Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 16 March 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- CNET News reports Netcraft security says banks are increasing the risk of online fraud by not tackling the problem of cross−site scripting, an easily remedied Website loophole. (See item 6)
- The News Tribune reports the federally funded Highway Watch program generates between 200 and 300 calls a month nationally, with about one or two calls out of every 100 related to terrorism and passed along to the Department of Homeland Security. (See item 11)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact 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. *March 15, Reuters* — **More oil may not stop price rise.** The Organization of the Petroleum Exporting Countries (OPEC) oil producers on Tuesday, March 15, considered a Saudi proposal for a modest increase in output but said they could not guarantee to cap record−breaking crude prices. OPEC is under pressure from consumer countries to take action to bring prices down from $55 a barrel. Saudi Arabia is suggesting OPEC lift official output limits by 500,000 barrels a day (bpd), two percent, to 27.5 million bpd. Delegates said a committee of ministers from Iran, Kuwait and Nigeria recommended an increase be delayed until May 1 to allay concerns about a seasonal second quarter demand dip. "The price risks are more to the upside than the downside," said analyst Yasser Elguindi of Medley Global Advisors. "There is lot

more demand for the second half of the year than OPEC realized at the start of the year. They need to catch up to that reality," Elguindi said. With group output already close to a 25−year high, traders are concerned about OPEC's ability to meet rapid demand growth, led by China, in the second half of the year. "OPEC has done all it can do. This is out of the control of OPEC," said Qatar Oil Minister Abdullah al−Attiyah.
Source: http://www.washingtonpost.com/wp−dyn/articles/A37237−2005Mar 15.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *March 15, Environmental Protection Agency* — **Mercury emissions rule announced for power plants.** The Environmental Protection Agency (EPA) unveiled its new mercury rule for coal−fired power plants Tuesday, March 15. The Clean Air Mercury Rule (CAMR) is designed reduce mercury emissions from coal−fired power plants across the country. The CAMR will require reductions at electric utilities. Mercury is a persistent, toxic pollutant that accumulates in the food chain. While concentrations of mercury in the air are usually low, mercury emissions can reach lakes, rivers and estuaries and eventually build up in fish tissue. Americans are exposed to mercury primarily by eating certain species of fish. The CAMR limits mercury emissions from new and existing coal−fired power plants, and creates a market−based cap−and−trade program that will permanently cap utility mercury emissions in two phases: the first phase cap is 38 tons beginning in 2010, with a final cap set at 15 tons beginning in 2018. These mandatory declining caps, coupled with significant penalties for noncompliance, are designed to ensure that mercury reduction requirements are achieved and sustained.
Source: http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/91ab7266e65751b985256fc50067d9b0!OpenDocument

[Return to top]

Defense Industrial Base Sector

3. *March 15, Associated Press* — **European Union regulators aprove defense deal.** European Union regulators on Tuesday, March 15, approved a deal between Finmeccanica SpA of Italy and Britain's BAE Systems PLC to create a major joint venture in defense electronics. Finmeccanica announced in January that it had signed a final agreement with BAE to create Eurosystems, a set of three joint ventures in defense electronics. A BAE spokesperson said the deal would create a clearer management structure and increase the chances of landing contracts in an industry that is dominated by heavyweight manufacturers.
Source: http://www.washingtonpost.com/wp−dyn/articles/A36386−2005Mar 15.html

[Return to top]

Banking and Finance Sector

4. *March 15, Fiji Times (Fiji)* — **U.S. government helps Fiji combat money laundering.** The U.S. government donated US$60,000 to help strengthen regional measures in Fiji aimed at

combating money laundering. United States Ambassador to Fiji John Lyon presented the check to the South Pacific Forum's acting Secretary−General Iosefa Maiava on Monday, March 14. Maiava said the funding was timely because the Forum had organized a number of activities aimed at improving the skills of financial investigators in the region. He said the training would help investigators tackle money laundering within their own jurisdictions, generated by domestic criminal activity, and those by transnational−organized criminal groups.
Source: http://www.fijitimes.com/story.aspx?id=17875

