Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 09 March 2005

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

Daily Highlights

- InternetNews reports phishing fraudsters are using a pair of Domain Name System exploits to help give them the illusion of credible domains as part of their latest ploy to get people to part with sensitive information. (See item 12)
- The National Transportation Safety Board has criticized the New York City Department of Transportation in the 2003 Staten Island Ferry crash that killed 11 passengers, saying tougher medical screening of ferry captains and safer operating procedures are needed. (See item 15)
- The Sun−Sentinel reports a live hand grenade was found on a counter at Miami restaurant on Tuesday; it was disarmed by the bomb squad before it could explode. (See item 33)

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 08, The Globe and Mail (Canada)* — **Report warns about electricity crunch in Canada.** Canada has enough electricity to meet current demand, but even power−rich Quebec and British Columbia (BC) face potential problems down the road, Toronto−Dominion (TD) Bank says. In fact, like most other regions across the country, Quebec and BC have already experienced a deterioration in supply−demand positions in recent years as shown by a combination of declining power exports, rising imports and dropping reserve margins, TD said

in a report on electricity in Canada released Monday, March 7. As well as seeking out new sources of supply, the electricity sector will need to spend massive amounts of money to upgrade aging power transmission and distribution networks, while major expenditures also will be required just to accommodate soaring economic growth in some regions. However, government authorities also must encourage conservation, in particular by moving further toward market−based pricing for electricity, the report says. According to the U.S. Energy Information Administration, Canada enjoys a vigorous electricity trade with the United States, and the electricity networks of the two countries are heavily integrated. In 2003, Canada exported 29.3 billion kilowatt hours (Bkwh) of electricity to the U.S. while importing 23.6 Bkwh from the U.S. Report: http://www.td.com/economics/special/electricity05.pdf Source: http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20050308/RELEC08/TPBusiness/Canadian

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *March 08, Taunton Gazette (MA)* — **Massachusetts environtmental officials notified of chemical spill.** Officials at Harodite Industries, Inc., alerted the Massachusetts Department of Environmental Protection (DEP) on Monday, March 7, about a sodium hydroxide spill caused by an overflow of one of its tanks near the Three Mile River in Taunton, MA. According to Aaron M. Albert, Chief Operating Officer of Harodite Industries, in addition to the DEP, Clean Harbors, the U.S. Coast Guard, the Taunton Fire Department and the Dighton Fire Department were called to the scene. Albert said it could take two business days to clean up the spill. DEP Spokesperson Ed Coletta estimated the spill to be least 700 gallons, and he said sodium hydroxide does "dissipate" in water and should not be a problem for the river. In addition, Coletta said the chemical did not come into contact with people or businesses. Source: http://www.zwire.com/site/news.cfm?newsid=14100111&BRD=1711&PAG=461&dept_id=24232&rfi=6

3. *March 07, Government Accountability Office* — **GAO−05−163: Hazardous Waste Sites: Improved Effectiveness of Controls at Sites Could Better Protect the Public (Report).** The Environmental Protection Agency’s (EPA) Superfund and Resource Conservation and Recovery Act (RCRA) programs were established to clean up hazardous waste sites. Because some sites cannot be cleaned up to allow unrestricted use, institutional controls—legal or administrative restrictions on land or resource use to protect against exposure to the residual contamination −− are placed on them. The Government Accountability Office (GAO) was asked to review the extent to which (1) institutional controls are used at Superfund and RCRA sites and (2) EPA ensures that these controls are implemented, monitored, and enforced. GAO also reviewed EPA’s challenges in implementing control tracking systems. To address these issues, GAO examined the use, implementation, monitoring, and enforcement of controls at a sample of 268 sites. To ensure the long−term effectiveness of institutional controls, GAO recommends that EPA (1) clarify its guidance on when controls should be used; (2) demonstrate that, in selecting controls, sufficient consideration was given to all key factors; (3) ensure that the frequency and scope of monitoring efforts are sufficient to maintain the effectiveness of controls; and (4) ensure that the information on controls reported in new tracking systems accurately reflects actual conditions. EPA generally agreed with GAO’s

recommendations. Highlights: http://www.gao.gov/highlights/d05163high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−163

