



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 22 September 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)
www.whitehouse.gov/homeland

Daily Overview

- The Philadelphia Daily News reports a consumer representative for one of the nation's big credit-reporting bureaus has been indicted by a federal grand jury for allegedly taking "cash payoffs" to improve people's credit ratings. (See item [6](#))
- The Beaufort Gazette reports access to false driver's licenses is a growing problem, and currently, South Carolina has no system to verify that people applying for a driver's license have valid Social Security numbers. (See item [8](#))
- The Department of Homeland Security says a massive response is ready to help hurricane victims as Secretary Ridge visits impacted areas. (See item [27](#))
- CERT/CC has issued an Advisory concerning a vulnerability in the buffer overflow in Sendmail. (See item [33](#))

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. *September 20, Associated Press* — **Effects of Hurricane Isabel.** The huge storm knocked out electrical service for about 6 million homes and businesses from North Carolina's Outer Banks north to New York, and the extent of damage combined with debris-blocked streets

overwhelmed utility crews. **An estimated 2.8 million were still blacked out Saturday, September 20. At least 27 deaths had been blamed on the storm, 16 of them in hard-hit Virginia.** North Carolina, Virginia and Maryland had been declared federal disaster areas. **Virginia was hit hardest by the loss of electricity. The state's dominant provider, Dominion Virginia Power, still had about 1.2 million homes and businesses in the dark Saturday,** said Jimmy Staton, a company vice president. The North Carolina National Guard hoped to airlift Salvation Army mobile kitchens to Buxton on Hatteras Island, which was cut off from the mainland because the ocean cut through part of the highway, and to Ocracoke Island, NC. However, that plan had to be dropped Saturday, said Salvation Army spokesman John Edwards. The kitchens were too heavy for the helicopters supplied for the mission and they will have to be shipped out on barges, he said. **Federal emergency officials warned of new flooding as runoff from the storm pours into streams.**

Source: http://abcnews.go.com/wire/US/ap20030920_972.html

2. *September 19, Reuters* — **Isabel shuts Dominion's Virginia nuclear units. As electrical power to its cooling pumps dropped off amid the fury of Hurricane Isabel, Dominion Resources Inc. shut both generating units at its Surry nuclear power plant in Virginia, the company said Friday, September 19.** "Surry Units 1 and 2 were taken off line manually after we lost the electrical transformer that provides the energy for cooling pumps to move water from the James River to our cooling system," Dominion's spokesperson Jim Norvelle told reporters in a teleconference. **It was not yet known why the transformer failed, nor did the company know when the nuclear units would return to service.** The two-unit, 1,624 megawatt Surry plant near Gravel Neck, VA, was along the path Isabel cut across the state late Thursday after blowing ashore in neighboring North Carolina. With more than 80 percent of its 2.2 million customers still without power due to Isabel, however, Dominion's need for generation has been significantly reduced, the company said.

Source: http://biz.yahoo.com/rm/030919/utilities_dominion_surry_4.html

3. *September 17, Technology Daily* — **Federal officials detail response to August blackout.** House lawmakers on Wednesday, September 17, heard from federal critical infrastructure experts on what happened during the August power outage in parts of the United States and Canada. Robert Liscouski, the Department of Homeland Security's (DHS) assistant secretary for infrastructure protection, described how his directorate responded to the blackout, its first major event of that type during a hearing of the House Homeland Security Subcommittees on Cybersecurity, Science, and Research & Development, and Infrastructure and Border Security. **During the blackout, Liscouski said, the infrastructure coordination division focused on the outage itself and the impact on infrastructures, while the department's cyber division "looked into the possibility that the blackout might have been caused by a cyber attack."** Officials analyzed previous and current intelligence traffic and coordinated with the intelligence community and law enforcement to see if the cause was "attributed to a bad actor," Liscouski said. The Homeland Security Operations Center coordinated communications between state and local "first responders" to emergencies and the federal government. **Liscouski said the ability to communicate with the infrastructure sectors was in place, though no information on threats was sent.**

Source: <http://www.govexec.com/dailyfed/0903/091703tdpm1.htm>

4.

September 16, Associated Press — **Nuclear power plant rechecking employee backgrounds.** Officials at the Millstone nuclear power complex in Waterford, CT, have begun checking the criminal backgrounds of workers who have "unescorted" access to the facility and whose histories have not been recently reviewed. **Renewed orders by the Nuclear Regulatory Commission (NRC) prompted the background checks.** The FBI is helping with the new round of checks, said a spokesperson for Dominion Nuclear Connecticut, which owns the three-plant complex, one of which has been permanently shut down. Dominion recently dismissed five nuclear plant workers in Virginia after FBI checks showed misdemeanor arrest records. **The NRC requires nuclear facilities to check the criminal backgrounds of their workers at the time of hiring and every five years afterward. But the five-year checks had largely been ignored until the commission issued a fresh directive in January as part of a larger effort to protect nuclear sites from terrorist attacks.** "Every five years they're supposed to go back and do this review," said Neil Sheehan, a spokesperson for the commission. "They were supposed to be doing these updates, and they weren't. It's just part of security in a post 9-11 environment."

