



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 14 August 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The accountingweb reports a new identity theft scam is targeting those who apply for loans answering an advertisement with the actual logo of a recognized financial institution; the contact information is false and applicants are asked to provide their Social Security number, bank account numbers, and other private information. (See item [7](#))
- The Seattle Times reports two Pakistani men are being held by federal authorities in Seattle, after an airline employee at Seattle–Tacoma International Airport found one of their names on a terrorism–related no–fly list Saturday night. (See item [18](#))
- eWEEK reports computer users were scrambling on August 13, for alternate fixes for the havoc wreaked by the Blaster worm, since many people were unable to reach Microsoft Corp.'s main patch download site. (See item [22](#))

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. *August 13, The Sacramento Bee* — **Training triggers outage. On Tuesday, August 12, a grid operator receiving annual training on the Sacramento Municipal Utility District's (SMUD) emergency response system mistakenly started the computer program intended to be used only in a power disaster, the kind that could knock utility after utility off–line. In**

such an emergency, SMUD could use the program to shed lots of electricity load in a minute or less, potentially sparing its entire grid from crashing. Once the trainees realized that the power disaster program had been put into action, and was dumping about 15 percent of SMUD's load, they shut it off and began the slower process of bringing people back on line in an orderly way. **The outage affected nearly 70,000 homes and businesses and lasted for about 10 minutes.**
Source: <http://www.sacbee.com/content/news/story/7215754p-8161295c.html>

2. *August 12, The New York Times* — **Indian Point is said to pass U.S. test in mock attack. The private security force at the Indian Point nuclear power plant successfully repelled multiple mock attacks in a high-tech training exercise conducted two weeks ago,** the head of the Nuclear Regulatory Commission said in a letter released Monday, August 11, the first public assessment of the exercise. However, **environmental groups charge that the drill was unrealistic because the plant knew about the mock attack months in advance,** and it did not involve a suicide-attack situation. Last month the Federal Emergency Management Agency approved a plan to deal with a disaster at the plant despite complaints from surrounding communities that the plan would not adequately protect the 300,000 people who live within 10 miles of the plant. The Nuclear Regulatory Commission immediately accepted the emergency management agency's recommendation.

Source: <http://www.nytimes.com/2003/08/12/nyregion/12NUKE.html>

3. *August 11, The Associated Press* — **A renewed demand for anti-terrorist plan for Yucca. Nevada congresswoman Shelley Berkley is resurrecting a bill that would require the government to develop a comprehensive anti-terrorist plan for Yucca Mountain.** The bill directs Homeland Security officials to enlist federal, state and local law enforcers to prepare plans to counter possible terrorist attacks on nuclear waste shipments to Nevada. It also requires the Federal Energy Management Agency to develop an emergency response strategy in case of a terror attack. Berkley submitted a similar measure nearly two years ago that failed.

Source: <http://www.krnv.com/Global/story.asp?S=1396889&nav=8faOHOaL>

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

Chemical Sector

4. *August 13, The Town Talk (LA)* — **Residents return home after chemical mishap. Residents living near the Rapides Parish Water District #3 plant (Pollock, LA) were told to either evacuate or remain in their homes after a hazardous chemical incident at the plant Monday afternoon.** Nearby La. Highway 3130, which had been closed to traffic following the incident, was re-opened late Tuesday afternoon. Only the road leading directly to the plant remained closed late Tuesday. The continued closure was a precautionary measure, Grant Parish Sheriff's Chief Deputy Preston Mosley said. About 20 to 30 residents were asked to leave the area about 4:30 p.m. Monday after a delivery driver's mistake at the plant. **Authorities said the driver, who works for a Georgia company, accidentally mixed phosphoric acid and sodium chlorite in a tank, causing a reaction cloud.** Louisiana State Police Haz-Mat troopers arrived Monday and took over handling of the incident. A small cloud remained late Monday night, but emergency workers were applying water vapor to keep it under control. Farris said there were no reported injuries, but Mosley said that at least one person complained of feeling ill. **Residents near the plant were asked to leave, and those**

within a one-mile radius were asked to stay indoors.