5. *March 15, Las Vegas Review−Journal* — **Nevada officials frustrate potential identity theft victims.** Initially, authorities at a Nevada Department of Motor Vehicles (DMV) office said personal information of customers was safe after a recent theft. However, authorities are now saying that people who received licenses or identity cards at the 4110 Donovan Way bureau in North Las Vegas between November 25 and March 4 are at risk. Potential victims are frustrated. One person said she needed a copy of the police report DMV filed on the theft to forward the report to credit reporting companies to get an extended security alert that would watch for suspicious credit activity at no cost to her. However, police wouldn't release the report or take a new report in her name. "They're not actually victims of a crime until their information is used," said Sean Walker, a spokesperson for North Las Vegas police. Also, the DMV referred calls to an information hot line for which an incorrect number was inadvertently listed in the Saturday, March 12, issue of Review−Journal. However, it wasn't easy to get through to the correct number Monday, March 14. In 20 call attempts made by the Review−Journal, a reporter encountered busy signals, was put on hold, or was disconnected without getting through to an operator.
Source: http://www.reviewjournal.com/lvrj_home/2005/Mar−15−Tue−2005/news/26071396.html

6. *March 14, CNET News* — **Phishing hole left open by banks.** Banks are increasing the risk of online fraud by not tackling the problem of cross−site scripting, according to a security firm. An easily remedied Website loophole may be leaving banks and other companies that do business online more susceptible to phishing attacks, according to Netcraft. Online criminals are increasingly using cross−site scripting flaws to inject their own code into legitimate Web page URLs, the network security services company said in a note posted on its site Monday, March 14. With these sites, the attackers can try to dupe unsuspecting consumers into falling for phishing scams. Companies should expect to see more of the scripting threats, unless businesses carefully review server applications to eliminate the scripting glitch. Doing so would be more time−consuming than complicated, said Paul Mutton, an Internet services developer at Netcraft. Mutton also said banks, the most common targets of phishing threats, have done little to remedy the cross−site scripting problem.
Source: http://news.com.com/A+phishing+wolf+in+sheeps+clothing/2100−7349_3−5616419.html?tag=nefd.top

7. *March 14, CNET News* — **Zombie personal computers being sent to steal identities.** Bot nets, collections of compromised computers controlled by a single person or group, have become more pervasive and increasingly focused on identity theft and installing spyware, according to a report by the Honeynet Project, a security group that sets up heavily monitored systems, or honeypots, and allows them to be attacked report. The report, released on Monday, March 14, summarizes the findings of researchers who have tapped into more than 100

different bot nets since last summer. While many of the networks had been used to hit other bot nets with denial−of−service attacks, others had been used to gather sensitive identity information and install adware and spyware, a practice that is increasing, said Thorsten Holz, one of the primary authors of the paper. Over the past year, security experts have become increasingly wary of bot nets. Once used mainly by online vandals to attack each other, the large networks of compromised computers are now a tool for groups of criminals bent on making money through identity fraud or adware installation. A person whose computer is infected with bot software runs the risk of having sensitive information such as account passwords and credit card numbers sent to the controller of the network. Report: http://www.honeynet.org/papers/bots/
Source: http://news.com.com/Zombie+PCs+being+sent+to+steal+IDs/2100−7349_3−5616202.html?tag=nefd.top

[Return to top]

Transportation Sector

8. *March 15, Government Accountability Office* — **GAO−05−365: Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems (Report).** Mandated to screen all checked baggage using explosive detection systems at airports by December 31, 2003, the Transportation Security Administration (TSA) deployed two types of screening equipment: explosives detection systems (EDS), which use computer−aided tomography X−rays to recognize the characteristics of explosives, and explosives trace detection (ETD) systems, which use chemical analysis to detect traces of explosive material vapors or residues. This report assesses (1) TSA's use of budgeted funds to install EDS and ETD systems and the impact of initially deploying these systems, (2) TSA and airport actions to install EDS machines inline with baggage conveyor systems, and the federal resources made available for this purpose, and (3) actions taken by TSA to optimally deploy checked baggage screening systems. The Government Accountability Office (GAO) recommends that the Department of Homeland Security (DHS) direct TSA to take several actions needed to systematically evaluate baggage screening needs at airports, including identifying the costs and benefits of installing in−line EDS systems or stand−alone EDS machines in lieu of ETD machines, and prioritizing those airports where TSA would benefit by such actions. DHS generally concurred with GAO's findings and recommendations and described corrective actions that it has initiated or plans to take to address the issues identified.
Highlights: http://www.gao.gov/highlights/d05365high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−365

9. *March 15, The Business Journal (MN)* — **Mechanics' union authorizes Mesaba strike.** Members of the Aircraft Mechanics Fraternal Association (AMFA) have voted to authorize a strike against Mesaba Airlines. Ninety−two percent of the union's vote was in favor of authorizing a strike, according to the AMFA. The union represents 270 Mesaba mechanics. The National Mediation Board (NMB) must release both parties from negotiations before a mandatory 30−day cooling off period can begin. The mechanics can't strike until after that period is over. Mesaba Airlines operates as a Northwest Airlink affiliate under code−sharing agreements with Northwest Airlines Corp. Mesaba is a subsidiary of MAIR Holdings Inc. based in Minneapolis.

