



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 09 January 2004

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- CNN reports airline industry officials said they are prepared to maintain security for a heightened alert even if the U.S. terror threat level is lowered. (See item [9](#))
- The Oregonian reports shippers and Port of Portland officials say the effects of this week's winter storm on air travel and overnight deliveries might take days to sort out; FedEx canceled overnight delivery operations in Portland through Wednesday, stranding more than 5,000 packages. (See item [12](#))
- esecurity Planet reports right after the Mmail.P worm that surfaced on January 7, security vendor Sophos has issued an alert for the N variant, on January 8. (See item [26](#))

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: High, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 08, Associated Press* — Uranium imported through Norfolk sent to wrong plant. The federal government is investigating how six metric tons of blended Russian uranium shipped through Norfolk, VA, ended up in North Carolina instead of Kentucky. A Nuclear Regulatory Commission spokesperson says the mistaken shipment to a nuclear fabrication plant in Wilmington, NC, posed no risk to anyone. It was supposed to go to a plant in Paducah, KY. The Paducah plant enriches uranium for use as fuel for nuclear power plants. The Wilmington

plant takes the fuel and shapes it for reactor use. **The trucking company that transported the diluted uranium accidentally sent the load along with a similarly-numbered load from a dock in Norfolk to Global Nuclear Fuel in Wilmington on December 19th.** Transport Logistics International says the error was quickly spotted and Global was notified the Paducah shipment also would be coming, along with Global's intended shipment.

Source: <http://www.wavy.com/Global/story.asp?S=1592499&nav=23iiK4FV>

2. *January 08, Reuters* — **Pacific NW utilities whittle down storm outages. The lights were back on Thursday, January 8, in more than 150,000 homes in the Pacific Northwest as utility crews raced to reconnect lines downed by heavy winter storms that pounded western Washington and Oregon this week. At their peak, the storms knocked out electric service to nearly 260,000 homes and businesses, power companies said. "Our weather conditions are very good today to be able to get this restoration work completed," said Dorothy Bracken, a spokesperson for Bellevue, WA-based Puget Sound Energy. Heavy snow followed by freezing rain bent and sometimes broke tree limbs, in some cases sending them crashing into power lines and blacking out nearby neighborhoods, utility sources said.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_01_08_eng-reuters_pma_PACIFI_C-NW-UTILITIES-WHITTLE-DOWN-STORM-OUTAGES&SMContentSet=0

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *January 07, Reuters* — **New missile defense system being developed. The Pentagon has awarded an eight-year contract to a private contractor to develop and demonstrate the first system designed to knock out multiple ballistic missile warheads and decoys with a single launch, the Pentagon said on Wednesday, January 7. The system would carry multiple, small "kill" vehicles designed to destroy incoming warheads and decoys by colliding with them in space. It would be designed to fit on existing and planned rocket boosters for interceptor missiles, the Pentagon's Missile Defense Agency said. "Miniature Kill Vehicle (MKV) represents a potential game-changing capability for missile defense," the contractor said. "It is designed to counter future threats where it is hard to differentiate between threat objects." **The Missile Defense Agency said the system would add "firepower and robustness" to the rudimentary ground- and sea-based shield President Bush plans to begin deploying by the end of this year, notably against any warheads from North Korea.****

Source: http://biz.yahoo.com/rc/040107/arms_lockheed_missile_2.html

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

Banking and Finance Sector

4. *January 09, The Australian* — **Scam targets internet bank accounts.** Customers of the Australia's five leading banks are unwittingly having their savings siphoned online, after logging on to official internet banking Websites. **Australian police are investigating the latest international banking scam involving the use of online "trojans" to steal personal account details via computers that do not have anti-virus protection.** The perpetrators, believed to be working out of Russia and Latvia, recruit other local account holders to accept and transfer the funds in exchange for a cut of the proceeds. Customers of the National, Commonwealth, ANZ, Westpac and St. George have all fallen prey to the scam when using computers without updated anti-virus firewalls.
Source: http://www.theaustralian.news.com.au/common/story_page/0,574,4,8354034%255E2702,00.html

