



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 14 April 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- Microsoft has released "Security Bulletin MS04-011: Security Update for Microsoft Windows (Critical)" and an update is available on the Microsoft Website. (See item [25](#))
- Microsoft has released "Security Bulletin MS04-012 Cumulative Update for Microsoft RPC/DCOM (Critical)" and a patch is available on the Microsoft Website. (See item [26](#))
- Microsoft has released "Security Bulletin MS04-013 Cumulative Security Update for Outlook Express (Critical)" and a patch is available on the Microsoft Website. (See item [27](#))
- Microsoft has released "Security Bulletin MS04-014 Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (Critical)" and a patch is available on the Microsoft Website. (See item [28](#))
- Security Focus has raised ThreatCon to Level 2, citing a need for increased vigilance. Please refer to the Internet Alert Dashboard.
- Internet Security Systems has raised Alertcon to Level 2, citing a need for increased vigilance. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

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

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

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

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

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: **Physical: Elevated, Cyber: Elevated**

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

1. *April 13, Nuclear Regulatory Commission* — **NRC issues report on quality of technical information under development by DOE for Yucca Mountain application.** The Nuclear Regulatory Commission's (NRC) Office of Nuclear Material Safety and Safeguards has issued a report on its recent team evaluation of the quality of certain technical information in three documents that the Department of Energy (DOE) is preparing to support its expected application for a license to build and operate a high-level radioactive waste repository at Yucca Mountain, NV. **The report finds that, if DOE continues to use their existing policies, procedures, methods, and practices at the same level of implementation and rigor, the license application may not contain information sufficient to support the technical positions in the application.** The team found that the DOE and its contractor had used several good practices and found the technical information was much improved over what was presented in the DOE's Total System Performance Assessment for Site Recommendation in 2001. However, the team identified some concerns with both the clarity of the technical bases and the sufficiency of technical information used to support DOE's explanation of the technical bases. DOE could reasonably have identified and corrected these problems during the information checking and review process. Report: <http://www.nrc.gov/waste/hlw-disposal/reg-initiatives/resolve-key-tech-issues.html>. Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2004/04-041.html>
2. *April 13, Reuters* — **California power market vulnerable to manipulation according to report.** California's electricity trading market remains vulnerable to manipulative strategies linked to its 2000–01 energy crisis, the state's attorney general said on Tuesday, April 13. Three years after supply shortages led to rolling blackouts and bankruptcy of California's biggest utility, California agencies and the Federal Energy Regulatory Commission (FERC) are still at odds over how to close the door on the debacle. **California Attorney General Bill Lockyer said there is lingering potential for energy companies to attempt the kinds of "epidemic" market manipulation that FERC found in its investigation.** "The incentives to game the market and create disruption appear, for the most, to remain in place," according to a report issued by Lockyer. The report also criticized a longstanding FERC rule that limits electricity buyers from asking for refunds until 60 days after they file a complaint with the agency. **FERC spokesperson Bryan Lee blamed a badly-designed plan to deregulate California's electricity market,** and said "none of the manipulation would have been possible if not for the underlying supply–demand imbalance." Below-average hydropower supplies in California that led to the state's 2000–01 shortage could again restrict supplies this summer, Lee said. Source: http://biz.yahoo.com/rc/040413/utilities_california_1.html

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

Chemical Sector

3. *April 13, Associated Press* — **Hundreds evacuated after malfunction at Dalton chemical plant.** A malfunction at a Whitfield County (Georgia) chemical plant formed a vapor cloud that prompted the evacuation of several hundred people in the area Monday night, April 12. **Workers at MFG Chemical Inc., which produces coatings and other substances for the**

textile industry, were mixing chemicals about 9:30 p.m., when the reactor malfunctioned and formed the cloud that engulfed the nearby area, said Dalton, GA, police spokesperson Chris Crossen. The chemical, allyl alcohol, is commonly used as a starting material in making various polymers, pharmaceuticals and pesticides. **Hundreds of residents and workers from at least five other factories within a half-mile radius of the plant were evacuated, Crossen said. The local Red Cross set up a shelter at a church for those who didn't have a place to go for the night.** About 100 people, including some police officers and firefighters, were treated for minor symptoms, including burning sensations in the eyes and irritation in the throat, but no serious health problems were reported, he added. Residents and workers still were not allowed back in the area Tuesday. Authorities said they were waiting for the reactor that malfunctioned to cool down before cleanup could even begin. The cause of the malfunction is under investigation.