Source: <http://www.thetowntalk.com/html/D52F29F7-5269-44B6-8818-957878F15E44.shtml>

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

5. *August 13, The Leader (CA)* — **Police finding counterfeit bills in Burbank. Police in Burbank, CA, have encountered at least two cases in one month of someone trying to pass a counterfeit \$100 bill recently, and said other fake bills may be in local circulation.** A police spokesperson said that because counterfeiters often pass several bills in one area and then move on to elude capture, the appearance of two instances of counterfeit bills in such a short period of time could mean other bills are in circulation in the area. Burbank Police have notified the Secret Service about the counterfeiting cases, which is a federal crime. In addition to the criminal investigations, Burbank Police hold training sessions to teach retailers how to identify counterfeit bills.

Source: <http://www.latimes.com/la-blr-counterfeit13aug13.0.4631095.story>

6. *August 13, The Washington Post* — **Plan would ask banks to warn of data vulnerability. Federal banking regulators proposed guidelines on Tuesday, August 12, that would direct financial institutions to notify customers when security breaches in their computer networks could lead to identity theft.** Under the guidelines, banks and other financial institutions would alert customers by mail, telephone or e-mail, when they find unauthorized access to personal data that could result in substantial harm or inconvenience. Banks also would be told to flag any accounts that may have been compromised and monitor them for unusual or suspicious activity. The proposed guidelines, not to take effect to next year at the earliest, were issued by the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Federal Reserve Board.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A51690-2003Aug 12.html>

7. *August 13, accountingweb* — **Latest identity theft scam centers on fake loans.** A new identity theft scam is targeting those who apply for loans. **The way the scam works is that an advertisement appears in a print publication bearing the actual logo of a recognized financial institution. The contact information, however, is false and typically leads to prepaid cell phone numbers.** Loan applicants are asked to provide their Social Security number, bank account information, and in some cases even a photocopy of a driver's license and Social Security card. Loans are approved and applicants are asked to send a pre-payment of the first loan payment via Western Union wire transfer. The Federal Deposit Insurance Corporation is asking those who have been victimized to file a complaint with the Federal Trade Commission.

Source: <http://www.accountingweb.com/cgi-bin/item.cgi?id=97962&d=815&h=817&f=816&dateformat=%25B%20%25e.%20%25Y>

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

Transportation Sector

8. *August 13, Evening Standard (London)* — **Grounded: BA has suspended flights to Saudi Arabia.** British Airways on Wednesday cancelled flights to Saudi Arabia amid fears of a terrorist attack. **All flights to Riyadh and Jeddah, a total of four to each destination every week, were suspended indefinitely amid fears that groups linked to al Qaeda could use a shoulder-mounted rocket launcher against a British plane.** The possibility of cancelling scheduled flights to other destinations, especially in the Middle East, has not been ruled out. The dramatic development came amid heightened tensions in Saudi Arabia where a terror cell of at least 10 militants is on the run after a shoot-out involving special forces and a helicopter gunship on Sunday in the capital Riyadh. A Department for Transport spokesman said: "There is credible intelligence of a serious threat to UK aviation interests in Saudi Arabia."
Source: <http://www.thisislondon.co.uk/news/articles/6207248?source=PA>

9. *August 13, Associated Press* — **Nuclear detectors for major port. Europe's busiest seaport will be equipped with new radiation detection equipment to intercept illicit shipments of nuclear material.** Energy Secretary Spencer Abraham was expected to join Dutch officials Wednesday at the international seaport in Rotterdam to announce the agreement, which clears the way for deploying both fixed and hand-held devices to monitor cargo going through the port. The U.S. Energy Department will provide the equipment, which is expected to begin arriving within a few months, and conduct training, officials said. **The Rotterdam port, a vast maze of docks and container vessels, handles more than 300 million metric tons of cargo annually. Thousands of commercial ships pass through the port, many of them hauling cargo from the Middle East and other regions of the world destined for the United States.** Security officials have long worried about terrorists using container shipments to hide nuclear material that could be used to make a dirty bomb, which uses conventional explosives to spread radiation, or conceal an actual nuclear device.
Source: <http://www.cnn.com/2003/WORLD/europe/08/13/rotterdam.nuclear.ap/index.html>