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

Transportation Sector

5. *January 08, Associated Press* — **Ice storm grounds planes, closes roads in Northwest. Thousands of passengers remained stranded as icy runways and jets shrouded in frost shut down the Portland International Airport again Thursday.** The Federal Aviation Administration said Thursday morning that the airport will not reopen before Friday morning. **The ice covering the runway Wednesday was so thick it peeled off in sheets, and attempts to plow the snow or clear the runways with de-icer proved fruitless.** Passengers were sent home or to hotels. But a few hundred slept at the airport, using blankets distributed by the Red Cross Around Portland, car, bus and light rail travelers were also stranded for a second day in a row because of the ice and snow. Crews scattered sand on major thoroughfares in Portland, but side streets were blocked by mounds of snow. Interstate 84 through the Columbia River Gorge from Troutdale to Hood River remained closed, and many other roads and highways were closed at various times because of ice, accidents and downed trees.
Source: http://www.usatoday.com/weather/news/2004-01-08-northwest-ice_x.htm
6. *January 08, Reuters* — **US Airways looking to sell assets—source.** US Airways, the No. 7 U.S. airline, is looking to sell assets, including one of its three East Coast route hubs, to scale back costs, a source close to the situation said Thursday, January 8. **The assets being considered for sale include the airline's shuttle service between Boston, Washington and New York, the company's US Airways Express regional jet service and one of its three hubs, which are in Pittsburgh, Philadelphia, and Charlotte, NC, the source said.** The decision to sell assets, first reported in Thursday's New York Times, was prompted by the company's failure to win union support for a revised business plan proposed by management. The airline believes the new plan is necessary to help it compete against new low-cost services being offered by competitors. Arlington, VA-based US Airways emerged from Chapter 11 bankruptcy protection last March but is still struggling to compete with other airlines and to lower costs.
Source: http://www.forbes.com/business/newswire/2004/01/08/rtr120289_8.html
7. *January 08, Associated Press* — **Safety group finds gaping holes in nation's highway laws. A coalition of insurance companies and consumer and law-enforcement groups finds the**

various state laws on highway safety appear to be a patchwork quilt with gaping holes in need of repair. For instance, the group — Advocates for Highway and Auto Safety — reports 30 states don't have a tough law requiring the use of seat belts. Also, 31 states don't require motorcyclists to wear helmets. And the group reports 16 states have "dangerous gaps" in their child restraint laws. The group's report comes as Congress is gearing up to debate major highway financing legislation. **Advocates hope Congress will adopt national highway standards or at least pressure states to toughen laws if they want to get a share of federal highway financing.**

Source: <http://www.wkrn.com/Global/story.asp?S=1592605&nav=1ugFK4wu>

8. *January 08, The Columbian (Clark County, WA)* — **Amtrak passengers stranded in Vancouver. Amtrak's northbound Coast Starlight arrived in Vancouver at 2:15 a.m., almost 10 hours behind schedule. Frozen switches put the train well behind schedule, and it arrived in Vancouver with its crew having worked the federal maximum of 12 consecutive hours.** Then it stayed in Vancouver for the next five hours. All 180 passengers stayed on board as the train idled outside the darkened Vancouver depot, with stewards serving the passengers complimentary food and coffee. By 7 a.m., a rested crew of engineers drove the train back to Portland. Maintenance workers for Burlington Northern Santa Fe Railway fought to clear ice from switches on the bridge spanning the Columbia River. The tracks' owner is accustomed to dicey weather, with Burlington Northern main lines running through the nation's northern tier. But railroad spokesman Gus Melonas said even deep winter snow drifts in places such as Montana, Wyoming and North Dakota are generally easier to clear than the moisture-laden ice that clogged tracks throughout Western Washington and the Columbia River Gorge.