Source: <http://www.ledger-enquirer.com/mld/ledgerenquirer/8421226.htm>

4. *April 13, Associated Press* — **No decrease seen in accidents at chemical plants.** The number of accidents at chemical manufacturing plants shows no sign of decreasing, and there are no federal or state safety benchmarks to make the industry accountable to the public, according to a report by an environmental and consumer advocacy group. **Pennsylvania ranked seventh of 13 states in which more than 500 accidents have been reported since 1990 at chemical plants that met safety standards required for members of the American Chemistry Council, according to the report issued this month by the U.S. Public Interest Research Group.** The General Accounting Office, the investigative arm of Congress, has reported that many chemical factories are in populated areas, and cited a U.S. Environmental Protection Agency estimate that 123 of them could endanger a million people in a toxic worst-case scenario. **In the Philadelphia region, according to the EPA, seven plants could each endanger more than a million people in the event of a worst-case scenario, the highest concentration on the East Coast.** Plants in Texas led the nation in accidents with 7,072. Those in Louisiana followed with 5,375. Plants belonging to London-based BP P.L.C.; the DuPont Co. of Wilmington, DE; and the Dow Chemical Co. of Midland, MI, accounted for one-third of the reports, or 8,242 of the total accidents at the facilities studied, according to the advocacy group.

Source: <http://www.philly.com/mld/inquirer/news/local/states/pennsylvania/8417021.htm?lc>

5. *April 13, HeraldNet (Everett, WA)* — **Ammonia leak closes down highway, forces evacuations.** A suspicious ammonia leak at North Star Cold Storage in Stanwood, WA, closed down a section of Pioneer Highway and forced the evacuation of a handful of nearby businesses Tuesday morning, April 13. **Fire and police officials believe someone broke into the ammonia tank. The business has been burglarized in the past. Ammonia is a common ingredient to make methamphetamine.** Witnesses reported smelling the ammonia and seeing a cloud of gas on the north side of the building just before 6 a.m., according to Stanwood firefighter Rob Buchanan. Firefighters confirmed the leak and the Snohomish County Hazardous Materials Team was called in to assist. One firefighter was exposed to ammonia through a breach in his protective suit, Buchanan said. He was taken to a local hospital. His condition is not known. **Nearby businesses, including a veterinary clinic have been evacuated.** A company has been called in to transfer the remaining ammonia from the leaking tank.

Source: <http://heraldnet.com/Stories/04/4/13/18474766.cfm>

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

Defense Industrial Base Sector

6. *April 13, Aerospace Daily and Defense Report* — **UAV Battlelab experiments with feature recognition software. The U.S. Air Force's Unmanned Aerial Vehicle Battlelab (UAVB) has tested software that can pick desired features out of UAV video long before they become visible to the naked eye,** according to Lt. Col. Timothy Cook, chief of the UAVB's Combat Applications Division. Dubbed DIVOT (Digital Imagery and Video Object Tracking), the software was put to work on pre-recorded video taken by a Predator UAV in Iraq. The system was provided with imagery of certain objects, then told to identify them in another video. **DIVOT can compress video at rates of up to 400 to one, then search through the compressed data very quickly,** according to Cook. It also features 256-bit revolving encryption, which should make it more than up to the standards of the National Geospatial-Intelligence Agency (NGA), he said. Based at Eglin Air Force Base, FL, the UAVB's mandate is to take existing hardware and weapons and integrate them with UAVs. Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/bat04134.xml

7. *April 13, Government Computer News* — **Defense agencies develop data-sharing standard. The Department of Defense (DoD) and defense agencies from several other countries have developed a standard for documenting and sharing configuration information about large systems. Military services and contractors can use the standard to maintain up-to-date descriptions of how large items are configured, such as weapons systems.** The Product Life Cycle Support Technical Committee of the Organization for the Advancement of Structured Information Standards developed the standard, known as the PLCS ISO Standard. Government members of the committee include the Defense Information Systems Agency, British Ministry of Defense, Norwegian Defense Logistics Organization and Swedish Defense Materiel Administration. The committee sent 140 modules, or building blocks, to the ISO for final publication as ISO specifications, said Howard Mason, co-chairman of the technical committee. He expects the standards organization will make the modules available on the ISO Website within the next few days. The modules are "the building blocks for an information backbone," Mason said. "In the context of DoD, it would hold all the information you would need to associate with a particular unique identification number." Source: http://www.gcn.com/vol1_no1/daily-updates/25551-1.html

