Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 21 March 2005

Daily Highlights

- The Associated Press reports the recent theft of thousands of dollars via card skimming from people who used their debit cards at a New Hampshire ATM is one type of identity theft becoming more common as consumers increasingly rely on electronic transactions. (See item 7)

- The New York Times reports the Coast Guard is seeking to improve security on the nation's commuter ferries, which are vulnerable to attack since they often carry cars and large trucks that could hide bombs, they run on a schedule, and they are screened less intensely than airplanes. (See item 11)

- The Associated Press reports the Citizen Corps, a nationwide volunteer movement organized after 9/11 and based on the theory that local people have to deal with disasters, is thriving in cities and towns across Arizona. (See item 28)

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 19, East Valley Tribune (AZ)* — **Transformer delays should not cause problems for Phoenix.** Two transformers being built for the Westwing Substation northwest of Phoenix, AZ, failed initial tests at the manufacturer, forcing a delay of more than two months in their delivery

to Phoenix, Arizona Public Service (APS) utility officials said. At a meeting of the Arizona Corporation Commission on Friday, March 18, APS officials tried to assure commissioners and the public that Phoenix will still have adequate power supplies this summer. They said expansion of the San Tan Power Plant in Gilbert, which will add 550 megawatts to Phoenix's power supplies when it's turned on later this spring, should prevent a repeat of last summer's electricity crisis triggered by a fire at Westwing. The Westwing substation, a critical component of Phoenix's electricity system, was severely damaged in a fire July 4. APS officials had expected that replacement transformers for Westwing would begin being delivered March 30. However, unexpected problems developed at the ABB factory near Montreal, where the first two replacement transformers failed tests. The cause of the problem has been identified, and the units are being fixed, said Jan Bennett, APS vice president of customer service. Assuming there are no further delays, the first unit is expected to be operating in mid−June, he said.
Source: http://www.eastvalleytribune.com/index.php?sty=38211

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *March 19, WLNS (MI)* — **Chemical incident sends four to the hospital.** An athletic club in East Lansing, MI, was evacuated, and four people were sent to the hospital, Friday, March 18, after club employees mixed the wrong pool cleaning supplies and accidentally sparked a dangerous chemical reaction. Lansing's metro Hazmat team arrived on the scene just minutes after the incident. Three employees and another victim were taken to a local hospital due to respiratory problems. All were treated and released. Fire officials say employees were trying to add chlorine to the pool's chlorine tank, but poured muriatic acid in instead. Tracy Holtzer, one of those staff members, says the Michigan Athletic Club acted swiftly to evacuate the building.
Source: http://www.wlns.com/global/story.asp?s=3099513

3. *March 18, KFOX (TX)* — **Fire engulfs plastics factory.** Talco Plastics Inc., a plastics factory in Vinton, TX, caught fire Thursday, March 17 at 11:30 p.m. Firefighters from El Paso, and from as far away as Dona Ana County have been called out to the huge blaze. The structure was completely engulfed, and it is a hazardous situation with both cardboard and plastic burning. The Bill Childress Elementary School nearby was closed Friday due to the smoke and fumes, and several residents have been evacuated from the area.
Source: http://www.kfoxtv.com/news/4297213/detail.html?rss=elp&psp=n ews

4. *March 18, Honolulu Advertiser (HI)* — **Hazmat crews remove chemical vials from Hawaii home.** Teams of experts in protective suits converged on a quiet neighborhood on Oahu Island, HI, Thursday March 17, with fire engines, ambulances and trucks filled with sophisticated equipment capable of sniffing the air for the faintest scent of deadly chemicals. The more than 50 police officers, firefighters, Hawaii National Guard members who specialize in weapons of mass destruction, city paramedics and state Department of Health environmental emergency response personnel and hazardous materials crews were there to remove 78 glass vials thought to be from a military test kit for mustard gas. None of the vials was broken and four were empty, said Honolulu Fire Department Capt. Kenison Tejada. The vials were transported from the site inside a triple−sealed container system to Wheeler Army Airfield under police escort. A team from the Army's Aberdeen Proving Ground in Maryland was expected to examine the

vials. Authorities closed a portion of a local street and told neighbors within a quarter−mile radius to stay indoors or leave the area entirely.
Source: http://the.honoluluadvertiser.com/article/2005/Mar/18/ln/ln0 1p.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