Source: http://www.columbian.com/01082004/clark_co/106504.html

9. *January 08, CNN* — **Officials: Airlines ready to stay on orange alert.** Airline industry officials said Thursday, January 8, they are prepared to maintain security for a heightened alert even if the U.S. terror threat level is lowered. "We will comply," said Air Transport Association President Jim May, noting that the airline industry hasn't been told officially if it will remain at orange alert. **Bush administration officials said this week that certain sectors, such as the aviation industry, could be kept on a higher alert while the national threat level is lowered to yellow but that no decisions have been made.** May said U.S. airlines are not experiencing any significant reduction in passenger bookings or curtailed flights because of the tighter security. Air France, which was forced to cancel three flights in the past two weeks because of U.S. terrorism concerns, also said it is not experiencing a high volume of cancellations. Air France also reported that its advanced bookings for January are ahead of last year's level. **Air Transport Association's May acknowledged airlines face higher costs for personnel, insurance and equipment associated with countermeasures to handle the elevated threat alert, but he said such costs are incremental.** Airline travelers seem to be getting accustomed to the more stringent security, he said. "Anecdotally ... it seems the public is accepting at this point of the world we live in," he said.

Source: <http://www.cnn.com/2004/US/01/08/airlines.orange.alert/index.html>

10. *January 07, Federal Computer Week* — **FAA sets target for telecom backbone.** The Federal Aviation Administration (FAA) plans to deploy the backbone of its \$3 billion FAA Telecommunications Infrastructure (FTI) program by September. **The agency's telecom**

manager, Steve Dash, announced today that a decision was made last month to deploy the FTI program at 27 major operational facilities, including all air route traffic control centers. The FTI program is 15-year effort by the FAA and a contractor team to integrate older systems into one telecom infrastructure while delivering a greater range of services. When complete, the network will encompass more than 5,000 FAA facilities nationwide. Dash also said the FAA plans to make its decision on going forward with the second phase of deployment to more than 5,000 smaller facilities in July 2004. Phase two will include approximately 600 manned facilities, with 349 of these considered significant air traffic control centers. FTI was deployed at two test sites — Kansas City, MO, and Fort Worth, TX — last fall, and Dash expects the services between those two sites to be operational by the first week of February. **The test sites are connected to the FTI Network Operations and Control Center in Melbourne, FL. This center will manage all operations of the FTI program, including security.**

Source: <http://www.fcw.com/fcw/articles/2004/0105/web-faa-01-07-04.a.sp>

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

Postal and Shipping Sector

11. *January 08, DM News* — Postal panel announces hearing schedule. U.S. Representative John M. McHugh, R-NY, who leads a special panel on postal reform and oversight, will hold three hearings in the next two months focusing on postal reform. The first hearing will take place January 28 in Washington. Representatives from the U.S. Postal Service (USPS) and the General Accounting Office will testify. The second hearing, which takes place February 5 in Chicago, will hear from USPS employee organizations. The National League of Postmasters has already signed up to testify. The third hearing, which will take place on February 11, will hear comments from mailers, postal-reliant businesses, and competitors. **A spokesperson for the Senate Governmental Affairs Committee Wednesday also said it will hold two postal reform hearings the first week of February that will focus on recommendations from the President's commission.**

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=26116

12. *January 08, Oregonian* — Packages pile up. Shippers and Port of Portland officials say the effects of this week's winter storm, in Oregon, on air travel and overnight deliveries might take days to sort out. **With cargo planes unable to leave or land and its trucks straining just to start, FedEx canceled overnight delivery operations in Portland from noon Tuesday through Wednesday, stranding more than 5,000 packages.** Company officials said it might be the first shut down in FedEx's history serving Portland. Four wide-bodied planes bound for FedEx hubs in Oakland, CA, Memphis, TN, and Indianapolis, IN, remained stuck on Portland International Airport's (PDX) tarmac all day, layered in ice. Even when planes start flying, it will take a few days for business to return to normal. Fernando Morton, senior manager at FedEx's Port of Portland station, said he expects to dispatch drivers Saturday and Sunday to clear the package pileup. **UPS canceled routes in Vancouver but attempted to deliver packages throughout the Portland area, Jeff Grant, a spokesman, said.** At least one cargo plane landed overnight, enabling the company to deliver some next-day air packages. UPS dispatched 32 trucks in Portland at 10:40 a.m., two-and-a-half hours later than normal after loaders failed to make it to work and packages arrived late from PDX.