[Return to top]

Defense Industrial Base Sector

4. *March 08, Associated Press* — **Lockheed Martin machinists strike in Georgia.** Machinists went on strike at a Lockheed Martin plant on Tuesday, March 8, over stalled contract talks. At issue between the company and the roughly 2,800 members of the International Association of Machinists Local 709 are pay, health care premiums and retiree insurance benefits. No new negotiations are scheduled. The plant builds F/A−22 Raptor fighters and C−130J transports, and both workers and management are wary about possible cuts in U.S. defense spending.
Source: http://www.nytimes.com/aponline/business/AP−Lockheed−Martin− Strike.html

5. *March 08, Washington Post* — **U.S. increasingly looks abroad for competitive defense contracts.** The Pentagon is increasingly shopping overseas for its weapons, ending a long made−in−America tradition that assured U.S. defense contractors of nearly exclusive sales to their best customer. The consolidation of the defense industry in the 1990s reduced the number of domestic defense companies so sharply that the Pentagon has been forced to widen the field of bidders to keep costs down, industry analysts said. For some products, only one U.S. manufacturer exists. Chicago−based Boeing Corp. is the last domestic maker of wide−body jets, forcing the Pentagon to consider Europe's Airbus SA if it wants a competition. With the Pentagon's budget squeezed by war costs and deficit concerns, military leaders are increasingly willing to buy a foreign product rather than pay more to develop a U.S. alternative, analysts said. The Pentagon's purchases overseas could have a silver lining for American contractors: Foreign governments may be more willing to buy U.S. products. Like its counterpart in the United States, the European defense industry also has consolidated and developed expertise, and is aggressively pursing work with the Pentagon, which is still flush with cash compared with their nations' defense departments.
Source: http://www.washingtonpost.com/wp−dyn/articles/A15461−2005Mar 7.html

[Return to top]

Banking and Finance Sector

6. *March 09, Sydney Morning Herald (Australia)* — **Australian online bankers face double layer of security.** Internet banking customers in Australia will be required to use mobile phones or carry plastic tokens to log into their accounts as banks tighten up security for online services. The chief executive of the Australian Bankers' Association, David Bell, said an industry standard requiring all banks to use two methods of identifying internet customers would be introduced later this year. Under the standard, each bank will choose its own method of secondary identification, which Bell said would be based on "something customers have," as distinct from "something they know." Research by the bankers' group has found that customers do not want to use biometric devices that involve physical contact, such as fingerprints, because of privacy concerns. Banks are testing systems that send text messages to customers when they

first enter a bank's website. The message contains an extra number that is needed to complete the transaction. A spokesperson for the Australian Consumers' Association, Lisa Tait, said banks should not be charging customers for security devices and they should also provide updated anti−virus software free of charge. "Online banking is cheap for banks," she said. "After all, going into a branch is more secure."
Source: http://smh.com.au/news/National/Online−bankers−face−double−layer−of−security/2005/03/08/1110160830039.html

7. *March 08, Associated Press* — **Identity equipment stolen from Nevada Department of Motor Vehicles.** Authorities are worrying what thieves could do with about 1,700 blank driver's licenses stolen from a Nevada Department of Motor Vehicles (DMV) office in North Las Vegas. Thieves rammed a truck into the office about 1:00 a.m. Monday, March 7, where they also loaded up and took a digital license camera and camera computer, plus a license printer. Police think it took less than 20 minutes. Investigators say it looks like the thieves now have almost everything they need to make fake ID's. However, DMV officials say all that equipment might prove useless. It doesn't contain any driver information, and it won't work unless it's connected with the DMV mainframe computer in Carson City.
Source: http://www.krnv.com/Global/story.asp?S=3046165&nav=8faOXDm9