Source: <http://www.newsday.com/news/local/wire/ny-bc-ct--millstone-b-ackgro0916sep15.0.5317830.story?coll=ny-ap-regional-wire>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

5. *September 20, Sydney Morning Herald (Australia)* — **Australian banks resist device aimed at foiling account hackers.** Australia's estimated 7.2 million registered internet bankers are being left open to increasingly numerous and sophisticated scams as banks fall behind on security. "Security mechanisms are not keeping up with fraud," said Tommy Viljoen, head of security at Deloitte Australia. **This week a British security firm, mi2g, listed Australia's five largest banks among 13 world banks hit by so-called "phishing" scams, whereby online bankers are duped into giving their passwords and PINs to scammers via fake websites. The big five banks have faced at least 10 such attacks this year, but are still rejecting security technologies that could stop it.** They still rely on a password and PIN entered via the keyboard – "the weakest level of authentication," Viljoen said. By comparison, online customers of ABN AMRO's retail banks in Holland are being issued with a slim, calculator-like device dubbed an e.identifier that is used along with the customer's normal card and PIN. Tony Burke, director of the Australian Bankers Association, says customers have historically rejected services that favoured security over convenience.

Source: <http://www.smh.com.au/articles/2003/09/19/1063625219332.html>

6. *September 19, Philadelphia Daily News* — **Fourteen tied to a scam to falsely alter credit histories. A consumer representative for one of the nation's big credit-reporting bureaus was indicted Friday by a federal grand jury in Philadelphia, PA, for allegedly taking "cash payoffs" to falsely improve people's credit ratings.** Banks, retailers and mortgage firms lost more than \$500,000 after those who paid the bribes failed to pay the debts they had accumulated after their credit histories were rewritten. Terri Whatley, who worked for several years in the TransUnion office in Delaware County, PA, has agreed to plead guilty later to computer fraud. TransUnion, based in Chicago, discovered the scam, reported it to federal authorities, and cooperated "extensively" with a probe by Secret Service agents, said U.S. Attorney Patrick L. Meehan. **Whatley allegedly took payoffs from 13 people "to alter their computerized credit histories." Whatley lowered or removed debts owed, and erased unfavorable credit information from their credit histories,** said Assistant U.S. Attorney Paul Gray.

Source: <http://www.philly.com/mld/dailynews/news/local/6808397.htm>

7. *September 19, Wired* — **Windows to power ATMs in 2005. By 2005, 65 percent of bank ATMs (not including free-standing machines in places like convenience stores and casinos) in the United States will use a stripped-down version of Windows.** About 12 percent of the machines will use the operating system by the end of this year, according to Gwenn Bezar, an analyst at market researcher Celent. Bezar asked 20 of the top 60 banks in the country about their plans to upgrade ATMs. He concluded the banking industry is ready to scrap IBM's OS/2 operating system, which powers most ATMs today. They would prefer Windows, a platform they consider "open" in that it is compatible with their internal corporate networks. Also, it's so ubiquitous that they can add features to all their ATMs without having to write multiple pieces of code for different machines. **While there are concerns about cyberattacks, the reason bank robbers still tend not to focus on ATMs to do their dirty work is that ATMs have almost never fallen prey to malicious hacking.** Roughly \$1 trillion of ATM withdrawals will take place this year, with losses of only \$15 million. **The losses are largely attributed to fraud — stolen ATM cards or bank insiders in charge of restocking the machines with cash.**

Source: <http://www.wired.com/news/technology/0,1282,60497,00.html>

8. *September 18, The Beaufort Gazette (SC)* — **Access to false driver's licenses a growing problem. At present, the South Carolina Division of Motor Vehicles (DMV) has no system to verify that people applying for a driver's license have valid Social Security numbers, even though a Social Security number is one of several pieces of identification that U.S. citizens need to apply for a license in the state.** Beth Parks, a spokesperson for the DMV, said the agency plans to get computer software that will help it check for valid Social Security numbers, perhaps as early as the end of the year. "Currently, the verification for the Social Security card is done manually by the clerk," she said. "The safety features we use right now are on the card itself." As of June, more than 20 state DMVs have such Social Security number verification systems, according to Jason King, spokesperson for the American Association of Motor Vehicle Administrators, a non-profit information clearinghouse for DMV offices. **The systems cross reference with the Social Security Administration database to match names with valid numbers. Proponents say that the systems help guard against identity theft by**

making it harder to apply for licenses -- and by extension a false identity -- using stolen or made-up social security numbers.