Source: <http://www.oregonlive.com/business/oregonian/index.ssf?/base/business/1073566600194250.xml>

13. *January 08, EU Observer* — **Security services: more bombs on the way.** The German security services said Wednesday that more letter bombs are probably on their way to senior European Union (EU) figures. In an internal document reported by German daily Die Welt, the German security services say that a "series of pre-prepared letters" is to be feared. **The German police added that "further letter bombs are already in the postal system or have recently been given to the postal service."** Especially high vigilance will have to be maintained at the beginning of next week when the European Parliament holds its session in Strasbourg, due to a backlog of unopened letters possibly containing bombs. Further details have also emerged about the group suspected of carrying out the bombing campaign. The anarchist group "Federazione Anarchica Informale" (FAI) is believed to be behind the bombing and is estimated by Italian officials to have about 350 members.

Source: <http://www.euobserver.com/index.phtml?aid=14035>

[[Return to top](#)]

Agriculture Sector

14. *January 08, Reuters* — **Beef industry offers plan to resume exports to Japan. Calming the mad cow concerns of Japan, the single biggest buyer of U.S. beef, is seen as the key to reinstating all American exports, which totaled \$3.2 billion last year.** U.S. consumers have shrugged off news of the first U.S. case of bovine spongiform encephalopathy (BSE), but Japanese consumers are more wary. Moving too quickly to resume imports "could result in loss of confidence" among the Japanese, Japanese Trade Minister Shoichi Nakagawa told reporters after meeting with U.S. Agriculture Secretary Ann Veneman on Wednesday evening. Nakagawa was scheduled to hold further talks on Thursday with U.S. Trade Representative Robert Zoellick. U.S. industry sources told Reuters that a new program was being discussed to reassure Japan that U.S. beef is safe to eat. Under the program, slaughter plants would carefully plan when they handle cattle whose meat was intended for Japan. **"Plants will do production on designated days for shipment to Japan and they'll make sure the cattle they have lined up for that day include nothing that's over 30 months,"** said one industry official.

Source: <http://www.reuters.com/newsArticle.jhtml?type=scienceNews&storyID=4091199>

15. *January 08, Wisconsin Ag Connection* — **More CWD cases confirmed. Two more whitetail deer from a Portage, WI, hunting preserve have tested positive for chronic wasting disease (CWD), State Veterinarian Robert Ehlenfeldt announced Wednesday.** The latest numbers brings the total to six CWD-positive animals from Buckhorn Flats Game Farm in Almond. The National Veterinary Services Laboratory in Iowa reported Tuesday that two three-year-old bucks shot at the hunting preserve were infected with the fatal disease. The animals were routinely sampled for CWD after being shot in paid hunts last fall. **According to the game farm owner, one animal was born on the premises and the other was purchased from the same Walworth, WI, farm that was the apparent source of the first CWD-positive animal shot on the preserve in September 2002.** The game preserve's herd was ordered killed in July 2003, based on the first positive result, but the owner appealed the order. That appeal is in process before an administrative law judge. The game farm has been

under quarantine since September 2002, when the first CWD–positive animal found on a Wisconsin farm was shot there. **The game farm has been permitted to conduct paid hunts because the quarantine applies only to live animals.**

Source: http://www.wisconsinagconnection.com/story–state.cfm?Id=34&y_r=2004

16. *January 08, Associated Press* — **U.S. bans Chinese pears. The U.S. pulled Chinese pears from grocery stores and banned them from imports after a federal plant pathologist discovered diseased pears at a Wenatchee, WA, grocery store while shopping in December.** Rodney Roberts, who works at the Tree Fruit Research Laboratory in Wenatchee, found the bad fruit, federal officials said. Roberts sent information and photos to a U.S. Department of Agriculture (USDA) laboratory in Maryland. There is no human health risk but the recall and import suspension were ordered to protect U.S. apple and pear industries, USDA officials said Tuesday. **The USDA found more of the bad fruit in stores in 18 cities within the next few days after Roberts' discovery, and issued a recall and import suspension on December 19, said Dore Mobley, a public affairs specialist for the Animal Plant Health Inspection Service.** Mobley said the recall of 3.25 million pounds of Chinese pears from West Coast and East Coast stores and distribution centers was mostly completed by the weekend after Christmas. The yellow Ya pears also were recalled in December 2001 for the same strain of post–harvest fungus disease, *Alternaria* sp, that causes rot, Mobley said.