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

Banking and Finance Sector

8. *April 13, Associated Press* — **Five arrested in identity theft probe. Baltimore County, MD, police are investigating what they say appears to be a large-scale identity-theft ring with a link to a worker at a private medical lab.** Police have arrested five Baltimore men so far. Four were arrested after they tried to make a purchase at a Home Depot using the identity of a patient at who had lab tests done at Quest Diagnostics near Arbutus. **One of those men is**

linked in court documents to identity thefts from about 20 Navy officers aboard an aircraft carrier stationed in Norfolk, VA. A fifth man, Darren Rogers, is a Quest employee. According to court documents, Rogers is accused of stealing personal information about at least five Quest patients and using it to buy vehicles and home-improvement merchandise.

Source: <http://www.thewbalchannel.com/news/2999128/detail.html>

9. *April 13, Accountancy Age* — **IMF implements anti-money laundering rule.** International Monetary Fund (IMF) policies towards borrower countries will henceforth be influenced by their capacity to implement Financial Action Task Force (FATF) recommendations on fighting money laundering. IMF directors have agreed these assessments "do not contravene the prohibition of the Fund to exercise law enforcement powers." The decision follows a 12-month pilot involving cooperation with the World Bank and FATF on improving global money laundering standards. **This has sparked IMF conclusions that although compliance with FATF's original 40 recommendations is widespread, it is weaker with its newer (2001) eight special recommendations on terrorist financing.** It noted many poorer countries have installed the legal elements of anti-money laundering regimes, but implementation remains a challenge. Noted problems include "poor coordination amongst government agencies, ineffective law enforcement, weak supervision, inadequate controls among financial firms, and shortcomings in international cooperation."

Source: <http://www.accountancyage.com/News/1136763>

[[Return to top](#)]

Transportation Sector

10. *April 13, Reuters* — **Marshal leaves gun in airport bathroom. A federal air marshal accidentally left her gun in a restroom beyond the security checkpoints at Cleveland Hopkins International Airport on Thursday, April 8, officials say. The weapon was discovered by a passenger who alerted an airline employee.** The marshal remained on the job after Thursday's incident when she visited an airport restroom and inadvertently left her gun behind, Dave Adams, spokesperson for the Federal Air Marshal Service in Washington, said Saturday. The restroom was beyond security checkpoints, airport spokesperson Pat Smith said. So the risk was that someone could have discovered the gun and taken it on a flight. "Right now we're still doing the investigation," Adams said. "It will determine what disciplinary action will be appropriate." He declined to identify the marshal for security reasons, but said her work in the past had been "outstanding." The United States deploys armed air marshals disguised as passengers on thousands of flights each week as part of security measures implemented after the September 11, 2001, hijacked airliner attacks that killed about 3,000 people.

Source: http://money.cnn.com/2004/04/13/news/funny/air_marshal.reut/

11. *April 13, PRNewswire* — **Northwest Airlines welcomes Air Tahiti Nui to WorldPerks Network.** Northwest Airlines today, April 13, announced that Papeete, Tahiti-based Air Tahiti Nui is joining the Northwest Airlines WorldPerks network of airline partners. **The partnership, effective May 1, 2004, will offer attractive destinations for Northwest's WorldPerks members to redeem their frequent flyer miles.** Serving Papeete, Tahiti and Auckland, New Zealand from Northwest's hub at Tokyo as well as from Los Angeles and Osaka, Japan, Air Tahiti Nui's route network is a welcome addition to the WorldPerks Program.

Source: http://biz.yahoo.com/prnews/040413/cgtu004_1.html

12. *April 13, Associated Press* — **Los Angeles Airport power failure blamed on bird. The power failure Monday morning caused delays of 15 minutes to 90 minutes for an estimated 80 to 100 Los Angeles-bound flights, Federal Aviation Administration spokesperson Donn Walker said.** Apparently, a bird came in contact with the line and at the same time touched a cross-arm or some other grounded device. The line re-energized moments later. Despite the immediate restoration of the power supply, the effect on the airport's control tower lasted longer. **All radar, radios and telephones were hit by the outage, disrupting everything that Los Angeles tower controllers use to communicate with aircraft and other control facilities. The airport's ground radar also did not immediately work properly after the blackout.** Most functions came back quickly but some important equipment remained out, including critical switching equipment that allows instantaneous communication between Los Angeles tower controllers and the approach control facility in San Diego County, Walker said. However, he added, "tower controllers were always in contact with aircraft" after the failure. The switching equipment was restored after about three hours.