8. *March 08, Association for Payment Clearing Services* — **United Kingdom card fraud losses increase.** According to figures released on Tuesday, March 8, by the Association for Payment Clearing Services (APACS), the United Kingdom (UK) payments association, UK card fraud losses totaled almost US$1 billion in 2004, up by 20% compared to 2003. The rise is attributed to fraudsters increasing their illegal activity. They are also targeting other areas such as card−not−present and identity fraud. Card−not−present fraud continues to be the biggest fraud type (up by 24%), however these losses only grew in proportion to the number of businesses now offering transactions made by phone, fax or online. Online credit card payments have increased five−fold since 1999, to the point that 10% of all credit card spending now takes place online. Identity theft on cards has grown significantly over the last two years (up 22%), but remains a small proportion of overall fraud losses. Counterfeit card fraud increased slightly (up 17%) and there was a small rise in fraud on lost and stolen cards (up 2%). Together fraud on lost and stolen cards and counterfeit cards accounted for almost half (48%) of all losses.
Source: http://www.apacs.org.uk/downloads/cardfraudfigures%20national&regional%20−%208mar05.pdf

9. *March 08, IT Week* — **Online blackmail grows.** Companies are being advised to ensure their systems are protected against denial−of−service (DoS) attacks, as the problem of online blackmail is growing. According to Duncan Hine, business center director at Qinetiq, formerly the United Kingdom government's Defense Evaluation and Research Agency, attacks on company systems are becoming more professional, and now often involve organized gangs. Hine said the number of blackmail threats is growing steadily. In response, firms should establish procedures for coping with threats and attacks in advance. "Companies that have not prepared face a problem," Hine warned. "There is real danger in reacting on the hoof," he added. Furthermore, firms should not assume that only well−known organizations will be targeted. "The targets will not be the larger firms as they have resilient hosting and counter−measures in place. This is not the case for smaller firms," warned Hine.
Source: http://www.itweek.co.uk/news/1161777

10. *March 08, Associated Press* — **Man sentenced in ChoicePoint identity theft case.** A Nigerian national who stole the identities of thousands of people has been sentenced to 5.5 years in federal prison. Adedayo Benson was also ordered in Los Angeles court on Monday, March 7, to pay nearly $155,000 in restitution to ten financial companies. He and his sister were arrested in 2002 on charges of tapping into several public records databases, gaining access to records of over 7,000 people and using their identities to buy at least one million dollars in merchandise. Authorities say the siblings posed as real estate agents and opened accounts with ChoicePoint, Advantage Financial and Equifax. Benson's sister was sentenced to 4.5 years in prison.
Source: http://www.kesq.com/Global/story.asp?S=3045143

11. *March 07, Federal Times* — **Lost data prompts Bank of America to tighten handling of federal accounts.** After losing tapes with more than one million federal employees' personal information, Bank of America has changed how it handles sensitive backup information on federal accounts, the bank told government officials. For security reasons, the bank could not say what the changes were, General Services Administration Administrator (GSA) Stephen Perry said in a March 4 letter to Senator Susan Collins (R−ME). In December, Bank of America lost five backup tapes, two of which had personal information from 1.2 million federal SmartPay accounts. Employees enroll in SmartPay to pay for work−related purchases, and travel and fleet expenses. Perry told Collins that Bank of America is using "sophisticated monitoring tools to look for unusual or fraudulent activity." The bank has not found any evidence that the tapes' information has been compromised.
Source: http://federaltimes.com/index.php?S=705180

12. *March 07, InternetNews* — **Domain Name System phishing attacks on the rise.** Phishing fraudsters are using a pair of Domain Name System (DNS) exploits to help give them the illusion of credible domains as part of their latest ploy to get people to part with sensitive information. According to research firm Netcraft, phishers have begun to use wildcard DNS records to help trick unsuspecting users into giving up their information about their identity. Wildcard DNS is designed to help users arrive at their intended Web destination by redirecting mistyped and/or errant addresses. The technique, known as DNS cache poisoning, is also being utilized by phishers in an attack know known as "pharming" where a poisoned DNS server redirects users to the phisher's Website. The "poison" is essentially false DNS information that is injected into a vulnerable DNS server. According to Netcraft, an attack on Saturday, March 5, exploited a known vulnerability in Symantec's firewall product. The firewall vulnerability had not been patched by Symantec last year, however, Symantec issued an emergency patch for the DNS poisoning hole on Friday, March 4. The Saturday attack redirected user requests from eBay, Google and weather.com to a trio of phisher−directed sites.
Source: http://www.internetnews.com/dev−news/article.php/3488216