Source: http://www.beaufortgazette.com/local_news/story/2878861p-2654178c.html

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

Transportation Sector

9. *September 18, Associated Press* — **United Airlines to launch low-cost carrier.** United Airlines said last Wednesday it will launch a low-cost carrier from its Denver, CO, hub in February, flying to destinations in the Southwest and Southeast before expanding service nationwide. **The bankrupt airline's goal is to compete better with discount carriers such as Frontier, JetBlue and Southwest, who've grown quickly amid the economic downturn.** "Customers want low fares, low fares, low fares, and they're not willing to pay extra for a free meal," said Sean Donohue, vice president for the new operation. **The new airline, which has not yet been named, will initially fly to Reno and Las Vegas, Nevada; Phoenix, Arizona; New Orleans, Louisiana and Tampa, Florida. Tickets will go on sale in November.** Since filing for Chapter 11 last year, United has restructured its labor contracts -- saving \$2.6 billion a year through 2008 -- and its airplane leases. The Illinois-based airline is trying to end years of heavy losses and compete better.

Source: <http://www.cnn.com/2003/TRAVEL/09/18/bi.united.lowcost.ap/index.html>

10. *September 18, Associated Press* — **Fort Myers airport workers arrested on identity fraud charges. Eight employees of Southwest Florida Regional International Airport are facing federal identity fraud charges, the U.S. Attorney's Office announced Thursday. The workers are not believed to be involved in terrorism, but gave false Social Security numbers and resident alien cards when they applied for work at the airport, U.S. Attorney Paul Perez said in a statement.** The arrests were part of "Operation Tarmac," which has targeted airport employees working in restricted portions of the airport. The five men and three women in Thursday's case worked in a variety of jobs, including custodian and construction workers, with access to the tarmac, baggage screening areas and cargo storage facilities. They each face up to five years in prison and a \$250,000 fine if convicted. Airport officials had no comment on the arrests.

Source: <http://www.sun-sentinel.com/news/local/florida/sfl-918airportidfraud.0,1032942.story?coll=sfla-news-florida>

11. *September 18, Mercury News (CA)* — **JetBlue admits it shared data. JetBlue Airways has apologized for disclosing five million of its passenger records to a military contractor.** "This was a mistake on our part and I know you and many of our customers feel betrayed by it," said David Neeleman, chief executive of the Forest Hills, NY, airline, in an apology e-mailed to JetBlue customers. The airline, which uses Oakland International Airport as its Bay Area hub, said it supplied the passenger records more than a year ago to Torch Concepts, a Defense Department contractor based in Huntsville, AL, according to Neeleman's note. **He said the data included passenger names, addresses and phone numbers. It remained unclear Friday whether all the company's passenger records were disclosed as well as whether JetBlue was paid for them. The problem was that Torch then used the information in ways JetBlue didn't authorize, Neeleman said. By apparently comparing JetBlue's data**

with information in commercial databases, Torch was able to obtain passenger Social Security numbers, travel histories and even incomes, according to a report it prepared for a federal Department of Homeland Security symposium in February.

Source: <http://www.siliconvalley.com/mld/siliconvalley/6818691.htm>

12. *September 17, WSFA-TV (Montgomery, AL)* — Tanker truck spills dangerous chemical. It was touch-and-go last Wednesday after a tanker truck full of dangerous chemicals overturned in Lowndes county, Alabama. The driver of the truck was killed. Before it was all over, people had been evacuated, the electricity had gone out, and the truck driver had been killed. WSFA was among the first to arrive at the scene on Wasden Road in the Hope Hull community. The Montgomery Fire Department's hazardous materials unit arrived a short time later at 4:45 p.m. They were there to stop a tanker truck from leaking Sodium Hydroxide. "It was not a large release, but there were chemicals coming from the tanker," said Lowndes County EMA Director Fannie Davis. Sodium Hydroxide is harmful if inhaled or touched. "It's a very strong bleach that's used to disinfect, but it's much stronger than the household kind that we use," David explained. The truck was from Slay Transportation in Pensacola, Florida. The driver remained unidentified Wednesday night. When the truck ran off the road, it also hit a power pole, causing at least 30 homes and businesses in the area to lose electricity. As many as a dozen homeowners were evacuated as Hazmat teams patched the leak.

Source: <http://www.wsfa.com/Global/story.asp?S=1447459&nav=0RdEI3XG>

13. *September 17, Associated Press* — American Airlines flight gets close to military planes. An American Airlines jet plunged about 100 feet to avoid military aircraft in an incident over Oklahoma. Fort Worth-based American reported September 17 that three flight attendants and two passengers were slightly hurt. The incident happened about 15 miles northwest of Tulsa on a flight from Oklahoma City to St. Louis. Airline spokesperson Julia Bishop-Cross says Flight 490 continued to St. Louis, where it landed safely. The jet was at about 29,000 feet when the airplane's collision alarm system went off. The pilot descended, then saw three or four jet fighters. The Federal Aviation Administration is investigating. About 70 aircraft from Seymour Johnson Air Force Base in North Carolina flew to Tinker Air Force Base in Oklahoma yesterday afternoon. The aircraft were moved to Tinker to avoid Hurricane Isabel.

