OK, in 2002. The National Transportation Safety Board (NTSB) also said that fewer people might have died if there had been a warning system to alert motorists that the Arkansas River bridge had fallen. The safety board found that some of the 14 people who died in the accident could not stop before driving over the edge of the collapsed bridge. **NTSB chairman Ellen Engleman Connors said that only a handful of the nation's 6,000 bridges have systems to warn motorists that a bridge has fallen. She compared the absence of warning systems on bridges to the abundance of alert methods on the interstate highway system.**

Source: <http://www.nj.com/newsflash/topstories/index.ssf?base/politics-4/109397154822040.xml&storylist=>

12. *August 31, Government Computer News* — **FAA says IT reduces airport runway hazards.** Runway incursions at the nation's airports dropped 20 percent over a four-year period, due in part to technology, said a Federal Aviation Administration (FAA) report released on Tuesday, August 31. U.S. airports recorded 324 incursions last year, 15 fewer than in 2002. Last year, 32 of the incidents were characterized as high risk, five fewer than in 2002 and a 50 percent drop since 2000. For the second consecutive year, none of the most serious incursions involved two large commercial jets. "Pilot awareness programs and new technology continue to pay real safety dividends on the nation's runways," said FAA administrator Marion Blakey. **To prevent runway accidents, FAA has delivered to 34 airports new technology called the Airport Movement Area Safety System, which warns air traffic controllers of potential runway accidents, and is deploying the new Airport Surface Detection Equipment Model X to another 25. ASDE-X creates up-to-the-minute maps of all airport operations that controllers oversee. It is especially helpful at night or in bad weather, when visibility is poor,** FAA has said. A runway incursion is when an aircraft, vehicle, person, or object on the ground creates a collision hazard or is too close to an aircraft taking off, intending to take off, landing or intending to land. The report is available on this site:

http://www.faa.gov/Newsroom/highlights/runway_safety.cfm

Source: http://www.gcn.com/vol1_no1/daily-updates/27122-1.html

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

Postal and Shipping Sector

13. *August 31, DM News* — **Postal facilities' anthrax testing. Further testing is not necessary at postal facilities originally deemed free of anthrax spores after the attacks of 2001, federal health, safety, and security agencies working with the U.S. Postal Service (USPS) said in a report that was issued last week.** Five people died and several were sickened after the anthrax-by-mail attacks. Postal facilities in Washington, DC, New Jersey, and elsewhere were decontaminated. The report responded to General Accounting Office recommendations that the USPS reassess the risk levels to employees and customers in facilities not contaminated. The report was prepared in conjunction with the Centers for Disease Control and Prevention, Environmental Protection Agency, Occupational Safety and Health Administration, the American Postal Workers Union, the National Association of Letter Carriers, the National Postal Mail Handlers Union, and the National Rural Letter Carriers Association. **The unions and government agencies concluded that the anthrax risk level for postal workers in the facilities tested and that the general public served by those facilities is negligible.** More testing would not increase the safety of postal facilities for employees or customers, they said. The USPS is installing anthrax detection equipment in mail-handling facilities nationwide. Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=3025_1

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

Agriculture Sector

14. *August 31, United Press International* — **Mystery illness hits Indonesian farms. Indonesian poultry farmers, following a bird flu outbreak, are facing another mysterious disease that has killed thousands of chickens in the past few days. Apart from the deaths, which have caused heavy losses, farmers say the problem has been aggravated by the fact that the surviving chickens are not breeding, the Straits Times reported Tuesday, August 31.** And the disease is spreading rapidly. Sick chickens first salivate and show symptoms of diarrhea, then die within hours, farmers said. The head of the poultry division of the Sleman agriculture agency, Suwadi Azis, said his office had not received any reports from poultry farmers on the disease outbreak. But he said the symptoms indicated the outbreak could be Newcastle Disease. Source: http://washingtontimes.com/upi-breaking/20040831-015915-7762_r.htm
15. *August 31, Sunday Times (South Africa)* — **Bird flu contained on ostrich farms. Tests for bird flu on ostriches across the Somerset East quarantine zone, in South Africa, have been completed and indicate the disease has been contained, the agriculture department said Monday, August 30.** Blood tests were conducted on every flock on 31 farms near Middleton where the disease was first detected in late July. "According to the reports so far, there is no indication of the disease anywhere else," agriculture department spokesperson Segoati Mahlangu said. A second round of testing will be undertaken after a three-week window period. South Africa could officially give the "all clear" for the district 21 days after the last

negative test result had been confirmed, Mahlangu said.