10. *August 13, WXIA-TV Atlanta* — **K-9s take bite out of terrorism.** MARTA riders can expect to see bomb-sniffing dogs as they arrive and depart from the Hartsfield Atlanta International Airport rail station. **In a landmark deal between the federal government and MARTA, Atlanta's public transit system, the K-9s will be brought in to provide additional security for MARTA trains at the airport. The explosives detection team -- comprised of K-9s and their handlers -- is specially trained by the Transportation Security Administration (TSA).** TSA officials say that since the September 11 attacks, the ranks of bomb-sniffing dogs at U.S. airports have doubled. The total number is expected to quadruple by the end of 2003. **Thus far, the TSA-certified K-9s have secured airplanes, screen baggage areas and patrol parking lots at the nation's airports.**
Source: http://www.11alive.com/news/news_article.aspx?storyid=35254

11. *August 12, Reuters* — **Taiwan seizes chemical cargo from N. Korean ship. Taiwan has seized 158 barrels of chemicals from a North Korean ship for inspection on a tip-off that the chemicals may be dangerous, a customs official said on Tuesday.** The North Korean ship, Be Gae Bong, was allowed to leave for Pyongyang after unloading the chemicals at Taiwan's largest port, Kaohsiung, late on Monday, said a customs official in the southern port city. The ship had arrived from Bangkok. **"We suspect the chemicals carried by the North Korean ship are dangerous and are holding the 158 barrels for inspection," the official said by telephone. He declined to give more details. The state-run Central News Agency said Taiwanese authorities boarded the ship last week on a tip-off it was carrying substances that can be used for "military purposes."** The United States, which pushed other nations to do more to prevent trade in weapons of mass destruction, hailed the Taiwanese move. The United States, Japan and South Korea will meet in Washington this week to prepare for wider talks on North Korea's suspected nuclear weapons program that could take place later this month in Beijing.

Source: <http://www.nytimes.com/reuters/international/international-taiwan-korea-ship.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

12. *August 13, Washington Post* — **WHO urges end to use of growth promoters. The World Health Organization (WHO) will recommend Thursday that nations phase out the use of antibiotic growth promoters in animal feed, saying the move will help preserve the effectiveness of antibiotics.** Based on a study of Denmark's experience following a voluntary ban on antibiotic growth promoters, WHO concluded that under similar conditions the use of low-dosage antibiotics "for the sole purpose of growth promotion can be discontinued." **WHO's findings and recommendation do not require nations to act.** But they will add to the growing movement to stop routine use of antibiotics on farms. There were negative effects from the ban on antibiotic growth promoters, the cost of producing pigs rose by about 1 percent, and the use of antibiotics to treat sick animals increased. But even with that increase, the amount of antibiotics used on Danish farms fell by about 50 percent after the ban went into effect. The report also found the amount of resistant bacteria in pork and chicken declined. In chicken, 60 percent to 80 percent of birds had bacteria resistant to three widely used antibiotics before the ban; afterward 5 percent to 35 percent of birds had resistant bacteria. A similar decline was found in pigs.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A51996-2003Aug 12.html>

13. *August 13, Associated Press* — **A new concern: agro-terrorism. Beginning this fall, all U.S. border inspectors will be trained to look for signs of "agro-terrorism", the deliberate importation of pests or plant and animal diseases, the head of customs and border protection said Tuesday. Currently about 2,000 of the agency's 18,000 border agents are**

trained to look for suspect crops or livestock, U.S. Customs Commissioner Robert Bonner said. Those inspectors were with the U.S. Agriculture Department before March 1, when Congress created customs and border protection as part of the new Department of Homeland Security. Beginning in October, the agency will expand training for new inspectors to cover agriculture, including agro-terrorism as well as pests or diseases that might be imported accidentally. In addition, agents already working the border will be "cross-trained" by other agents. **For example, agents with expertise in agriculture will train inspectors with expertise in immigration law and vice versa. The effects of agro-terrorism could be devastating,** Bonner said. For example, mad cow disease could cost American farmers millions of dollars if it were ever to enter the country.