Source: http://www.news24houston.com/content/top_stories/default.asp?ArID=14978

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

Postal and Shipping Sector

14. *September 18, DM News* — USPS has time for reform. Postal reform is urgent but time remains for Congress, labor, and postal management to design the solutions that will make the U.S. Postal Service (USPS) viable for the next two decades, a member of the presidential reform commission told lawmakers Wednesday. James A. Johnson, who co-chaired the commission, spoke before the Senate Governmental Affairs Committee at a hearing in which lawmakers addressed postal reform for the first time since the reform commission issued its recommendations in July. Johnson reiterated the commission's conclusion that postal reform is needed and that Congress must act. However, thanks largely

to a bill this year that reduced the postal service's liability to the Civil Service retirement fund, and also in part to the USPS transformation plan, the postal service is in better shape financially than it was just a year ago, he said. Nevertheless, budding financial problems before the USPS will grow unless reform is enacted, Johnson said. The reform commission's recommendations represent best practices that can be put into place regardless of future developments.

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=2502_8

15. *September 18, Associated Press* — **Authorities probe hoax calls to UPS. Law enforcement authorities on Wednesday were investigating a pair of threatening phone calls that forced a UPS cargo plane to make an emergency landing.** The calls turned out to be a hoax. The package the anonymous caller referred to contained only bottled water, fabric softener, cabbage, cheese, and marijuana, said Mark Giuffre, public relations manager for UPS. The caller provided the same package tracking number in both calls, but it was not immediately clear if the calls came from the same person, said Giuffre. **Giuffre noted that the company can provide investigators a lot of information about the packages it ships. It tracks the originating address, the intended recipient and every truck and plane in between. Most drivers follow the same routes daily and often are acquainted with their pickup and delivery locations as well. "Anonymity is very difficult," he said. No arrests had been made Wednesday, but the FBI was investigating and had a few leads, said FBI spokesperson Susan Herskovits.**

Source: http://www.azcentral.com/arizonarepublic/local/articles/0918_phxplane.html

[[Return to top](#)]

Agriculture Sector

16. *September 19, High Plains Journal* — **Canadian live cattle import rules. U.S. Department of Agriculture (USDA) Secretary Ann Veneman says the USDA will publish within "a matter of weeks, not months" a proposed rule to allow some Canadian live cattle to enter the U.S. The rule, which the USDA will publish in the Federal Register, is the first step in a process that USDA and U.S. industry officials expect will take several months.** The U.S. banned all Canadian beef and cattle in May when a case of bovine spongiform encephalopathy (BSE) was discovered. The USDA eased the ban on some boneless beef products on August 8, but said it would not be able to do the same for live cattle until the department went through a full rule-making process. USDA Undersecretary Bill Hawks, head of USDA's marketing and regulatory programs, said recently, "Under a normal rule-making process, I would say that it will take some several months to address that." When the proposed rule is published, Bobby Acord, administrator of USDA's Animal and Plant Health Inspection Service, said it will be straightforward. **Cattle under 30 months of age will be allowed in, he said, and stressed there will not be much more to it. The USDA considers only Canadian cattle under 30 months old to present no risk of transmitting BSE.**

Source: <http://www.hpj.com/testnewstable.cfm?type=story&sid=9850>

17. *September 18, Edmonton Sun* — **Clubroot fungus threatens crops. The Alberta, Canada, government has launched an investigation after a highly destructive fungal disease that decimates crop growth was found in Alberta canola for the first time. Clubroot, which**

attacks the roots of crops including canola, cabbage, and cauliflower, can be spread from field to field in water, soil, and manure, and contaminates the earth for up to 18 years.

There is one confirmed and several probable cases in Alberta, but officials said it's too early to say how many farms have been infected. "It's a disease that could be very serious if left untreated. We are getting very concerned about it," said Alberta Agriculture cereal and oilseed specialist Jay Byer. "Anything that carries mud on the tires could conceivably spread it. This is a brand new situation for us, but we are hoping and expecting it to be very isolated." **In order to control clubroot, infected farms will have to maintain a seven-year rotation between vulnerable crops, control certain weeds, and ensure any people or equipment leaving an infected field are free of contaminated soil.** They will also have to avoid applying contaminated manure from animals fed the crops and use a fungicide.