Source: http://twincities.bizjournals.com/twincities/stories/2005/03 /14/daily11.html

10. *March 14, USA TODAY* — **Airport officials push for government aid.** Airports are pushing the federal government to spend $5 billion on a new luggage screening system that could more accurately check for bombs, speed up passenger lines and save taxpayers billions of dollars. But the Bush administration says airports should pay for it themselves. More than 50 airports want to install the new equipment but haven't received federal money, even though a government audit says the system could pay for itself in just over a year. "They are not without the resources to do some of these projects on their own," says Transportation Security Administration (TSA) associate administrator Tom Blank. The new system uses conveyor belts to carry luggage from airline check−in counters through bomb−detection machines. At most airports now, TSA screeners lift and carry the bags. TSA is spending $958 million to install belt systems at nine airports. Those systems could be paid for and generate $1.3 billion in savings over seven years by eliminating 5,168 of 6,645 baggage screening jobs, the Government Accountability Office says. Belt systems typically have hefty costs −− up to $200 million −− that the airports say they can't afford. Airport officials want the federal government to pay three−quarters of the cost or more.
Source: http://www.usatoday.com/news/washington/2005−03−13−airport−s creeners_x.htm

11. *March 14, News Tribune (WA)* — **Program helps train truckers in security.** Officially called “Highway Watch,” the program generates between 200 and 300 calls a month nationally to a 24−hour center in rural Kentucky, said John Willard, spokesperson for the American Trucking Associations, the trade group for the nation’s truck drivers and the group that runs Highway Watch. About one or two calls out of every 100 are related to terrorism, and those get passed along to the Department of Homeland Security. Some have triggered FBI investigations, said Willard. Highway Watch started receiving federal money in 2004. This year, it will receive $21 million to recruit more of the nation’s 3.2 million truck drivers as well as bus drivers and other mass transit operators. With 50,000 volunteers signed up, the program has a goal of reaching 200,000 by next July. The course involves an introduction to what a threat is, and then instructors go through scenarios. If truckers spot something suspicious, first they call 911, and then they call the Highway Watch number. For more information:
http://www.highwaywatch.com
Source: http://www.thenewstribune.com/business/story/4680518p−433325 4c.html

12. *March 14, PostNewsweek Tech Media* — **Panel calls for secured border perimeter.** The United States, Canada and Mexico should create a common North American security perimeter by 2010 with combined visa, visitor screening, cargo inspection and political asylum policies, the chairmen of an independent task force of former government officials recommended on Monday, March 14. The governments should “strive toward a situation in which a terrorist trying to penetrate our borders will have an equally hard time doing so, no matter which country he elects to enter first,” the three chairmen of the Independent Task Force on the Future of North America said in a press release. The task force was co−created in October 2004 by the New York−based think tank the Council on Foreign Relations, as well as the Canadian Council of Chief Executives and the Consejo Mexicano de Asuntos Internacionales. The chairman also recommend harmonized visa and asylum regulations, joint inspection of container traffic and “synchronized screening and tracking of people, goods and vessels, including integrated ‘watch’ lists,” the chairmen said. “Like free trade a decade ago, a common security perimeter