Source: http://seattlepi.nwsourc.com/local/134794_agroterror13.html

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

Food Sector

14. *August 12, Wine Spectator* — **New U.S. security regulations could restrict wine imports. Regulations in the works at the U.S. Food and Drug Administration (FDA) could hamstring the market for high-end foreign wines in the United States, limiting consumer choice, according to importers and retailers. The regulations are being developed in accordance with the Bioterrorism Act of 2002.** As initially devised, the FDA regulations could affect any importer that currently purchases wine through the gray or parallel market, a source of small-production bottlings. The proposed regulations would require importers to file a prior-notification form that, among other information, includes the registration number of the wine's producer.

Source: <http://www.winespectator.com/Wine/Daily/News/0.1145.2162.00.html>

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

Water Sector

Nothing to report.

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

Public Health Sector

15. *August 12, Associated Press* — **Panel advises against smallpox shots. Despite worry about the possibility of a terrorist attack using smallpox, a panel of scientists is recommending that members of the general public not get vaccinated against the disease unless they are part of a carefully monitored research study.** The Institute of Medicine committee cited potential risks from the vaccine, for those receiving it as well as people with whom they have close contact and was sending its recommendation to the U.S. Centers for Disease Control and Prevention (CDC) on Tuesday. As part of the preparation for a bioterror attack, the committee said, CDC should help create registries of health care workers and others who have been vaccinated, including former members of the military and reservists. Those people could help organize a prompt response to a bioterror attack, said the panel.

Source: <http://www.cnn.com/2003/HEALTH/08/12/smallpox.vaccine.ap/>

16. *August 11, University of California San Francisco* — **Malaria's cycle. In a finding that could enhance scientists' ability to develop and test drugs and vaccines to treat the most common and lethal form of malaria, a University of California team has identified the genetic activity at a key stage of development in the parasite Plasmodium falciparum.** The study revealed a high percentage of genes were expressed at the critical stage in the parasite's life cycle. The analysis showed that the pattern of gene expression was unique, with most genes expressed only once during the stage, and in a certain order, for a continuous cascade of gene expression. The discovery of the pronounced level of activity, in which a gene is transcribed into messenger RNA on the path toward producing a protein, points to numerous new potential targets for drug and vaccine therapy. **In addition, the revelation that the genes were expressed in a relatively rigid pattern suggests a possible vulnerability in the organism's manufacturing process.** Normally, unicellular organisms that cause disease are dynamic capable of shifting their patterns of gene expression in response to environmental conditions. The expression pattern seen in Plasmodium falciparum suggests that a relatively small number of transcription factors could regulate the entire cascade.

Source: http://www.eurekalert.org/pub_releases/2003-08/uoc--srg08110_3.php

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

Government Sector

17. *August 14, Washington Post* — **Tapes show suspect talked about downing U.S. airliner. An alleged British arms smuggler was ordered held without bail in New Jersey Wednesday, August 13, on charges that he sold a Russian shoulder-fired missile to federal agents posing as terrorists, who told the man that they intended to use the weapon to shoot down a U.S. commercial airliner.** Hemant Lakhani, 68, described by one U.S. prosecutor as a "significant international arms dealer," was the main target of a complex, 18-month sting by U.S., British and Russian law enforcement authorities using undercover officers, secret videotapes and a dummy missile to fool Lakhani into thinking he was dealing with real terrorists, officials said. British Airways, in response to a different plot uncovered in Saudi Arabia, announced today that it was suspending flights to Riyadh due to concerns about the risk of a terrorist attack. **Two other men charged in connection with the case are alleged to have helped arrange financing for the deal.** Moinuddeen Ahmed Hameed of Malaysia was ordered held without bond in Newark federal court on charges of operating an unlicensed money transmitting business. Yehuda Abraham is scheduled to be arraigned Wednesday in Manhattan on money-laundering charges.