Source: <http://www.canoe.ca/EdmontonNews/es.es-09-18-0028.html>

18. *September 18, Daily Times* — **Farmers race to harvest before hurricane. Farmers were rushing Wednesday to harvest their crops earlier than usual to salvage what they can before Hurricane Isabel is expected to sweep through Delaware and the Maryland Eastern Shore Thursday.** Only 36 percent of the corn in Delaware is mature enough for harvest, according to Monday's weekly crop report by the state Department of Agriculture. Farmers are using their judgment to determine whether to harvest their corn even if it isn't dry enough for storage. Grain elevators prefer the corn moisture level to be about 15 percent, compared with the 20 percent to 30 percent moisture in most corn now, University of Delaware Cooperative Extension agents said. Farmers who have corn with high moisture levels will likely be penalized by grain elevator operators. Perdue Farms spokeswoman Tita Cherrier said the poultry and grain dealer has increased premiums, put staff on overtime, and decreased discounts to help bring in the corn before the hurricane hits.

Source: <http://www.dailytimesonline.com/news/stories/20030918/localnews/279638.html>

19. *September 18, Reuters* — **Hurricane shuts down pork operations. Hog and pork operations in North Carolina and Virginia suspended operations on Thursday in preparation for Hurricane Isabel, which reached the East Coast late Thursday morning.** "We are in fact shut down," said Charlie Arnot, spokesman for Premium Standard Farms, which has a 17,100-head-per-day hog slaughter plant at Clinton, North Carolina. "The anticipation is that we will be back up Friday." Officials at Smithfield Foods Inc. said their pork plants in North Carolina and Virginia were probably shutdown, although they said it has been difficult reaching officials at those plants. The three affected plants have a combined estimated daily slaughter of 50,300 head. Shipping of hogs from farms to pork plants was suspended on Thursday by both companies. **In 1999, high winds and flooding from Hurricane Floyd killed more than 30,000 hogs, 2.5 million poultry, and hundreds of cattle.**

Source: <http://www.forbes.com/markets/commodities/newswire/2003/09/18/rtr1085395.html>

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

Food Sector

20. *September 18, Associated Press* — **USDA finds less E. coli in beef samples. After pushing meatpackers to update plans to prevent ground beef contamination, U.S. Department of Agriculture (USDA) inspectors are seeing a drop-off in the number of samples tainted**

with E. coli. Elsa Murano, undersecretary of food safety, said the department has spent the last year getting 1,000 meat plants, from very small to large, to improve efforts to keep meat free of the potentially deadly bacteria by adding steps like hot water rinses and organic acid washes to processing. **As a result, she said, inspectors found 0.32 percent of 4,432 samples of hamburger meat tested positive for E. coli from January to August this year. That compares to 0.78 percent of samples testing positive for the same period in 2002 and 0.84 percent in 2001.** The decline is significant when considering that the agency switched to using a sensitive test for the bacteria that can detect a single germ of E. coli in a 325-gram sample of hamburger, Murano said. Department inspectors plan to review 1,500 other plants by next year. Source: <http://www.billingsgazette.com/index.php?id=1&display=rednews/2003/09/18/build/health/ecoli.inc>

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

Water Sector

21. *September 19, Washington Post* — **Fast-drained water reserve in Virginia. About 11 p.m. Thursday, as Hurricane Isabel approached in full force, all four of the Fairfax County, VA, water purifying plants lost power. The utility's sparse reserves, calculated at about four hours of use, quickly dwindled. And, its power backups were too meager to make up the loss.** By 4 a.m., crews dispatched to check the gauges at storage tanks reported troubling low pressure. **It was a rare but foreseeable electrical coincidence that deprived more than one million Virginians of reliable drinking water and raised questions about the vulnerability of the supply system.** Although, Dominion Virginia Power had restored electricity to all four of the plants by 4:30 p.m. Friday, the utility is still urging customers to boil water for drinking and cooking until full quality tests can be completed early next week. **None of the large utilities in the Washington, DC area keeps any more than 24 hours of reserve water, representatives said.** However, a significant portion of those systems are gravity fed, meaning the water comes from elevated storage tanks and thus are not as dependent on electricity for pumping.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A33820-2003Sep 19.html>

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

Public Health Sector

22. *September 19, Reuters* — **West Nile virus and blood transfusions. With the introduction of a new test for West Nile virus this season, the risk of infection from blood transfusions is "very low but not zero," the U.S. Centers for Disease Control and Prevention (CDC) said on Thursday.** In late June, blood-banking officials began screening blood for West Nile virus. It's an effort that is paying off, CDC Director Julie Gerberding said. **"Overall the test has identified more than 600 infected units of blood, which were pulled from the blood supply."** Currently, blood-banking agencies are testing pooled blood samples taken from 6 to 16 donors. "The blood is mixed together and then tested and if the pool is found to be positive, than the individual donors are evaluated," Gerberding said. "This is a major step forward in protecting the blood supply but it is not perfect," she said. "Clinicians and public health

officials need to be on the look out for cases of fever, headache, and brain inflammation in blood transfusion recipients so we can look back and make sure an infected unit didn't slip through the cracks." **The CDC is recommending, when feasible, the screening of individual units of donated blood. "In high-risk areas, this is being done," Gerberding noted. "This is not yet possible at every donation center."**