Source: <http://www.sundaytimes.co.za/zones/sundaytimes/business/business1093941369.asp>

16. *August 31, News Leader (VA)* — **Oak disease threatens. A California–born disease that quickly kills oak trees by attacking their root systems has been found in Virginia.** Sudden oak death was found in a Hampton nursery camillia and on a rhododendron at a Chesapeake nursery, said Frank Fulgham, program manager for the office of plant and pesticide services. Both plants were found in nursery stock by the U.S. Department of Agriculture. A variety of trees and shrubs can carry the disease across state lines as they are shipped from growers to consumers. The forest service is surveying wooded areas around nurseries. Virginia and Carolina are marked "high risk" in a map on the forest department's Website.

Source: <http://www.newsleader.com/news/stories/20040831/localnews/1147473.html>

17. *August 31, Wisconsin Ag Connection* — **Animal ID system. Wisconsin has the nation's first mandatory livestock premises registration law, a necessary first step toward the goal of 48–hour traces in animal disease outbreaks. While that law hasn't taken effect yet, farmers can already register on a voluntary basis using the same system that will be used when registration becomes mandatory beginning January 1, 2006.** The Wisconsin premises registration system is a product of a five–year effort by a private–public partnership called the Wisconsin Livestock Identification Consortium, or WLIC. It has received \$1.75 million in federal funding and developed a database where producers can register either online or on paper, from home or through agents such as cooperatives or government offices. The system assigns each premises a unique number and protects the confidentiality of producers. It is available voluntarily now, and has been named by the U.S. Department of Agriculture as the prototype for a national system. Producers in other states can also register.

Source: <http://www.wisconsinagconnection.com/story–state.cfm?Id=1035 &yr=2004>

18. *August 30, Associated Press* — **U.S., Mexico confront threat of agroterrorism. Multiple agencies from the U.S. and Mexico are working together to track cattle, prevent agroterrorism, and ensure that a major livestock disease doesn't pass between the countries.** George Perea works on the Mexican side of the border. He checks a steer's ears for fever ticks, runs his hands down its neck feeling for lumps, and makes sure it's been castrated. Further down the line, a U.S. Department of Agriculture veterinarian marks the lame animals. The inspectors also look for cuts or other symptoms of diseases. While border authorities have worked to ensure there won't be an outbreak of any natural diseases, agroterrorism has become a concern. New Mexico is spending some of its homeland defense money to learn how to stop a potential disease outbreak, Brig. Gen. Annie Sobel, head of the New Mexico Office of Homeland Security, said. "Make sure you understand who the workers are transporting milk and where they are taking it," Sobel said. "And make sure they adhere to the timelines for deliveries. If there are any deviations from the schedule, the delivery points, you have to have traceability as to who, what, when, where, how," Sobel said. **New Mexico, Arizona, Colorado, two Mexican states, the Navajo Nation, and Hopi Tribes plan to use a \$1.2 million regional grant from the USDA grant for the Tri–National Health and Identification Consortium.**

Source: <http://www.santafenewmexican.com/news/3695.html>

[[Return to top](#)]

Food Sector

Nothing to report.