Source: http://www.washingtonpost.com/wp-dyn/articles/A54129-2003Aug_13.html

18. *August 13, The Seattle Times* — **Two Pakistani men arrested at Sea-Tac; one man's name on terror list. Two Pakistani men are being held in Seattle after an airline employee at Seattle-Tacoma International Airport found one of their names on a terrorism-related no-fly list Saturday night.** One of the men, 36, carrying a British Columbia driver's license, paid cash for a one-way ticket to New York's John F. Kennedy International Airport. After the airline employee called 911, the man left the counter, abandoning his ticket. The other man, 29, who had a New York driver's license, also paid cash for a one-way ticket to Kennedy Airport

on a different airline, police reports show. **Port police detained both men, then turned them over to the FBI. They are being held on immigration violations as part of a growing international investigation being conducted by the FBI's Joint Terrorism Task Force and the Bureau of Immigration and Customs Enforcement (BICE).** "We are aware of the situation," said Assistant U.S. Attorney Todd Greenberg, a counter-terrorism prosecutor in Seattle. "We are expending all available resources toward the investigation." The two men both were using Pakistani passports and reportedly were seen together at the airport earlier in the evening. **After their arrests, the men told investigators they paid to be smuggled into Blaine from Canada last month, two sources said.**

Source: http://seattletimes.nwsourc.com/html/localnews/2001493387_terror13.html

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

Emergency Services Sector

19. *August 13, Government Technology* — California launches satellite pilot. Gov. Gray Davis signed legislation that creates a pilot emergency satellite technology program, using GPS and GIS technologies to respond to California emergencies. "We rely on a strong, working communication system during any emergency crisis," Davis said. "This program will allow us to explore state-of-the-art technology." AB 1509 by Assembly Member John Benoit requires the Office of Emergency Services to conduct a demonstration project on the use of satellite devices that use GIS and GPS technologies in the management and deployment of mobile emergency response equipment and personnel. **In an emergency or the aftermath of a disaster, the proper use and deployment of emergency response personnel and vehicles is critical in mitigating the effects of the disaster.** New technologies, based on GPS technology, have the advantage of being independent of terrestrial systems that may have been damaged by the disaster event or overburdened with voice traffic.

Source: <http://www.govtech.net/news/news.php?id=2003.08.12-63702>

20. *August 12, Milwaukee Journal Sentinel* — Terrorism drill to simulate stadium attack. **Officials in Milwaukee, WI, will test their ability to respond to a biological or chemical attack at a ball game attended by 15,000 to 20,000 people on Wednesday.** The drill begins around 9 a.m. with the mock attack at Miller Park. To simulate the mayhem and multiple problems that emergency workers likely would face, planners have scripted sideshows. **A bomb will be simulated with a smoke grenade, and law enforcement will be told that long-sought fugitives are running through the crowd and must be caught.** Several dozen volunteers will play victims who need to be assessed and decontaminated at emergency triage tents at the ballpark. In the afternoon mock victims will start arriving at Froedtert Memorial Lutheran Hospital, Columbia St. Mary's, and West Allis Memorial Hospital. **People from other area hospitals will be on hand to observe and critique the hospital's performance and give feedback on how to improve,** said Froedtert spokesman Mark McLaughlin.