[Return to top]

Transportation Sector

13. *March 08, Associated Press* — **Delta in talks with SkyWest to sell regional feeder carriers.** Delta Air Lines Inc. is in talks with SkyWest Inc., to sell the Utah airline one or two of its regional feeder carriers. Delta has said publicly in the past that it was evaluating all of its assets,

including its feeder carriers Comair and Atlantic Southeast Airlines, as it seeks to return to profitability. The company lost more than $5 billion last year and has been racked by continually high fuel prices. Bradford Rich, chief financial officer of SkyWest, said at an investor conference Monday, March 7, in Orlando, FL, that the discussions were in the early stages.
Source: http://biz.yahoo.com/ap/050308/delta_regional_carriers_2.htm l

14. *March 08, Chester Sun Times (IL)* — **Blagojevich administration hosts transportation safety summit.** The administration of Illinois Governor Rod Blagojevich, led by Illinois Department of Transportation (IDOT) Secretary Tim Martin, held the first Illinois Highway Safety Summit to begin development of the state's first−ever Comprehensive Highway Safety Plan (CHSP). The American Association of State Highway and Transportation Officials encourage all states to develop a CHSP as a way to reduce traffic fatalities. A CHSP will focus on what are referred to as the four E's of highway safety: Engineering, Enforcement, Education, and Emergency Services. Working with public and private transportation professionals, state and local law enforcement officials and others to determine what needs to be included in the plan, IDOT's Division of Traffic Safety and Bureau of Safety Engineering will be responsible for developing and implementing the CHSP. A second safety summit for development of the plan will be held later this month in Springfield, IL. Approval of the plan is expected later this year and implementation is expected to begin in the fall or winter of this year.
Source: http://www.suntimesnews.com/2/news_archive/mar_05archives/03 08blag.htm

15. *March 08, Associated Press* — **Ferry crash probe cites NYC.** The National Transportation Safety Board (NTSB) on Tuesday, March 8, sharply criticized New York City and the Coast Guard in the 2003 Staten Island Ferry crash that killed 11 passengers, saying tougher medical screening of ferry captains and safer operating procedures were needed. NTSB chairperson Ellen Engleman Conners said the crash "was a wake−up call to all modes of transportation," and said closer review was needed of the effect of certain prescription drugs on transportation workers. The Staten Island ferries have an annual ridership of 19 million, and the crash of the Andrew J. Barberi was one of the worst mass−transit disasters in New York history. Ferry pilot Richard Smith has pleaded guilty to 11 counts of manslaughter, acknowledging he neglected his duties by taking medications that made him lose consciousness at the helm. In its report, the NTSB criticized "the failure of the New York City Department of Transportation to implement and oversee safe, effective operating procedures." Better emergency drills, training of ship crews and safety management systems are needed, the board said. In addition, NTSB recommended that the Coast Guard revise its procedures so that the results of physicals are reported each year. Synopsis of NTSB report:
http://www.ntsb.gov/publictn/2005/MAR0501.htm
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/n/a/2005/03/08/
national/w105916S14.DTL

16. *March 08, Department of Transportation* — **Grants to enhance safety at Montana airports.** Federal grants totaling nearly $17 million will help make Montana airports safer and more efficient, Department of Transportation Secretary Norman Y. Mineta announced on Tuesday, March 8. The grants include $11.7 million to install an instrument approach aid at Great Falls International Airport and $1 million to continue construction of a new airport in Broadus, including paving, runway lighting and a precision approach path indicator. Seven airports will

receive money for projects that include rehabilitating and extending runways, constructing taxiways, improving runway safety areas, purchasing firefighting vehicles and upgrading a terminal. Among other grants, Helena Regional Airport will receive $1.2 million to modify the terminal building to improve passenger service and the efficiency of operations, and to acquire a replacement aircraft rescue and firefighting vehicle. Liberty County Airport will receive $66,500 to rehabilitate runway 7/25 and taxiways, maintain an apron, and install a wind cone and runway guidance sign. The funds come from the Airport Improvement Program of the Department of Transportation's Federal Aviation Administration.
Source: http://www.dot.gov/affairs/dot4205.htm