Source: <http://www.newsday.com/news/nationworld/nation/sns-ap-airport-blackout.0.3683224.story?coll=ny-nationalnews-headlines>

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

Postal and Shipping Sector

13. *April 13, American City Business Journals* — **Airborne waved off from San Jose landing. An Airborne Express Boeing 767 jet failed to make a scheduled landing at Mineta San Jose, CA, International Airport Tuesday, April 13, when one of its sets of landing gear malfunctioned.** The jet with four crew members aboard on a flight from Airborne's freight distribution center in Wilmington, OH, was diverted to Mather Air Force Base near Sacramento, CA. The plane managed to get the gear down and landed safely at the air force base shortly before 8 a.m. Airborne is part of the freight shipping firm DHL.

Source: <http://sanjose.bizjournals.com/sanjose/stories/2004/04/12/dayily15.html>

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

Agriculture Sector

14. *April 13, Canadian Press* — **Three more Canadian farms infected by avian flu. The number of farms infected with avian flu inside British Columbia's Fraser Valley high-risk area has increased to 25, officials said Monday, April 12.** The increase, with three new infected sites since Friday, April 9, is not a surprise, according to the Canadian Food Inspection Agency. Agency spokesman Blaine Thompson said a flock of 10,000 birds was reported April 12 to be infected. The farm was outside the surveillance area but inside the general control zone, he said. The infection was found as part of a pre-slaughter check. "There's obviously still some active virus out there that's still moving around and getting into these barns," Thompson said. "It's not surprising we found this one. There may be a few more through the pre-slaughter surveillance." **Thompson said the disease's spread will slow as**

more birds are slaughtered. Four known infected flocks remain to be slaughtered, he said.

Source: <http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20040413/AVAN13/TPNational/Canada>

15. *April 12, Oster Dow Jones Commodity News* — **Canada declares emergency in fight to control avian flu. The British Columbia Emergency Program Act has been invoked in the destruction of millions of poultry carcasses, part of an effort to halt the spread of avian flu in Canada.** Solicitor General Rich Coleman signed an order Saturday, April 10, to allow the use of incinerators and landfills for disposing of infected chickens, turkeys and other poultry from the depopulation of 19 million birds. Provincial Agriculture Minister John Van Dongen said "transport will be in sealed trucks and the security from an environmental health point of view will be very tight," Van Dongen said. The provincial Ministry of Agriculture, Food and Fisheries also confirmed that biological heat will be used to destroy the virus in half of the flocks which tested positive since the outbreak began in the Fraser Valley a few miles across the border from Sumas, WA. Under that plan, dead birds will be layered in barns, dampened and aerated to generate enough heat to kill the virus naturally.

Source: http://www.agprofessional.com/show_story.php?id=24495

16. *April 12, Purdue University* — **Purdue scientists finding ways to outsmart crop-damaging bugs. A new screening method aimed at boosting pesticide effectiveness may be commercially viable, according to Purdue University researchers. The process is designed to identify chemical compounds that could be added to current pesticides to overcome resistance insects have developed to them.** The scientists report that the method will be applicable to a variety of insects and chemicals. "It's becoming more and more difficult to find new, effective pesticides," said Barry Pittendrigh, assistant professor of entomology and senior author of the study. "If we can kill these pesticide-resistant insects in the field, then we have the potential to increase the functional life of the insecticides currently in use." Crop-damaging insects mutate over time so they are able to overcome the effects of chemicals developed to kill them. A toxin that protected a crop for more than a decade or two eventually may lose its lethality due to resistance in the insect population.

Source: http://www.eurekalert.org/pub_releases/2004-04/pu-psf041204.php

[[Return to top](#)]

Food Sector

17. *April 12, Food Safety and Inspection Service* — **Deli meat and cheese trays recalled. H.C. Schau & Sons, Inc., a Woodridge, IL, firm, is voluntarily recalling approximately 135 pounds of fresh deli meat and cheese trays that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced April 12.** The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease. Healthy people rarely contract listeriosis. However, listeriosis can cause high fever, severe headache, neck stiffness, and nausea. Listeriosis can also cause miscarriages and stillbirths, as well as serious and sometimes fatal infections in those with weak immune systems.

Source: <http://www.fsis.usda.gov/oa/recalls/prelease/pr013-2004.htm>

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

Water Sector

Nothing to report.