Source: <http://asia.reuters.com/newsArticle.jhtml?type=healthNews&storyID=3470478>

23. *September 19, San Jose Mercury News* — **Flu virus to be studied as bioterror agent. Stanford University has received a five-year, \$15 million federal grant to study the possible use of the flu virus in bioterrorism.** Researchers at Stanford Medical Center will study how the immune system responds to the influenza virus, which causes the common flu. Researchers hope to improve vaccines against the virus in the event it is used as a bioweapon. Ann Arvin, a Stanford professor of immunology and pediatrics, said influenza is easily transmitted and can potentially be delivered as an aerosol for maximum exposure.
Source: <http://www.bayarea.com/mld/mercurynews/6811727.htm>
24. *September 18, Globe and Mail* — **SARS patients responded well in combination drug test. A drug cocktail shows promise in the treatment of Severe Acute Respiratory Syndrome (SARS), according to the results of a small Canadian study. Patients given a combination of interferon and steroid medications showed quicker improvement in lung function compared with those who received only steroids.** They were weaned off oxygen about a week sooner than patients who did not receive the combination therapy. The study was carried out on 19 patients in Toronto, Canada, this year during the city's second outbreak of SARS. "The data is encouraging, but it is not definitive," said one of the researchers, Mario Ostrowski, a physician at St. Michael's Hospital in Toronto. **Even so, the results are promising enough that researchers hope to do a much more extensive study if SARS makes a comeback.** Health Canada gave the green light to a larger, randomized study, but "by the time it was approved, all the cases had disappeared because the outbreak had ended," Dr. Ostrowski said. An earlier study, by Hong Kong and German researchers, also found that recombinant interferons could be helpful in treating SARS.
Source: <http://www.globeandmail.com/servlet/ArticleNews/TPStory/LAC/20030918/UDRUGM/TPScience/>
25. *September 17, CIDRAP* — **NIAID launches program to apply immunology to biodefense. The National Institute of Allergy and Infectious Disease (NIAID) Wednesday announced a new program to study the human immune response to diseases of bioterrorism and develop vaccines, drugs, and other countermeasures.** The NIAID named five Cooperative Centers for Translational Research on Human Immunology and Biodefense: Baylor Research Institute; Dana-Farber Cancer Institute; Emory University School of Medicine; Stanford University School of Medicine; and the University of Massachusetts Medical School. **The agency said it will provide about \$85 million over 4 1/2 years for the centers. "A particular emphasis of these cooperative centers will be moving new findings about immune system function out of the lab and into clinical trials,"** NIAID Director Anthony S. Fauci said. Investigators working in the new program will form a research network with a focus on the human immune system, the NIAID said. The agency noted that it is much harder to study immunity in humans than in animals because humans can't be deliberately exposed to pathogens. One aim of the new program is to develop technologies to help overcome the

obstacles to studying immune responses.

Source: http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/news/sep_1703niaid.html

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

Government Sector

26. *September 21, Milford Daily News (MA)* — **Immigrant licenses hit roadblock. A bill that would allow undocumented immigrants to obtain Massachusetts driver's licenses is inching its way through the Legislature, despite critics' concerns that the proposal poses a threat to national security and could encourage illegal immigration.** The bill's supporters, including state Rep. Deborah Blumer, D–Framingham, argue that the roads would be safer for all motorists if the state's estimated 150,000 undocumented immigrants can obtain driver's licenses and purchase car insurance. **Many other MetroWest lawmakers, however, are strongly opposed to changing the law. "That's like saying let's give robbery licenses to bank robbers because they're going to do it anyway,"** said Rep. James Vallee, D–Franklin. "If they're here illegally, they shouldn't benefit from having a license. A driver's license isn't a right. It's a privilege." **Under existing state law, an applicant for a driver's license must have a Social Security number. Undocumented immigrants can't apply for Social Security numbers, but they can obtain a taxpayer ID number. The Internal Revenue Service issues the numbers to anyone who is required to file an income tax return, but isn't entitled to a Social Security number.**

Source: http://www.milforddailynews.com/news/local_regional/immigran_tlicenses09212003.htm

27. *September 20, Department of Homeland Security* — **The Department of Homeland Security says a massive response is ready to help hurricane victims as Secretary Ridge visits impacted areas.** The U.S. Department of Homeland Security, through its Federal Emergency Management Agency, U.S. Coast Guard and other emergency response elements, is coordinating the massive Federal response to millions of citizens throughout the mid–Atlantic region impacted by Hurricane Isabel. **Homeland Security Secretary Tom Ridge said that a full range of response and recovery assets have been deployed to the disaster areas. Several thousand emergency responders are providing life–saving missions as recovery begins.** President Bush has signed disaster declarations for North Carolina, Virginia, Maryland and the District of Columbia that authorize a full range of disaster assistance to disaster victims as well as public assistance for infrastructure damages. **Secretary Ridge and Under Secretary Brown are viewing storm–damaged areas today in North Carolina and Virginia.** They are getting a first–hand look at the damage left by Hurricane Isabel and meeting with North Carolina Governor Mike Easley and Virginia Governor Mark Warner as well as members of Congress from the affected areas to discuss and coordinate federal, state and local response efforts.