Source: <http://www.kgw.com/sharedcontent/APStories/stories/D7VUB4B80.html>

17. *January 08, Vietnam News Agency* — **Prime Minister orders strict measures to fight chicken epidemic.** Vietnam's Prime Minister Phan Van Khai on Thursday requested that provinces and cities which are plagued by the chicken epidemic to take scores of preventive measures to fight the disease and prevent it from further spreading. **In an official telegram, the PM also asked local authorities to establish steering committees, carry out control measures, and monitor the transportation of poultry around–the–clock in a bid to prevent infected poultry from entering other localities.** The Prime Minister urged them to cull all dead and infected poultry and request market managers, veterinary and health services, and police to intensify inspections on the issue. The Prime Minister asked other provinces and cities to quarantine strictly those inbound poultry and cull infected poultry if discovered and quickly take steps to deal with the epidemic. **The Ministry of Agriculture and Rural Development was also ordered to work with relevant ministries and even international organizations in defining the virus that caused the disease for developing effective preventive measures.** The Ministry will also have to work with localities to quarantine infected areas and carry out early measures to prevent the disease from spreading.

Source: http://www.vnagency.com.vn/NewsA.asp?LANGUAGE_ID=2&CATEGORY_ID=29&NEWS_ID=38206

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

Food Sector

18. *January 08, Food Navigator* — **Emerging food pathogen. Enterobacter sakazakii, a potential foodborne pathogen, has been linked to outbreaks of illness in new–born and premature infants.** Contamination of infant formula has been suggested as a source of infection. A recent study by Dutch scientists aims to shed light on the issue. Little is known

about the pathogenesis of *E. sakazakii* although there appears to be differences in virulence among the various strains and there may be several different biotypes of the organism that causes human illness. **The pathogen has been implicated in outbreaks of severe meningitis or necrotizing enterocolitis in premature babies. A mortality rate of 40 to 80 percent has been reported in these outbreaks.** Infant formula is pasteurized during manufacturing and *E. sakazakii* does not survive such heat treatment. Nevertheless, *E. sakazakii* has been isolated from such infant formula and it is thought that the pathogen originates from the factory environment, possibly from heat sensitive micro-nutrients added after pasteurization or from bottle preparation. **The Dutch team investigated the extent of the spread of the bacteria by testing nine factories and 16 households. Eight of nine food factories and five of 16 households contained *E. sakazakii*.**

Source: <http://www.foodnavigator.com/news/news-NG.asp?id=48880>

19. *January 08, Canadian Press* — Canada rules out ban on abattoir waste in cattle feed.

Canadian officials have ruled out a ban on feeding slaughterhouse waste to cattle even though some government scientists say such a ban is the only way to be sure of stopping mad cow disease. **Brian Evans, chief veterinarian for the Canadian Food Inspection Agency, said a ban would not be based on science and would be impossible to enforce. European countries have maintained such a ban for years and it has been under study in Canada. But a panel of foreign experts advised against the idea, said Evans.** "We proposed it as an option back in June last year in order to look at what the merits were but the international panel in fact said, don't do that." Evans said the European approach is based on public perception rather than science. **Under current Canadian regulations, cattle cannot be fed remains from other ruminants, including sheep and deer which can carry brain-wasting diseases linked to bovine spongiform encephalopathy (BSE).** But cattle can still be fed the remains of horses, pigs, chickens, and fish. Cattle blood and fat can be used in cattle feed, and many calves are weaned on cattle blood. Also, cattle remains can be fed to other animals such as pigs and horses.

Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1073517011421&call_pageid=968332188774&col=968350116467

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

Water Sector

20. *January 08, Daily Herald – Illinois* — Elgin to strengthen water plant security. As the nation remains on high alert for possible terrorist attacks, Elgin, IL, leaders are pressing ahead with plans to step up security at their water treatment facilities. **City officials plan to build an eight-foot-tall security barrier around the Riverside Water Treatment Plant property. They also plan to add more security cameras and secured gates at the main water facility and others in the city,** according to Larry Deibert, director of Elgin's water department. "This was recommended in two security analyses we've had performed here at the plant and for the entire water system," Deibert said. Elgin used a \$115,000 federal grant to hire a security firm to conduct a vulnerability assessment of its water system, and the top recommendation was to surround the water plants with security fences. Elgin officials have announced they intend to spend two million dollars over the next two years to install a massive generator at the Riverside

plant. It would allow Elgin to continue providing its residents and businesses with water during an extended lackout. The council made the commitment to buy a generator after the September 11 terrorist attacks raised concerns about the city's disaster preparedness.

Source: http://www.dailyherald.com/search/main_story.asp?intid=3799374

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

Public Health Sector

21. *January 08, Washington Post* — **China says second case of SARS suspected.** China reported a second suspected case of Severe Acute Respiratory Syndrome (SARS) on Thursday, as the first confirmed victim of the latest outbreak of the disease was released from the hospital. **The one-sentence announcement by the official New China News Agency said a waitress hospitalized in China's southern city of Guangzhou was suspected of having SARS.** A spokesman in Beijing for the World Health Organization, Roy Wadia, said he did not have any information on the waitress's case. On Tuesday, a rights group and a reporter said a newspaper in southern China had come under pressure from authorities after breaking news last month of the television producer's infection. Prosecutors detained the editor in chief of Southern Metropolis Daily for eight hours on Tuesday, according to the Hong Kong-based Information Center for Human Rights and Democracy. Chinese media have been under strict orders since last year to stick to the daily SARS updates issued by the Health Ministry, which did not report the latest case until after the Southern Metropolis report.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A63798-2004Jan7.html>

22. *January 08, Associated Press* — **Judge permits military to resume anthrax shots.** A federal judge Wednesday allowed the military to resume anthrax inoculations. **U.S. District Judge Emmitt Sullivan announced his decision from the bench and then issued a two-page order, which ended the injunction he imposed December 22 to halt the vaccinations.** The Pentagon has not said whether it will resume the shots. Eight days after the injunction, the Food and Drug Administration announced that the vaccine was safe and effective for use against inhaled anthrax. Sullivan's order still banned forced vaccination for six military personnel who filed a class-action lawsuit to stop the mandatory vaccinations that started in 1998. The Justice Department, citing the FDA order, had asked Sullivan to set aside his preliminary ban, except for the plaintiffs.

Source: <http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/107356149038030.xml>

23. *January 08, Agence France Presse* — **Seven dead from mystery virus. Seven children aged between nine months and 12 have died from a mysterious respiratory disease in the Vietnamese capital, but health officials have ruled out Severe Acute Respiratory Syndrome (SARS) as the cause, state media said Thursday.** Since mid-October, 12 children have been admitted to Hanoi's Central Pediatric Hospital with a high fever and a chesty cough. Their symptoms have not reacted to antibiotics. Seven of the 12 children died in the hospital, while five others are receiving treatment in an isolation ward. Pascale Brudon, the World Health Organization's representative to Vietnam, said two were recovering but three were in a poor condition. The mother of one of the dead victims has also been struck down with the virus and was undergoing treatment at Hanoi's Bach Mai hospital.

Source: http://www.news.com.au/common/story_page/0,4057,8354022%255E1702,00.html

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

Government Sector

24. *January 08, Government Computer News* — **Department of Homeland Security to get new CFO. President Bush plans to appoint Andrew B. Maner, a senior Customs and Border Protection official, to be the new chief financial officer at the Department of Homeland Security, the White House said.** Maner will succeed Bruce Marshall Carnes, who left the position last year. Maner is chief of staff and director of the transition management office at Customs and Border Protection, which falls under the Border and Transportation Security Directorate. In his CFO job, he will report to undersecretary for management Janet Hale. In his new job, Maner will oversee the progress of the Emerge2 program, which is intended to build an administrative and IT infrastructure for most of the department's finance, accounting and back-office operations.