17. *March 08, Department of Transportation* — **Grants to expand and enhance safety at South Dakota airports.** Federal grants totaling nearly $7.5 million will help to enhance safety and expand capacity at airports in South Dakota, Department of Transportation Secretary Norman Y. Mineta announced on Tuesday, March 8. Twenty−four airports will receive money for projects that include rehabilitating and extending runways, constructing runways and taxiways, renovating terminals and other structures, and purchasing fire and rescue equipment. Among other grants, Brookings Municipal Airport will receive $599,757 to buy an aircraft rescue and firefighting vehicle and construct an aircraft rescue and firefighting building. Also, Hot Springs Municipal Airport will receive $106,750 to install weather reporting equipment. The funds come from the Airport Improvement Program of the Department of Transportation’s Federal Aviation Administration.
Source: http://www.dot.gov/affairs/dot4305.htm

18. *March 07, Associated Press* — **CSX agrees to $1.5M settlement.** The CSX Corp. freight railroad company has agreed to several safety measures for hundreds of street crossings statewide under a $1.5 million settlement, New York state Attorney General Eliot Spitzer said Monday, March 7. Under the voluntary agreement, CSX will perform a series of safety monitoring and reporting changes and pay for a $500,000 pilot program that would reimburse local police for their costs in protecting railroad crossing identified as having malfunctioning safety equipment, Spitzer said. CSX agreed to pay $1 million to the state to end the investigation, Spitzer said. "It is critical that railroad companies maintain the highest safety standards possible," Spitzer said in a statement released Monday. "As a result of this agreement, CSX will undertake a number of reforms that will produce the quickest response possible to any potential crossing safety problems."
Source: http://biz.yahoo.com/ap/050307/railroad_inquiry_3.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19.

March 08, Statesman Journal (OR) — **Diseased salmon destroyed.** Disease problems have forced Oregon Department of Fish and Wildlife (ODFW) officials to kill 23,600 spring−run chinook salmon that were being raised at a hatchery in northeast Oregon. The fish had been scheduled for release in the Lostine River sometime during the next two weeks. But fish in one of the raceways have been battling a major outbreak of infectious hematopoietic necrosis virus and bacterial kidney disease since January, and the fish were not responding to treatment, said Bruce Eddy, the acting North Region manager for ODFW.
Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20050308/OUTDOORS/503080339/1034

20. *March 07, Animal and Plant Health Inspection Service* — **Oriental fruit fly eradicated in California.** The U.S. Department of Agriculture Monday, March 7, announced the eradication of the Oriental fruit fly in Orange, CA. The last finding of an Oriental fruit fly in the state was September 29, 2004. Additionally, the Animal and Plant Health Inspection Service is lifting the Oriental fruit fly quarantine in the state to relieve restrictions that are no longer needed to prevent the spread of the pest to non−infested areas of the U.S. Orange County was the last remaining area in California that the U.S. quarantined for the Oriental fruit fly. The Oriental fruit fly is a destructive pest of citrus and other types of fruit, nuts, vegetables and berries. The short life cycle of the Oriental fruit fly allows rapid development of serious outbreaks, which can cause severe economic losses. Heavy infestations can cause complete loss of crops.
Source: http://www.aphis.usda.gov/lpa/news/2005/03/offeradi_ppq.html

21. *March 07, Desert Morning News (UT)* — **Elk implanted with computer chips.** Computer chips were implanted into six elk March 3, the first domesticated elk in the U.S. to be entered into the National Animal Identification System (NAIS). The implants are part of a Utah Department of Agriculture and Food (UDAF) pilot program to "speed up and streamline our systems of identifying animals with health issues," said Larry Lewis, UDAF spokesperson. When NAIS is in full operation, agriculture officials hope to be able to trace all animals exposed to a diseased animal within 48 hours. To participate in NAIS, a rancher, feedlot owner, slaughter plant, etc., first registers its premises. That creates a master file for the location. As an animal is moved, it keeps the same chip number. But the number is moved from one premise file to another in the NAIS database.
Source: http://deseretnews.com/dn/view/0%2C1249%2C600116843%2C00.htm l

[Return to top]