Source: <http://www.dhs.gov/dhspublic/>

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

Emergency Services Sector

28. *September 18, Government Computer News* — **First responders could get access to military technologies.** State and local police, fire departments, and emergency medical services should use many of the military's advanced technologies but have no structure for taking advantage of them, Defense officials say. **A provision in the Defense Authorization Bill, if approved, would correct that, according to Pete Verga, principal deputy assistant secretary of Defense for homeland defense. "This requires the secretary of Defense to appoint a senior official to ensure the transfer of technology to first responders," Verga said.** That appointee will likely be Paul McHale, first assistant secretary of Defense for homeland defense, Verga said today before a gathering of military, civilian and industry leaders at an Army homeland defense conference. September 11, 2001, highlighted America's dire need of an integrated domestic communications system so that all National Guard, firefighters, police and other first responders can communicate at disaster scenes—from wildfires to earthquakes. Source: http://www.gcn.com/vol1_no1/daily-updates/23582-1.html
29. *September 18, New York Times* — **After pinpoint tracking, forecasting turns to intensity.** For a dozen days, Hurricane Isabel has seemingly rolled on tracks laid out by government weather forecasters. Its neatly predicted ride toward a collision with the mid-Atlantic coast reflected enormous advances in computer modeling of the atmosphere's vagaries and growing understanding of the forces that steer such giant storms. **Forecasters say a five-day tracking forecast now has the same reliability as a three-day forecast 15 years ago. But forecasters have been far less successful in predicting the strength of hurricanes, a characteristic almost as important as the storms' routes in determining their destructive potential. Better prediction of intensity is important, he said, because an increase in winds of just 20 or 30 miles per hour can vastly increase the scale of damage and threat to life.** An audacious research effort, though, has begun to probe hurricanes for clues that could improve intensity forecasts. The five-year project, by a team of several dozen government and academic researchers, has sent two specially equipped airplanes, augmenting the aircraft that routinely track all hurricanes, gathering information as they skim just above the cresting waves in clear areas between the storms' thunderclouds. Source: <http://www.nytimes.com/2003/09/18/national/18PRED.html>
30. *September 18, U.S. Department of Transportation* — **DOT responds to Hurricane Isabel.** Anticipating the threat from Hurricane Isabel and storm damage to transportation infrastructure, the U.S. Department of Transportation (DOT) last Friday activated special plans to support affected states and communities. **At 7:00 a.m. Thursday, September 18, the department planned to activate its Crisis Management Center (CMC). Drawing on expertise within the department by building on information from states and aviation, marine, rail, highway, pipeline and transit authorities, the Department of Transportation Crisis Management Center will assist the affected regions in coping with Hurricane Isabel and its effects.** Hurricane preparations and responses include repair crews being dispatched and pre-positioned at critical aviation and rail sites to quickly restore service, coordinating with the military for rescue flights, assessing needs for emergency relief, and securing the National Defense Reserve Fleet at Ft. Eustis, VA. **Among other points, on Monday, September 15, the Federal Aviation Administration (FAA) established a special hurricane position within the Air Traffic Control system to coordinate any necessary military and civil aircraft evacuations.**

Source: <http://www.dot.gov/affairs/dot11403.htm>

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

Information and Telecommunications Sector

31. *September 19, Reuters* — New worm targets Internet Explorer. Anti-virus companies warned on Thursday, September 18, of a new computer worm circulating through e-mail that purports to be security software from Microsoft Corp. but actually tries to disable security programs that are already running. The worm, dubbed "Swen" or "Gibe," takes advantage of a two-year-old hole in Internet Explorer and affects systems that have not installed a patch for that security hole, according to an Internet security company. The malicious program arrives as an attachment to an e-mail pretending to contain a patch for holes in Internet Explorer, Outlook and Outlook Express and then mails itself off to addresses located on the victim's computer. The worm also can spread over Internet relay chat and the Kazaa peer-to-peer network, as well as copy itself over shared networks. Microsoft has cautioned customers in the past against e-mail software updates, saying it does not distribute patches as attachments, but rather directs them to its website.