for North America is an ambitious but achievable goal that will require specific policy, statutory and procedural changes in all three nations," they said.
Source: http://www.gcn.com/vol1_no1/daily-updates/35269-1.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *March 15, Agricultural Research Service* — **Genetic mapping lays groundwork for cattle disease treatments.** Agricultural Research Service (ARS) scientists at the National Animal Disease Center's Bacterial Diseases of Livestock Research Unit in Ames, IA, are producing maps that could one day lead researchers to discover preventative and therapeutic treatments for several important cattle diseases. For example, Mycobacterium paratuberculosis, the bacterium that causes Johne's disease, was sequenced in 2002 by Ames scientists. The sequencing and discovery of several genes will help differentiate the bacterium from other closely related bacterial species and could help in the detection of the disease and development of a vaccine. Meanwhile, other ARS researchers at Ames have either completed or are actively sequencing additional cattle pathogens. ARS microbiologists sequenced Brucella abortus, a bacterium that causes bovine brucellosis, a highly contagious bacterial disease that induces late-term abortions and infertility in cows. They hope to identify those genes that mediate protective immunity. Also, an ARS microbiologist is leading sequencing of the pathogen Leptospira borgpetersenii serovar hardjo, the most common cause of leptospirosis in cattle, using an automated analyzer for rapid analysis of the organism's genes. Leptospirosis causes abortions, stillbirths and weak offspring in cattle and swine. It can also reduce milk production in cows.
Source: http://www.ars.usda.gov/is/np/ha/han21.htm

14. *March 15, Times-Herald (CA)* — **Eggs from glassy-winged sharpshooter found in California wine region.** The discovery of a small clump of insect eggs could cause worries for California's Napa Valley wine industry. The Napa County Agricultural Commissioner's office has announced that the third glassy-winged sharpshooter egg cluster in a month has been found on a plant shipment. Even more troubling, the last batch of plants came from Lodi in San Joaquin County, a region not known to harbor the pest. The egg cluster was discovered Thursday, March 10, on ground cover plants bound for a landscaping project. Two previous egg clusters were found on February 9 and 14 on nursery shipments from Southern California. San Joaquin agricultural officials said they were notified of the sharpshooter find and have spent the last several days vigorously inspecting the stock of the Lodi nursery wholesaler that sent the plants. A sharpshooter infestation would pose a major threat to San Joaquin Valley's own 80,000 acres of grapes and its wholesale nursery industry, said Vicki Helmar, San Joaquin County's assistant agricultural commissioner. The insect is an efficient carrier of Pierce's disease, which kills grape vines by choking off their ability to move water within the plant.
Source: http://www.timesheraldonline.com/Stories/0,1413,296~31531~27 63497,00.html

[Return to top]

Food Sector

15. *March 14, Food and Drug Administration* — **FDA officials issue health advisory about certain soft cheeses.** The Food and Drug Administration (FDA) is advising that some soft cheeses made with raw milk present a health risk. Such cheeses can cause several serious infectious diseases including listeriosis, brucellosis, salmonellosis, and tuberculosis. Recently, cases of tuberculosis in New York City have been linked to consumption of queso fresco style cheeses, either imported from Mexico or consumed in Mexico. The raw milk soft cheeses of most concern can originate from Mexico and Central American countries. Queso fresco style cheese, which is soft and white, can include Queso Panela, Asadero, Blanco, and Ranchero, among other styles and may be imported or produced in the U.S. FDA recommends that consumers do not eat any unripened raw milk soft cheeses from Mexico, Nicaragua, or Honduras. Data show that they are often contaminated with pathogens. FDA further recommends that consumers not purchase or consume raw milk soft cheeses from sources such as flea markets, sellers operating door−to−door or out of their trucks or shipped or carried in luggage to them from Mexico, Nicaragua, or Honduras. FDA further advises that there is some risk of infection from a number of pathogenic bacteria for anyone who eats raw milk soft cheese from any source.
    Source: http://www.fda.gov/bbs/topics/news/2005/NEW01165.html

16. *March 14, Food and Drug Administration* — **Tuna salad recalled in Northeast.** Hans Kissle is conducting a voluntary recall of all prepared tuna fish salad sold in the retail deli section because it has the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections. Hans Kissle tuna fish salad is available for purchase in the deli section of select supermarkets under the Hans Kissle, Shaw's, Stop & Shop, and Block & Barrel label. The product was distributed in Massachusetts, Rhode Island, New Hampshire, Vermont, New York, and New Jersey. No illnesses have been reported related to this recall.
    Source: http://www.fda.gov/oc/po/firmrecalls/hanskissle03_05.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *March 15, Reuters* — **Doctors suspect bird flu killed Vietnamese man.** A Vietnamese man who died Sunday, March 13, may have been killed by the bird flu virus that has claimed the lives of 46 people in Asia since 2003, a doctor said Tuesday, March 15. The man died in the southern province of Kien Giang, three days after he was transferred from the Chau Thanh

district health center, where he had been on a respirator, Dr. Tran Thanh Tung said. "We have sent the patient's samples for bird flu tests," said Tung, who heads the anti−bird flu team at Kien Giang's General hospital. He gave no further details.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=7904260