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

Water Sector

19. *August 31, Toledo Blade (OH)* — **Firms must stop using wells.** Five more businesses on South Bass Island, OH, have been told to stop using their well water because of possible contamination, state officials said Monday, August 30, as they continued investigating a mysterious gastrointestinal outbreak that has sickened more than 1,100 people. One of the wells is at the Put-in-Bay Airport, and the others are at businesses that cater to tourists. **All five facilities' wells tested positive for total coliform bacteria, "which is an indication that there could be more serious bacteria or pathogens present in the water,"** said Mike Baker, chief of the Ohio Environmental Protection Agency (EPA) drinking and ground waters division. Officials repeated that they have not identified a source of the outbreak but made it clear they are focusing on the island's water supplies. The agency is focusing on groundwater with possible sewage contamination, Baker said. Frequent testing of water samples at the businesses where orders have been issued will continue, according to EPA spokesperson, Heidi Griesmer. Both raw water and water treated with chlorine will be sampled, she said.

Source: <http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20040831/NEWS17/408310361/-1/NEWS>

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

Public Health Sector

20. *August 31, The Business Journal– Phoenix* — **Research groups close in on genetic key to anthrax.** Science is a step closer to understanding the genetic makeup of anthrax, thanks to the efforts of several Arizona institutions. Researchers at Northern Arizona University (NAU), the Translational Genomics Research Institute (TGen) and The Institute for Genomic Research (TIGR) have worked hard to define the genetic and evolutionary types of several anthrax strains. **Officials say this new bacterial typing system will help create bio-defenses against anthrax to protect people and animals and provide forensic investigation into previous events.** The work provides the raw material for highly specific and sensitive tests for anthrax in human cases, animal cases and within the environment. The results are scheduled for publication online this week by the journal "Proceedings of the National Academy of Sciences."

Source: <http://phoenix.bizjournals.com/phoenix/stories/2004/08/30/day11.html>

21. *August 30, The Moscow News (Russia)* — **Suspected anthrax death puts Russian city on alert. A man has died with symptoms of anthrax in the south Russian city of Orsk, and eight others, including one child, have been hospitalized on suspicion of being infected with the deadly bacteria.** Epidemiologists in the region have said the infection may have been caused by beef brought in for sale in the city, which borders Kazakhstan, by a local resident, the

Itar–Tass news agency reported. The Soviet Union has developed and stored anthrax spores in the past for potential use as biological weapons. It surfaces occasionally in Siberia and in south eastern Russia. Anthrax, depending on the form, can kill from one fourth to over half of those it infects. While it is not generally passed from person to person, it is often spread through animal contact or eating undercooked meat.

Source: <http://www.mosnews.com/news/2004/08/30/anthrax.shtml>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

22. *August 31, Federal Computer Week* — Pennsylvania's Justice Network provides a model of integration. Pennsylvania's state officials have developed an integrated network that Department of Homeland Security officials are touting as a model for the kind of information sharing and collaboration that are crucial to preventing future attacks. **Pennsylvania's Justice Network (JNET) is a secure system that allows users to access criminal data, mug shots, driver's license photos and other law enforcement data. It is available to federal and state agencies and local police departments.** The Pennsylvania Justice Network is a TCP/IP–based extranet that connects agency servers to one another. At the center is the JNET hub, which provides the platform for housing limited content, namely driver's license photos and mug shots, and applications and communications services that belong collectively to JNET agencies. Firewalls are deployed between the JNET hub server, each JNET agency and the commonwealth's metropolitan–area network. **Since its inception in 1997, JNET has helped locate a terrorism suspect days after the September 11 attacks, track down individuals wanted in connection with the murder of two New York City detectives and nab a bank robbery suspect less than two hours after the crime was committed.**

Source: <http://www.fcw.com/supplements/homeland/2004/sup3/hom-collab-08-30-04.asp>

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

Information Technology and Telecommunications Sector

23. *August 31, Secunia* — WS_FTP server file path parsing denial of service vulnerability. According to Secunia Advisory SA12406, vulnerability exists in WS_FTP Server version 5.0.2, which can be exploited by malicious users to cause a DoS (Denial of Service). The problem is caused due to an error in the parsing of file paths and can be exploited to cause a vulnerable system to use a large amount of CPU resources. Successful exploitation requires that the user has been authenticated. **There is no vendor solution available at this time. As a workaround, restrict access to the FTP server and disallow anonymous usage.**