Source: <http://www.cnn.com/2003/TECH/internet/09/19/worm.swen.reut/index.html>

32. *September 18, Associated Press* — Virus sender helped FBI bust hackers. Federal prosecutors credited the man responsible for transmitting the Melissa virus -- a computer bug that did more than \$80 million in damage in 1999 -- with helping the FBI bring down several major international hackers. Court documents unsealed Wednesday, September 17, at the request of The Associated Press show that David Smith began working with the FBI within weeks of his 1999 arrest, primarily using a fake identity to communicate with and track hackers from around the world. According to the court document, Smith helped the FBI bust virus senders abroad and stop viruses in the U.S. The letter says that two months after his arrest, Smith gave the FBI the name, home address, e-mail accounts and other Internet data for Jan DeWit, the author of the so-called Anna Kournikova virus in the Netherlands. The FBI passed the information on to authorities in the Netherlands. DeWit was arrested and later sentenced to probation. The federal prosecutor also said that Smith was working with the FBI to develop an investigative tool that theoretically could help identify an e-mail sender who was trying to mask his or her identity.

Source: <http://www.cnn.com/2003/LAW/09/18/fbi.hackers.ap/index.html>

33. *September 18, CERT/CC* — CERT Advisory CA-2003-25 Buffer Overflow in Sendmail. A vulnerability in sendmail could allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon, typically root. This vulnerability is different than the one described in CA-2003-12. The email attack vector is message-oriented as opposed to connection-oriented. This means that the vulnerability is triggered by the contents of a specially crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability may pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through packet filters or firewalls. Depending on platform and operating system

architecture, a remote attacker could execute arbitrary code with the privileges of the sendmail daemon. This vulnerability is resolved in Sendmail 8.12.10. Sendmail has also released a patch that can be applied to Sendmail 8.9.x through 8.12.9. Sendmail 8.12.10 is designed to correct malformed messages that are transferred by the server. This should help protect other vulnerable sendmail servers.

Source: <http://www.cert.org/advisories/CA-2003-25.html>

Internet Alert Dashboard

| Current Alert Levels | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  AlertCon: 2 out of 4 https://gtoc.iss.net |  Security Focus ThreatCon: 2 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), 1433 (ms-sql-s), 1434 (ms-sql-m), 137 (netbios-ns), 80 (www), 445 (microsoft-ds), 139 (netbios-ssn), 4662 (eDonkey2000), 25 (smtp), 4444 (CrackDown) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |

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

General Sector

34. *September 20, Reuters* — **Strong quake hits Japan. An earthquake measuring 5.5 on the Richter scale jolted Tokyo and nearby areas on Saturday, injuring several people, but there were no reports of major damage.** The quake, with its epicenter 50 miles below the surface in the Pacific Ocean east of Tokyo, occurred at 12:55 p.m. (11:55 p.m. EDT Friday), the Meteorological Agency said. No tsunami warning was issued, but fire officials quoted by Kyodo news agency said seven people were slightly injured when part of a temple wall collapsed in central Tokyo. The tremor did not seriously affect transportation.

Source: <http://www.washingtonpost.com/ac2/wp-dyn/A37996-2003Sep20?language=printer>

35. *September 19, Associated Press* — **Police suspect radical environmentalists in fires.** A fire that destroyed three homes under construction early Friday was the work of a radical environmentalist group, officials said. **The California Highway Patrol said the blaze was an Earth Liberation Front (ELF) fire. The environmentalist group has previously claimed responsibility for dozens of acts of arson and vandalism, including an August fire at a San Diego apartment complex under construction that caused \$50 million in damage.** The fire started at about 2 a.m., in the north-central part of the city, said Susan Smith, a fire department

dispatcher. About two hours later, another home under construction caught fire about three miles away. **A banner was hung on a building near the first fire, but police would not immediately say what was written on the banner. In the August ELF fire, banners were hung at the site reading, "If you build it, we will burn it."** Federal investigators are also looking into an arson and vandalism attack last month that targeted Hummers and SUVs in Los Angeles County, causing \$1 million in damage.

Source: <http://www.cnn.com/2003/US/West/09/19/construction.fire.ap/index.html>

36. *September 18, Reuters* — Spain arrests five more al Qaeda suspects. Spanish police arrested five people of Syrian origin on Thursday for suspected ties to al Qaeda, including a highly trained guerrilla prepared to commit a major suicide attack, police sources said.

A separate source involved in the investigation said some of the suspects were linked to a journalist for Arab TV network Al Jazeera who is already charged in Spain with belonging to the militant group led by wealthy Saudi exile Osama bin Laden. The arrests came a day after Spanish High Court judge Baltasar Garzon formally charged bin Laden, the journalist Tayseer Alouni and 33 others with "belonging to a terrorist group." Alouni strongly denies any wrongdoing. **The anti-terrorist police source said there were two arrests in Granada in southern Spain, where Alouni lived and was arrested earlier this month, two in Madrid and one in Alicante in the east of Spain.** The man arrested in Alicante was identified as Sadeq Merizak, said to have achieved "third level" status within al Qaeda, the same as September 11 lead hijacker Mohammed Atta, the source said. He said Merizak had trained at al Qaeda camps in Afghanistan.

Source: <http://asia.reuters.com/newsArticle.jhtml?type=worldNews&storyID=3467662>

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

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.