18. *March 15, Agence France Presse* — **WHO officials seek details from North Korea over reported outbreak of bird flu.** The World Health Organization (WHO) said Tuesday, March 15, it had asked North Korea for information after a news agency reported there had been an outbreak of bird flu at a farm in the capital, Pyongyang. "Our regional office has requested more information from the Ministry of Health. This report is based on conversations by traveling businessmen so right now it's at the level of rumor and we're in the process of verification," said WHO spokesperson Dick Thomson. If confirmed, it would be the first time that bird flu, which has caused serious health risks in Southeast Asia and China, has hit the isolated communist state.
Source: http://www.tdg.ch/tghome/tgnews.detailcateg.YWZwLmNvbToyMDA1MDMxNTowNTAzMTUxMDUxNTQuZXpiZjR6dnU6MQ==.1.0.html

19. *March 15, American Chemical Society* — **Microbial forensics.** The biological and ecological complexity of most biothreat agents present forensic microbiologists with a number of significant analytical and interpretive challenges. The U.S. is in the process of developing a strong microbial forensic program to attribute and prosecute such attacks, and perhaps deter them. "It is imperative to establish robust microbial forensic capabilities, with the power of the methods, results, and interpretations well understood and defensible," said Randall Murch, associate director for research program development at Virginia Tech, formerly deputy director of the FBI's Laboratory and Investigative Technology Divisions. "An effective program requires relevant, exploitative, fully validated methods and uses in all aspects of the forensic investigative process," Murch said. "This ranges from sample collection to interpretation of results, while achieving full integration into investigation, prosecution, intelligence, and decision making. Since the results of a microbial forensics investigation could be used for either criminal prosecutions or those at the national level, we must be sure that the methods and results will be admissible in court, and must be accepted by senior government decision makers."
Source: http://www.newswise.com/articles/view/510364/

[Return to top]

Government Sector

20. *March 15, Federal Computer Week* — **Homeland security to use geographic application.** Department of Homeland Security officials will use an application that mines data for geographic references that can be depicted on a map. Officials at the Information Analysis and Infrastructure Protection Directorate recently signed a one−year license to use a geographic information system application developed by MetaCarta, headquartered in Cambridge, MA. Randy Ridley, the company's vice president and general manager for federal systems, said several software applications provide similar functions but none can bridge the gap between so−called unstructured content and digital mapping. About 90 percent of data within an organization is unstructured, such as e−mail messages, reports, interviews and other documents.

The application, which is also used in the intelligence community as well as the Department of Defense, can fuse data from multiple databases. For example, if there were three reports about suspected individuals going to a flight training center in the same place, the application would be able to fuse that information and depict it on a map.
Source: http://www.fcw.com/article88302

[Return to top]

Emergency Services Sector

21. *March 15, Chicago Tribune (IL)* — **Illinois county to open homeland security operations center.** Will County, IL, plans to join with a private partner to open a homeland security operations center. The facility, to be called the Will County Solution Center, would be eligible for federal grant money from the U.S. Department of Homeland Security, county officials said Monday, March 14. The county's Emergency Management Agency and its emergency operations center, both located in the county building in downtown Joliet, would move to the facility, Will County Executive Larry Walsh said. "With our infrastructure and facilities −− like nuclear power plants, oil refineries, major interstate highways and one of the largest intermodal facilities in the country −− and proximity to Chicago, Will County has unique needs," Walsh said. The 80,000−square−foot operations facility will be completed in 2007. Sheriff Paul Kaupus said the facility would have technology that is not now available to the county's emergency operations center.
Source: http://www.chicagotribune.com/news/local/southsouthwest/chi−0503150321mar15,1,4465688.story?coll=chi−newslocalssouthwest −hed&ctrack=1&cset=true

22. *March 15, IDG News Service* — **WebTV virus writer sentenced to prison.** A Louisiana man was sentenced to six months in prison for sending a malicious program using e−mail that caused Microsoft WebTV customers to call the 911 emergency service without their knowledge, according to a statement released by the U.S. Attorney's Office for the Northern District of California. David Jeansonne, 44, pled guilty in February to charges of intentionally causing damage to computers and causing a threat to public safety. He was sentenced on Monday, March 14, by U.S. District Judge Ronald Whyte and will have to spend an additional six months of home detention and pay $27,100 to Microsoft after he is released, the U.S. Attorney's Office says. WebTV, which is now known as MSN TV, is a Microsoft service that allows subscribers to browse the Web and connect to the Internet through their television sets.
Source: http://www.pcworld.com/news/article/0,aid,120050,00.asp