Source: http://www.gcn.com/vol1_no1/daily-updates/24572-1.html

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

Emergency Services Sector

25. *January 08, York County Coast Star (ME)* — **Special training for town workers. Knowing about weapons of mass destruction is a necessity for more than just emergency service personnel, and some Kennebunkport, ME, employees will be augmenting their knowledge in a two-day training session this week. The comprehensive course developed by the federal government is meant to raise the awareness of town employees concerning what weapons of mass destruction do and how to address an emergency.** Although the awareness class is being held in Kennebunkport, ME, Village Fire Chief Gary Plamondon said it is open for employees of several other towns, including Ogunquit, Wells, Kennebunk, and Biddeford. Director of York County Emergency Medical Agency Bob Bohlmann said this is not the first course like this that they have helped coordinate, noting that recently an awareness training was held in Berwick which was very successful. While this and other types of training have been held throughout York county, Plamondon said that Walker's Point, home to former President George Bush and visited by current President George W. Bush, is a potential target, which punctuates the importance of the training. Bohlmann said that town clerks usually instinctively know whether a person is asking unusual questions, but the training might make them aware that such questions could indicate the person's motives.

Source: http://www.seacoastonline.com/news/yorkstar/ys1_8c.htm

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

Information and Telecommunications Sector

26. *January 08, esecurity Planet* — **Yet another Mimail variant surfaces.** On the heels of the Mimail.P worm surfacing on Wednesday, January 7, security vendor Sophos issued an alert

for the N variant on Thursday, January 8. Like Mimail.P, W32/Mimail-N is a mass-mailing worm that disguises itself as a legitimate form from Paypal credit card information. If a network connection is detected on execution then two forms are displayed asking for credit card and personal information. Once this information is filled in, it is sent to a remote web site. If a network connection is not detected then the start page of Internet Explorer is changed to a web site with a satirical picture. The worm copies itself to ee98af.tmp and winmgr32.exe in the Windows folder and sets the following registry entry so that the latter is run on system startup:HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinMgr32. This variant also creates a zipped copy of itself as zipzip.tmp in the Windows folder and drops the fake forms as index.hta and index2.hta to the root folder. The worm scans files on the hard disk for email addresses and stores the result in outlook.cfg in the Windows folder.

Instructions for removing this variant are at

<http://www.sophos.com/virusinfo/analyses/w32mimailn.html>

Source: <http://esecurityplanet.com/alerts/article.php/3297071>

27. January 07, The Register — Bogus FBI warning file contains malware. Virus writers are attempting to trick music fans into opening malicious code with a message purporting to arise from an FBI investigation into illegal file trading. Recipients of the bogus warning are told they are under investigation. Infectious emails contain an attachment allegedly containing evidence against the 'accused' which actually contains Windows malware, the Melbourne Age reports. **The message appear authentic but closer inspection reveals factual errors and spelling mistakes** that give the game away.

Source: <http://www.theregister.co.uk/content/56/34755.html>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.G Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	901 (realsecure), 135 (epmap), 1434 (ms-sql-m), 137 (netbios-ns), 6129 (dameware), 445 (microsoft-ds), 80 (www), 53 (domain), 139 (netbios-ssn), 1433 (ms-sql-s) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

28. *January 08, BBC News* — **Muslim group behind Thai raids. Thai officials have named a Muslim militant group they believe carried out a wave of attacks on southern Thailand which killed six soldiers and police. A government security adviser said the group, the Gerakan Mujahideen Islam Pattani, had links to al Qaeda and the regional network Jemaah Islamiah.** General Kitti Rattanachaya's comments were at odds with previous claims the attacks were linked to banditry. **Up to 30 people have been reported to have been arrested over the violence.** Thailand's army has offered a \$25,000 reward for information on those involved. General Rattanachaya, a former army commander in the south and now a government security adviser, said militants in South East Asia fought together in mujahideen against the Soviet occupation of Afghanistan, and then returned home to set up local groups. He said that the professional nature of the attacks, which included co-ordinated arson on several schools and an arms depot raid at the weekend, indicated the gunmen had outside help, "possibly from the Kampulan Mujahideen Malaysia". "At present, international terrorists are linked together like a network, with al Qaeda at the core," Kitti said.
Source: <http://news.bbc.co.uk/1/hi/world/asia-pacific/3379079.stm>

[[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.