Food Sector

22. *March 08, Agricultural Research Service* — **Antibiotic resistant Salmonella.** Antibiotics have been used for years to fight bacterial infections, but some bacteria are developing resistance to these antimicrobial drugs. Agricultural Research Service (ARS) scientists are tracking antimicrobial resistance and seeking ways to minimize it. ARS microbiologist Paula Fedorka−Cray leads a team that is testing for antimicrobial resistance in food−borne microbes. In these studies, bacterial samples are taken from sick farm animals, healthy farm animals, and animal slaughter facilities. The lab's scientists then isolate, test and characterize more than 17,000 bacterial samples a year. Patterns of resistance are difficult to discern because bacteria don't react predictably and uniformly to antibiotic treatment. Salmonella has more than 2,400

different types, and each one appears to develop resistance to antibiotics at a different rate. Of all Salmonella types tested from 1997 to 2003, the rate of single−drug resistance has remained relatively stable at 9.5 percent of the samples. However, the number of Salmonella types that are resistant to more than five drugs rose from 11 percent to 20 percent. Those that are resistant to more than 10 drugs rose from 0.8 percent to almost six percent.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *March 08, Associated Press* — **Seven Vietnamese patients found infected with bird flu after samples retested.** The World Health Organization (WHO) says seven Vietnamese patients who initially tested negative for bird flu have been found to be carrying the virus after their samples were retested −− suggesting that avian influenza may be more widespread than originally believed. All seven, who were first tested in January, have since recovered, WHO regional spokesperson Peter Cordingley said Tuesday, March 8. The WHO will wait to receive more details on the seven cases before adding them to the overall tally for Vietnam, Cordingley said. The samples were sent to a laboratory in Japan as part of a move earlier in the year by the WHO, Japan's National Institute of Infectious Diseases and the U.S. Centers for Disease Control and Prevention, to work with health authorities in Vietnam to improve the reliability of diagnostic tests. The seven people, all from southern Vietnam, did not have clinical or epidemiological factors typical of previous bird flu cases, the institute official said. One patient had tuberculosis.
Source: http://asia.news.yahoo.com/050308/ap/d88mpioo5.html

24. *March 08, Wired* — **Pigs hold clues to man−made flu.** Samples taken from South Korean pigs contain genes from a human flu virus created by scientists in 1933. The presence of a man−made human flu virus in pigs may be worrisome because a man−made virus has no business in pigs. Also, viruses often use pigs as a conduit to humans, who would have little or no immune resistance to this particular strain of flu since no one has been exposed to it. Sang Heui Seo, of Chungnam National University in South Korea, entered six genetic sequences from pigs into GenBank in late October. Henry Niman, founder of Recombinomics and a researcher who has studied the spread of bird flu for two years, came across the data in late November, and noticed they contained between three and seven genes from the WSN33 virus, which was created in 1933 by a British lab that was researching the 1918 flu pandemic. He reported the presence of the human WSN33 genes in Seo's samples to World Health Organization officials in early December. Labs in Hong Kong and at the University of Wisconsin are now verifying the samples.
Source: http://www.wired.com/news/medtech/0,1286,66824,00.html?tw=wn_tophead_3

[Return to top]

Government Sector

25. *March 08, Government Accountability Office* — **GAO−05−127: Gun Control: FBI Could Better Manage Firearm−Related Background Checks Involving Terrorist Watch List Records (Report). Written on January 19.** Membership in a terrorist organization does not prohibit a person from owning a gun under current law. Thus, during presale screening of prospective firearms purchasers, the National Instant Criminal Background Check System historically did not utilize terrorist watch list records. However, for homeland security and other purposes, the Federal Bureau of Investigation (FBI) and applicable state agencies began receiving notices (effective February 3, 2004) when such screening involved watch lists records. The Government Accountability Office (GAO) determined (1) how many checks have resulted in valid matches with terrorist watch list records, (2) procedures for providing federal counterterrorism officials relevant information from valid−match background checks, and (3) the extent to which the FBI monitors or audits the states' handling of such checks. Proper management of firearm related background checks involving valid matches with terrorist watch list records is important. GAO recommends that the Attorney General (1) clarify procedures to ensure that the maximum amount of allowable information from these background checks is consistently shared with counterterrorism officials and (2) either strengthen the FBI's oversight of state agencies or have the FBI centrally manage all valid match background checks. The Department of Justice agreed. Highlights: http://www.gao.gov/highlights/d05127high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−127