Source: <http://secunia.com/advisories/12406/>

24. *August 30, Network World* — **States prepping cyberalert plan.** Looking to gauge the risk of attacks against their networks, state officials this week will vote on new measures that would assess threats and dictate specific actions to take to protect key resources. If adopted, the common alert–level procedures would color–code the threat to state networks and recommend action to take in response to specific threats. The proposed cybersecurity alert system would establish a secure Website state officials could tap to determine why each state has the security ranking it does and whether they should take action based on what other states experience. **Homeland security ranked among the key topics considered last week at the National Association of State Telecommunications Directors (NASTD).**
Source: <http://www.nwfusion.com/news/2004/083004nastd.html>

Internet Alert Dashboard

DHS/US–CERT Watch Synopsis

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

US–CERT Operations Center Synopsis: The US–CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See <http://www.us-cert.gov/cas/alerts/SA04–243A.html> for more information.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 137 (netbios–ns), 445 (microsoft–ds), 9898 (dabber), 5554 (sasser–ftp), 1433 (ms–sql–s), 1023 (Reserved), 1434 (ms–sql–m), 3127 (mydoom), 1026 (nterm)
----------------------------	---

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

25. *August 31, WDIV (MI)* — **Detroit judicial building evacuated.** A security breach caused the evacuation of the Coleman A. Young Municipal Building in downtown Detroit on Tuesday, August 31. The occupants of the building were sent to nearby Hart Plaza as a precaution. Detroit Police officer Glen Woods said a 6–by–4–inch package was found on a window ledge of the sixth floor of the building. Building security said a suspicious package had been received, and X–rays were not able to determine the substance inside the package, said councilwoman JoAnn Watson. The Michigan State Bomb Squad was called to the scene to inspect the package and safely removed the package from the building.

Source: <http://www.clickondetroit.com/news/3694641/detail.html>

26. *August 31, Associated Press* — **Handheld computers aid convention security.** In addition to their usual weaponry, some officers responsible for securing federal buildings at the Republican National Convention in New York are armed with devices like handheld computers. The computers are part of a wireless arsenal the Federal Protective Service (FPS) is using to create an instantaneous flow of images between officers on patrol and those manning monitoring stations at a command center in an undisclosed location. Helmets and vehicle dashboards with digital video cameras are also on hand to expand the coverage provided by cameras atop federal buildings. **"It allows us to have a complete situational awareness of what's going on the street,"** said FPS New England Regional Director Ron Libby, who is overseeing security for some 30 Manhattan-area buildings where federal employees work. **FPS controls the technology, but it is available to other security organizations like the Secret Service and New York Police Department when they need it.** In one instance officers were able to quickly dispel reports that parachutists had landed on top of a federal building.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A48553-2004Aug 31.html>

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

General Sector

27. *August 31, Associated Press* — **Moscow subway station blast kills ten.** A woman strapped with explosives blew herself up outside a busy Moscow subway station Tuesday, August 31, killing at least ten people and wounding more than 50 the second terrorist attack to hit Russia in a week. Seven days earlier, almost to the hour, two Russian jetliners crashed within minutes of each other in what officials say were terrorist bombings. All 90 people aboard the aircrafts were killed, and the investigation has focused on two Chechen women believed to have been passengers. **There was no immediate claim of responsibility for Tuesday's bombing, but suspicion was certain to fall on Chechen separatists and their supporters. Several female suicide bombers allegedly connected with the rebels have caused carnage in Moscow and other Russian cities in a series of attacks in recent years.** Many are believed to be so-called "black widows," who have lost husbands or male relatives in the fighting. Mayor Yuri Luzhkov told reporters near the Rizhskaya subway stop in northern Moscow that the bomber was walking toward the station shortly after 8 p.m. but turned around when she saw two police officers. "There was a desire to cause maximum damage," he said.

Source: http://abcnews.go.com/wire/World/ap20040831_1422.html

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

DHS/IAIP Products & Contact Information

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

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

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues.

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644.

Subscription and Distribution Information: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov 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.

DHS/IAIP Disclaimer

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