[Return to top]

Information Technology and Telecommunications Sector

23. *March 15, SecurityFocus* — **LimeWire Gnutella client two vulnerabilities.** LimeWire client contains two vulnerabilities that allow a remote user access to many or all files on a users machine. These vulnerabilities result from inappropriate handling of "resource get" requests and "magnet" requests. Gnutella "push style" requests are not vulnerable, so a firewall that blocks access to the magnet port blocks the attack. The files accessible to a remote attacker

include all of the user's private, local files, and any file on the machine if the user has administrator privileges. Upgrade to LimeWire version 4.8.0:
http://www.limewire.com/english/content/home.shtml
Source: http://www.securityfocus.com/archive/1/393146?ref=rss

24. *March 15, K−Otik Security* — **Apache Tomcat "AJP12" remote denial of service vulnerability.** A new vulnerability was identified in Apache Tomcat, which may be exploited by attackers to conduct Denial of Service attacks. The flaw resides in the implementation of the AJP12 protocol and may allow a remote attacker who sends a specially crafted request, to cause Tomcat to stop processing requests. Update to Apache Tomcat 5.5.8:
http://jakarta.apache.org/site/downloads/downloads_tomcat−5. cgi
Source: http://www.k−otik.com/english/advisories/2005/0262

25. *March 14, SecurityTracker* — **paFileDB input validation errors permit SQL injection and cross−site scripting attacks.** An input validation vulnerability in 'viewall.php' and 'category.php' permit a remote user to inject SQL commands and conduct cross−site scripting attacks. No solution is currently available.
Source: http://www.securitytracker.com/alerts/2005/Mar/1013426.html

26. *March 14, TechWeb News* — **Weekend attack infects hosting servers.** The Internet Storm Center (ISC) tracked a large−scale hack over the weekend that infected site−hosting servers, which in turn transformed all the hosted sites into distributors of malicious code. "We have received reports and evidence that a number of companies that provide shared hosting Web servers have had their servers exploited and all of the customer homepages modified so that visitors are attacked," said the Storm Center's Daniel Wesemann Sunday, March 13, in an online posting. It seems that the attack used both direct and indirect means to infect users, said the ISC. But ICS also found some evidence that a DNS cache poisoning attack was part of the program. "We are not quite sure yet how this is being done, as the files that we've received so far do not seem to contain DNS/DHCP poisoning code." This latest incident of DNS cache poisoning is unrelated to an earlier event this month, which was created by exploiting vulnerabilities in Symantec's gateway products.
Source: http://www.techweb.com/wire/security/159402730

27. *March 14, Government Computer News* — **Air Force to get Microsoft security patches before official release.** The Air Force now has a jump−start on implementing Microsoft security patches thanks to a plan that allows the department to receive beta test versions of patches. Under the company’s Security Update Validation Program, the Air Force will receive beta patches before they are officially released. After the department tests them, the patches will be distributed to other federal agencies. The Air Force is “in discussions” with the Defense Department about ways to bring the security services concept to other branches of the military and federal agencies, according to John Gilligan, Air Force CIO. Under the program, Microsoft will identify vulnerabilities and implement fixes across the enterprise.
Source: http://www.gcn.com/vol1_no1/daily−updates/35271−1.html

28. *March 13, K−Otik Security* — **MySQL MaxDB Web Agent multiple denial of service vulnerabilities.** Several input validation errors have been identified in MySQL MaxDB and SAP DB Web Agent, which may be exploited by remote attackers to cause a Denial of Service.

A remote attacker can request the function with invalid parameters to cause a null pointer dereference resulting in a crash of MySQL MaxDB Web Agent. Update to MySQL MaxDB 7.5.00.24: http://dev.mysql.com/downloads/maxdb/7.5.00.html
Source: http://www.k−otik.com/english/advisories/2005/0263

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: Several vulnerabilities were identified in MySQL, which may be exploited by local attackers to execute arbitrary commands or obtain elevated privileges. For more information, please visit the following link: http://www.k−otik.com/english/advisories/2005/0252

Current Port Attacks

Top 10 Target Ports	[fetch Target Ports (auto)] [fetch Target Ports (manual)]

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[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:

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

Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

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

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

DHS/IAIP Disclaimer