[Return to top]

Emergency Services Sector

26. *March 08, Asheville Citizen−Times (NC)* — **North Carolina first responders training to combat bioterrorism.** Last month, four drills were conducted in Dallas, NC, to test the readiness of the state's seven public health regional surveillance teams and other emergency workers to handle 21st Century health threats. In addition to a simulated anthrax attack, the other exercises required teams to respond to a flaming rail car leaking a hazardous chemical, the contamination of individuals from stolen radiological material, and mass trauma resulting from a hijacked private plane flown into a government building. The drills were conducted in the Regional Emergency Services Training Center at Gaston College. The teams are a regional resource in North Carolina whose activities are paid by the state using federal Centers for Disease Control funds, said Dr. Leah Devlin, North Carolina's health director. The annual budget for the state's seven teams is about $2.7 million. As part of crafting emergency response strategies, the state has also re−examined its quarantine laws, health leaders said. Last year, to enhance their disease control capabilities, the power of health officials to quarantine contagious individuals was increased from 10 to 30 days in many instances.
Source: http://www.citizen−times.com/apps/pbcs.dll/article?AID=/20050308/HEALTH/50307008/1008

27. *March 08, Potomac News (VA)* — **Terrorism response drill to be held at Quantico.** The

Quantico Marine Corps base will conduct an anti−terrorism exercise Thursday, March 10, simulating a hazardous chemical incident. The exercise will impact traffic going aboard the base. Since many vehicles will be searched, drivers can help to minimize delays by clearing out unnecessary clutter and packages, especially from the trunks of their vehicles, said 1st Lt. Paul D. Duncan from the base Public Affairs Office. Having up−to−date registration and insurance information readily available will also speed up the process. The purpose of the exercise is to test and evaluate the base's as well as local civilian emergency responders' ability to respond to crises while operating under a heightened force protection level. Exercise events will require actual response from agencies and units supporting the emergency management of the base and will include the local, state and federal community agencies.
Source: http://www.potomacnews.com/servlet/Satellite?pagename=WPN%2FMGArticle%2FWPN_BasicArticle&c=MGArticle&cid=1031781445871&p ath=

28. *March 08, The McKinney Courier−Gazette (TX)* — **Teens participate in tornado training drill.** Nearly 150 Explorer Scouts from Collin, Dallas and Grayson Counties in Texas did everything from triage to search and rescue missions during a tornado drill on Saturday, March 5. Exploring is a worksite−based program that gives youth an opportunity to explore the dynamics of various careers. The Explorers participated in five different training drills designed to teach them how to respond to a tornado disaster to help the efforts of emergency personnel, McKinney Fire Department Training Officer Ron Moore said. In the search and rescue mission, two groups searched darkened areas of the Custer Road mock home to find missing persons who were injured during the tornado's touchdown. The triage had Explorer groups assigning levels of medical attention to a group of 30 people based on their "symptoms." In the shooting gallery, the groups had to put out simulated fires and shut off a gas meter with real fire extinguishers while wearing fire helmets that obstructed their view. This meant teams had to work to put the fire out quickly and safely. For more information on Explorer Scouts, visit their website at www.learningforlife.org.
Source: http://www.courier−gazette.com/articles/2005/03/07/news/news 03.txt

[Return to top]

Information Technology and Telecommunications Sector

29. *March 08, Government Computer News* — **Office of Management and Budget to study consolidation of IT security functions.** The Office of Management and Budget (OMB) expects this month to launch a six−month study of whether some federal IT security functions could be provided centrally by agencies or commercial vendors. Karen Evans, OMB administrator for e−government and IT, said Tuesday, March 8, at the Government Computer News Cybersecurity Conference in Washington, D.C. that a task force would complete its work by September so that guidance would be available to agencies for the fiscal 2007 budget cycle. The study will apply the Business Reference Model, a function−focused method for describing business operations, to cybersecurity. Each agency has its own security needs and acceptable risk profiles, and the study might not support the use of common providers for IT security, according to Evans. But she said there is enough common need that she doubts there is a good business case for 26 executive branch departments and agencies each going its own way for security. The study is part of a broader move by OMB toward focusing on the outcome of IT security management.