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

Public Health Sector

18. *April 13, ASCRIBE Newswire* — **Avian influenza outbreaks create concern about human infection. The occurrence of avian influenza in humans is a reminder of the vulnerability of people to an emerging pandemic, Mayo Clinic researchers warn.** "An immediate priority is to halt further spread of epidemics in poultry populations that would reduce the opportunities for human exposure to the virus," says Larry Baddour, of the Mayo Clinic Division of Infectious Diseases and Internal Medicine and the lead author of the article. Since mid-December 2003, Cambodia, China, Indonesia, Japan, Laos, South Korea, Thailand, and Vietnam have reported outbreaks of the avian influenza strain H5N1. Vietnam and Thailand have reported influenza H5N1 infection in humans with 32 laboratory-confirmed cases and 22 deaths, a mortality rate of nearly 70 percent. **Two of the three criteria that characterized the influenza pandemic of 1918-1919 have already been fulfilled in the current epidemic of avian influenza: the ability of the virus to infect humans resulting in high mortality, and a global immunologically naive human population.** The third criterion, efficient human-to-human transmission, has not been observed. Researchers are concerned because influenza viruses mutate frequently, potentially allowing them to change the host receptor specificity from avian to human.

Source: <http://www.ascribe.org/cgi-bin/spew4th.pl?ascribeid=20040412.125029&time=03%2002%20PDT&year=2004&public=1>

19. *April 13, Seattle Times* — **Man charged after authorities find ricin. Federal authorities have arrested a Kirkland, WA, man they say made ricin in his apartment from mail-order castor seeds. Robert M. Alberg was charged in federal court on Friday, April 9, with knowingly possessing a biological agent or toxin and was booked into the federal detention center in SeaTac pending indictment, U.S. Attorney's spokesman Lawrence Lincoln said.** Alberg's next court appearance is set for Thursday, April 15. Ricin is a biological agent that is considered a deadly toxin, according to the complaint filed against Alberg in U.S. District Court. Court documents don't specify how much ricin was found in Alberg's apartment, only that investigators found clear jars containing what appeared to be processed castor-seed pulp; labels on the jars read "caution ricin poison." They also found five pounds of castor seeds, chemicals used during different stages of ricin production, and equipment commonly used in the "underground" manufacturing of the poison, the papers say.

Source: http://seattletimes.nwsourc.com/html/localnews/2001901863_r_icin13e.html

20. *April 13, Reuters* — **Recruitment for smallpox trial halted. Acambis Plc, supplier of smallpox vaccine to the U.S. government, has stopped recruiting volunteers for trials on**

the job after three suspected cases of heart inflammation. The British firm, whose business has benefited from U.S. fears of bioterrorism, said on Tuesday, April 13, it was seeking additional data after the discovery of three cases of myopericarditis. "Once this analysis is completed...Acambis will be enlisting the assistance of the U.S. Food and Drug Administration and the U.S. Centers for Disease Control and Prevention to determine the next steps," Acambis said in a statement.

Source: <http://www.forbes.com/business/healthcare/newswire/2004/04/13/rtr1329824.html>

21. *April 12, Harbor–UCLA Research and Education Institute* — **Researchers identify unifying code among natural antibiotics.** Investigators at the Research and Education Institute (REI) at Harbor–UCLA Medical Center have identified a novel structural signature that is conserved in otherwise distinct classes of antimicrobial peptides. Antimicrobial peptides are small, naturally occurring protein antibiotics that protect organisms against infection. **The discovery of such a broadly encompassing structural signature within these ancient host defense peptides could significantly accelerate development of novel molecules to fight multi–drug resistant infections.** Principal Investigators Nannette Yount and Michael Yeaman integrated novel proteomic methods with established microbiologic techniques to reveal previously hidden structural codes common to broad classes of antimicrobial peptides from diverse organisms spanning nearly 4 billion years of evolution. "Our work builds upon the efforts of many excellent researchers in the field. We believe this discovery offers new insights into the evolution of immune defense against infection, and drives new technology that takes advantage of the fact that antimicrobial peptides inhibit many microbial pathogens that resist conventional antibiotics," said Yount and Yeaman.