5. *March 19, Los Angeles Times* — **Federal Deposit Insurance Corporation supports bank warning on identity theft.** U.S. regulators voted Friday, March 18, for a policy that would require banks to notify customers in certain cases of identity theft −− a proposal that consumer activists called inadequate. Federal Deposit Insurance Corp. (FDIC) officials said the proposal, which sets the rules for financial institutions to follow in designing their notification policies, still must be approved by the Federal Reserve before taking effect. It requires banks to quickly notify federal regulators if there is a security breach that might have compromised personal files. The policy would require banks infiltrated by identity thieves to notify affected customers only if the bank determined that it was "reasonably possible" that his or her private information had been misused. Privacy advocates said the proposal did not provide enough consumer protection. "It gives the banks too much discretion to decide whether a breach requires notification," said Edmund Mierzwinski, consumer program director for the advocacy organization U.S. Public Interest Research Group. A stronger standard, Mierzwinski said, was set by a 2003 California law. It requires all companies, not just banks, to notify consumers when they learn confidential information has been lost. It does not require a finding of possible harm.
Source: http://www.latimes.com/business/la−fi−idtheft19mar19,1,40494 52.story

6. *March 18, Reuters* — **U.S. government targeting global money laundering.** The U.S. government is working to ensure that other countries improve their procedures to counter money laundering, a senior Department of Treasury official focusing on financing for terrorism said on Thursday, March 17. Assistant Treasury Secretary Juan Zarate told an anti−counterfeiting conference that his department "spent a grand majority of time worrying about this issue." Banks operating in the United States are subject to a variety of directives aimed at detecting suspicious cash flows and cracking down on money laundering. However, standards in other jurisdictions can be different. This not only makes it difficult for U.S. institutions to comply with government mandates when operating abroad but opens loopholes for criminals to exploit. In a speech to the Securities Industry Association conference, Zarate also said the government was making efforts to provide more information to the private sector to help banks uncover illicit activities. "Because terrorist financing transactions may bear no inherent suspicious or identifying trademarks, it is particularly important that we share more information with the financial sector, so as to allow it to recognize accounts and transactions of interest," he said.

Source: http://www.nzherald.co.nz/index.cfm?c_id=3&ObjectID=10115987

7. *March 18, Associated Press* — **Identity theft in New Hampshire.** The recent theft of thousands of dollars via card skimming from people who used their debit cards at a Manchester, NH, ATM is one type of identity theft becoming more common as consumers increasingly rely on electronic transactions. Manchester, Nashua, Concord, Dover and Salem are New Hampshire's top identity theft hot spots, with credit−card and bank fraud taking first and third place on the list of most reported identity theft complaints. The issue is a priority for New Hampshire banks. "There's a huge amount of resources being committed to identity theft prevention," said Jerry Little, president of the New Hampshire Bankers Association. Little said ATMs are checked daily during cash drops, but that customers also must look for signs of tampering. "In ATMs you need to look at the hardware and make sure it's what you recognize. If it doesn't feel right, don't use it," he said. Wireless technology and online marketplaces are making it easier to steal financial information, Little said, and thieves are now turning to a new target −− gas stations that let customers pay at the pump. Thieves who manage to install wireless readers on a pump can easily steal credit card information to use or sell.
Source: http://nsnlb.us.publicus.com/apps/pbcs.dll/article?AID=/2005 0318/NEWS02/103180052/−1/news

8. *March 18, Techworld* — **New style of phishing attack discovered.** The rate of innovation in phishing has been underlined with the discovery of an attempt to hijack a Website frame on a legitimate banking site. The hack was revealed recently by UK security company Netcraft. The target in this instance was the online log−in of U.S.−based Charter One Bank. In contrast to established cross−scripting techniques where whole pages are hijacked by bogus sites, the new "cross−frame" scripting approach is able to inject content on to a real Web page, making it extremely difficult to detect. The technique works by adding links to the frame further down in what otherwise appears to be the legitimate charterone.com Website, without this being deemed invalid. While there is no evidence that anyone fell for the ruse, entering log−in details on this form would have given the phishers enough information to attempt fraud. An attack such as this would have to be directed at a specific bank Website and wouldn't necessarily be possible on all banking Websites.
Source: http://www.techworld.com/security/news/index.cfm?NewsID=3348

9. *March 18, Inman News* — **Consumers switch banks over identity theft fears.** Six percent of U.S. consumers surveyed by Financial Insights said they switched banks to reduce their risk of becoming a victim of identity theft, according to a report released by the research and advisory firm. The survey of 1,000 U.S. consumers over the age of 18 aimed to measure the impact of identity theft on consumer fears and on their banking and online behaviors. "Close to 60 percent of U.S. consumers sampled in January 2005 expressed concern about identity theft, and close to six percent admitted to switching banks to reduce their risk of becoming a victim of identity theft," said Sophie Louvel, research analyst at Financial Insights and author of the report. "Identity theft incidents have been taking their toll on banks and their customer relationships. Recent high−profile incidents of customer data theft at Bank of America, ChoicePoint, and LexisNexis may drive bank customers to worry further about the possibility of experiencing identity theft. However, our survey results show that not all consumers worry equally about identity theft, and the crime itself does not impact all consumers across the U.S. at the same rate," Louvel said.