Source: http://www.gcn.com/vol1_no1/daily−updates/35249−1.html

30. *March 07, Secunia* — **X11 libXpm XPM image buffer overflow vulnerability.** A vulnerability has been reported in libXpm, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to boundary errors in "GetImagePixels()" and "PutImagePixels()". This may be exploited to cause a buffer overflow when a specially crafted XPM image file is processed. Successful exploitation may potentially allow execution of arbitrary code. The vulnerability has been fixed in the CVS repository.
Source: http://secunia.com/advisories/14460/

31. *March 07, IDG News Service* — **Antivirus companies report first mobile messaging worm.** The first mobile−phone virus that spreads using the popular Multimedia Messaging Service (MMS) is circulating among Symbian Series 60 mobile phones, antivirus companies have warned. Antivirus vendors first spotted the new virus, dubbed CommWarrior.A, on Monday, March 7. When an infected attachment is opened, the virus places copies of itself on vulnerable mobile phones and uses the phone's address book to send copies of itself to the owner's contacts using MMS. Antivirus experts believe CommWarrior, which has been spreading slowly among cell phone users since January, is not a serious threat. However, the virus could herald a new age of malicious and fast−spreading cell phone threats, according to Mikko Hyppönen of F−Secure Corporation. MMS is a popular text messaging technology that allows mobile phone users to send multimedia content, such as sound files or photos, between MMS−compliant mobile phones.
Source: http://www.pcworld.com/news/article/0,aid,119918,00.asp

32. *March 07, Federal Computer Week* — **Department of Justice readies regional data exchange.** Department of Justice officials are readying an operational pilot to test the Regional Data Exchange, an FBI−led effort to share crime information between federal, state and local law enforcement organizations. The pilot will start within six months, said Vance Hitch, Justice Department chief information officer. "Getting the data in format that's shareable, that's going to take six months," Hitch told Federal Computer Week. "Then it'll be operational." Regional pilots of the National Data Exchange, an effort to create a central data repository of law enforcement incident and event reports also led by the FBI, are already underway, Hitch added. Both the national and regional data projects form part of the department's Law Enforcement Information Sharing Program (LEISP), an effort to distribute nationwide data captured by all levels of law enforcement.
Source: http://www.fcw.com/fcw/articles/2005/0307/web−doj−03−07−05.a sp

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: Microsoft will NOT be releasing any new security updates for the month of March. Therefore, the US−CERT encourages network administrators to take this extra time to ensure that all machines have the latest patches installed and current anti−virus signatures in place.
To obtain security updates from Microsoft, please visit the following link: http://www.microsoft.com/security/default.mspx

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 1025 (−−−), 1026 (−−−), 1027 (icq), 80 (www), 53 (domain), 137 (netbios−ns), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

33. *March 08, Sun−Sentinel (FL)* — **Live hand grenade found on counter at Miami restaurant.** At the corner of the counter, near where the salt and pepper and coffee pot and sugar and napkins and garnishments are kept, workers at the little cafe found a live hand grenade. Miami Police spokesperson Delrish Moss said the grenade was discovered around 6:30 a.m., Tuesday, March 8, when a customer noticed the grenade sitting on the corner of the walkup counter. He told a cafe worker, who told the owner, who told the police. When officers arrived, they discovered the grenade was live, but still had the pin firmly in place. The bomb squad was called in to dispose of the device while other officers searched the restaurant for other devices. None were found. Moss said there two customers in the cafeteria, located in a busy strip mall. Had the device exploded, he said, "it would have caused a significant amount of damage" and possibly killed or wounded the people. The cafeteria's owner and the worker "were smart because they didn't touch it and they kept everyone away," Moss said. Now, police and cafeteria workers are trying to figure out how and why the grenade got there, and how long it had been sitting on the edge of the counter.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−38handgrenade,0,2388473.story?coll=sfla−home−headlines

[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