Source: http://www.eurekalert.org/pub_releases/2004–04/hrae–riu040804.php

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

Government Sector

22. *April 12, Department of Homeland Security* — **Department of Homeland Security announces development of the Homeland Secure Data Network.** The U.S. Department of Homeland Security (DHS) announced a contract to initiate the implementation of the Homeland Secure Data Network (HSDN) on Tuesday, April 12. **The HSDN will provide DHS officials with a modern IT infrastructure for securely communicating classified information.** When completed the HSDN will be a private, certified, and accredited network that will fully support the mission goals of the department. **"The Homeland Secure Data Network will provide DHS personnel and their partners with a 21st century information technology infrastructure for securely communicating classified information,"** said Department of Homeland Security Secretary Ridge. The HSDN will significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the department's dependence on networks external to DHS. Looking to the future, the HSDN will be designed to be scalable in order to respond to increasing demands for the secure transmission of classified information among government, industry, and academia crucial to defending America from terrorist attacks.

Source: <http://www.dhs.gov/dhspublic/display?content=3444>

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

Emergency Services Sector

Nothing to report.

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

Information and Telecommunications Sector

23. *April 13, eSecurity Planet* — **Browser-based attacks surging.** The Computing Technology Industry Association (CompTIA), a global trade association based in Oakbrook Terrace, IL, reports that a new survey of 900 organizations shows that browser-based attacks are surging, and may pose the 'next significant security threat' to enterprise networks. **The study reports that 36.8 percent of the companies surveyed suffered a browser-based attack in the last six months.** That number is up 25 percent from when the same study was conducted last year. **These attacks, which are related to the recent spate of phishing scams, use a browser and user system permissions to allow an attacker to gain access to the computer to steal or destroy critical information.** The attacks generally occur when a user visits a Website that, on the surface, appears harmless, but contains malicious code that convinces the browser to execute commands designed to sabotage the machine or lift proprietary data or personal financial information. The Computing Technology Industry Association also reports that **while incidents of browser-based attacks are on the rise, computer viruses and worm attacks still far outweigh them.** The survey shows that 68.6 percent say viruses and worms are the most security threat they have to deal with.

Source: <http://www.esecurityplanet.com/trends/article.php/3339731>

24. *April 13, Federal Computer Week* — **IT pros see vendor mediocrity.** Six hundred federal information technology professionals surveyed in January graded the performance of manufacturers, integrators and resellers they do business with at about a C+ average, according to the survey from Market Connections Inc. The report, released this week, states that on 15 performance factors, no one factor got an average score higher than a B-. Forty-six percent of the respondents reported using a credit card to purchase IT products online, with an average purchase under \$2,500 for more than half of those surveyed. **The survey found that the respondents believe IT security and information sharing among agencies will be the most important initiatives in the immediate future to help agencies fulfill homeland security missions.**

Source: <http://fcw.com/fcw/articles/2004/0412/web-survey-04-13-04.asp>

25. *April 13, Microsoft* — **Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows.** This update resolves several newly-discovered vulnerabilities which are detailed on the Microsoft Website. **An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system,** including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to these issues and recommends that customers apply the update immediately.

Source: <http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx>

26. *April 13, Microsoft* — **Microsoft Security Bulletin MS04–012 Cumulative Update for Microsoft RPC/DCOM.** This update resolves several newly–discovered vulnerabilities in RPC/DCOM. Each vulnerability is documented on the Microsoft Website. **An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of the affected system.** An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends customers apply the update immediately.
Source: <http://www.microsoft.com/technet/security/bulletin/ms04–012.msp>
27. *April 13, Microsoft* — **Microsoft Security Bulletin MS04–013 Cumulative Security Update for Outlook Express.** This is a cumulative update that includes the functionality of all the previously–released updates for Outlook Express 5.5 and Outlook Express 6. Additionally, **it eliminates a new vulnerability that could allow an attacker who successfully exploited this vulnerability to access files and to take complete control of the affected system.** This could occur even if Outlook Express is not used as the default e–mail reader on the system. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install this update immediately.
Source: <http://www.microsoft.com/technet/security/bulletin/ms04–013.msp>
28. *April 13, Microsoft* — **Microsoft Security Bulletin MS04–014 Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution.** A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution. **An attacker who successfully exploited this vulnerability could take complete control of an affected system,** including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft recommends that customers install the update at the earliest opportunity.
Source: <http://www.microsoft.com/technet/security/bulletin/ms04–014.msp>

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:	[fetch #1 Virus (manual)]
Top 10 Target Ports	135 (epmap), 6129 (dameware), 137 (netbios–ns), 445 (microsoft–ds), 1434 (ms–sql–m), 80 (www), 3127 (mydoom), 2745 (urbisnet), 1025 (blackjack), 1026 (nterm)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	

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

General Sector

Nothing to report.

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

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) 883-3644

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

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at info@us-cert.gov or visit their Web page at www.uscert.gov.

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.