Source: <http://www.jsonline.com/alive/news/aug03/161824.asp>

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

Information and Telecommunications Sector

21. *August 13, Government Computer News* — **NIST releases guidelines for IT security metrics.** The National Institute of Standards and Technology (NIST) has released its final version of guidelines for developing metrics to help ensure agencies meet IT security requirements. Metrics—measurable standards—monitor the effectiveness of goals and objectives established for IT security. They measure the implementation of security policy, the results of security services and the impact of security events on an agency's mission. **The publication uses the critical elements, and security controls and techniques laid out in an earlier NIST publication, 800–26, Security Self–Assessment Guide for IT Systems.** NIST Special Publication 800–55, Security Metrics Guide for IT Systems is available online [http://csrc.nist.gov/publications/nistpubs/800–55/sp800–55.p df](http://csrc.nist.gov/publications/nistpubs/800–55/sp800–55.pdf)
Source: http://www.gcn.com/vol1_no1/daily–updates/23108–1.html
22. *August 13, eWEEK* — **Worm: long wait for fix. Computer users were scrambling Wednesday, August 13, for alternate fixes for the havoc wreaked by the Blaster worm as many people were unable to reach Microsoft Corp.'s main patch download site.** The Windows Update Web site was extremely sluggish Tuesday and Wednesday, and some users reported being unable to reach the site at all. The Blaster worm, also known as LoveSan, began infecting Windows NT, 2000 and XP machines Monday and continues to spread rapidly. The worm exploits a vulnerability in the Windows RPC (Remote Procedure Call) service and uses a lot of bandwidth scanning for other vulnerable machines once it has infected a PC. Microsoft made a patch available for the flaw in mid–July. **Blaster is also causing service problems on Comcast Corp.'s cable modem network. Several Comcast customers said their service had been down for extended periods during the last couple of days** and that Comcast officials said Blaster was to blame.
Source: <http://www.eweek.com/article2/0,3959,1218982,00.asp>
23. *August 12, National Journal* — **Industry comments on antiterror liability protection rule. A coalition of trade associations on Monday, August 13, filed comments on a Department of Homeland Security measure to protect security technology providers from liability if their products or services fail to prevent terrorist attacks.** The coalition, which included the Information Technology Association of America and National Association of Manufacturers, endorsed a proposal to distinguish between "qualified anti–terrorism technologies" and "approved products for homeland security." They cautioned that the proposed five– to eight–year limits on products exempt from legal liability under such designations could discourage the development of anti–terrorism technologies and said the regulations should be retroactive, with shorter review periods. The group also called for an extension of the immunity from lawsuits and a broadening of designations to include more products and services, and they are seeking greater confidentiality about their security roles and more financial support from the government if they are successfully sued for breaches in security.
Source: <http://www.govexec.com/dailyfed/0803/081203td2.htm>

Current Alert Levels	
 AlertCon: 3 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 3 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), 137 (netbios-ns), 80 (www), 54112 (----), 37852 (linkproof), 4244 (vrml-multi-use), 1433 (ms-sql-s), 1080 (socks), 139 (netbios-ssn), 23 (telnet) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

24. *August 13, Sun–Sentinel* — **Flood watch announced for coastal South Florida. The National Weather Service in Miami, FL, on Wednesday, August 13, announced a flood watch for the eastern coastal areas of Broward, Miami–Dade and Palm Beach counties that will remain in effect until 11 a.m. Thursday.** The announcement was fueled by a tropical system moving in from the Bahamas that threatens to bring 1 to 3 inches of rain and gusty winds as strong as 30 mph to South Florida, the National Weather Service said. **The approaching system had nothing to do with at least two waterspouts that formed on Biscayne Bay near Miami Beach on Tuesday morning,** weather officials said. One of the spouts briefly touched down near 75th Street and Collins Avenue, flipping a lifeguard stand and uprooting a couple of trees, officials said. The other dissipated before coming ashore. Waterspouts essentially are tornadoes that form over water. Because one made contact with land, the weather service will classify it as a weak F–0 tornado, meteorologist Jim Lushine said. Source: <http://www.sun-sentinel.com/templates/misc/printstory.jsp?slug=sfl-sweather13aug13§ion=/printstory>

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

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 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.