Source: http://www.inman.com/inmannews.aspx?ID=45329

10. *March 17, Bend.com (OR)* — **Identity theft risks demonstrated.** Representatives from law enforcement and financial institutions appeared with legislators in Salem, OR, on Thursday, March 17, to highlight identity theft risks and the connection to Oregon's methamphetamine problem. They say using technology to improve driver licenses will help with both problems. Marion County Sheriff Raul Ramirez showed the ease of which thieves produce fraudulent Oregon driver licenses and state issued identity cards. While others spoke, Ramirez and his staff accessed Department of Motor Vehicle (DMV) computer files acquired during a methamphetamine raid and made phony identification. The Sheriff provided reporters cards with their name and vital information, but his photo. "I am distributing these ID cards to show that that it only takes a matter of minutes to steal your identity," stated Ramirez. "Without greater security mechanism these are the tactics thieves and meth addicts will continue to use to destroy their lives and others." A new bill, Oregon Senate Bill 640, is backed by law enforcement, credit unions, banks, and legislators. It will incorporate biometric imaging to fight fraud. Employees at DMV offices will also use fingerprints to sign onto their computers and complete transactions, decreasing the likelihood of information theft.
Source: http://www.bend.com/news/ar_view.php?ar_id=21791

[Return to top]

Transportation Sector

11. *March 19, New York Times* — **Keeping the nation's ferries safe.** To improve security on the nation's commuter ferries, the Coast Guard has been trying to answer some critical questions: How much explosive force would be needed to sink a big ferry? Which screening methods are most effective? How many vehicles and passengers should be screened to create a deterrent? While there have been no reported threats to a ferry in the United States, officials say, the Federal Bureau of Investigation reported at least seven incidents last year involving surveillance of ships in Washington State, said Representative Jay Inslee (D−WA). Coast Guard officials say nearly 400 passengers would be likely to die if a large ferry were attacked, more than twice the number of deaths expected from an airplane crash. Officials worry that ferries may be attacked because they often carry cars and large trucks that could hide bombs, they run on a schedule and they are screened less intensely than airplanes. There have been attacks on ferries elsewhere: a 1,050−passenger ferry sank in the Philippines in February 2004 after a bomb, consisting of eight pounds of TNT packed into a television, killed more than 115 people. More than 700 ferries operate nationally, carrying 175 million passengers a year.
Source: http://www.nytimes.com/2005/03/20/national/nationalspecial3/ 20ferry.html

12. *March 18, Thunder Bay Chronicle−Journal (Canada)* — **Ports get money for upgrading.** Three Thunder Bay ports are getting Canadian federal government funding to help them catch up with new international security codes. The Thunder Bay Port Authority, Thunder Bay Terminal Ltd., and James Richardson International will get funding to improve their security equipment and training, as part of the government's Marine Security Contribution Program. Port authority CEO Tim Heney said the improvements are needed for ports to meet the International Ship and Port Security (ISPS) Code, which was introduced in July. "It was a U.S.−driven initiative, basically to ensure that ships entering U.S. waters had been visiting

secure facilities," he said. "If a shipping facility isn't ISPS certified, they face a coast guard search when they enter U.S. waters, and possible delays." As such, shipping companies are increasingly looking for ports to meet the new standards, Heney said. The government made the funding announcement Wednesday, March 16. The port authority will receive $78,000 for new fencing, security staff training and other access measures at Keefer Terminal. The Marine Security Contribution Program, announced in May 2004, will provide $115 million to ports over three years to modernize and strengthen their security systems and programs. It's part of the National Security Policy.
Source: http://www.chroniclejournal.com/story.shtml?id=26301

13. *March 17, Department of Transportation* — **Continental confirmed for U.S.−China air services.** The U.S. Department of Transportation (DOT), making final part of a February 22 proposed decision, on Thursday, March 17, confirmed Continental Airlines as a new entrant in the U.S.−China air market and awarded the carrier seven weekly passenger flights for rights that will become available on March 25 for a new daily trip between Newark, NJ, and Beijing. In its proposed decision, the Department also tentatively awarded U.S.−China rights to several other airlines that become available March 25, 2006, including a proposal to name American Airlines as a new entrant in the China market next year with approval to operate seven weekly passenger flights. The order issued on Thursday, as well as the show−cause order, carrier applications and other documents in this case may be obtained via the Internet at http://dms.dot.gov, docket number OST−2004−19077.
Source: http://www.dot.gov/affairs/dot4905.htm

14. *March 17, Associated Press* — **One billion air travelers in 2015.** More than one billion people a year will be boarding planes in the United States within a decade, nearly double the number now using an aviation system showing signs of being overburdened. The Federal Aviation Administration (FAA), which released the forecast Thursday, March 17, faces spending cuts for runways, air traffic control equipment and buildings. But the agency's administrator, Marion Blakey, said she was confident there would be enough money to accommodate the dramatic growth in air traffic. "We are redesigning airspace, deploying new software that will help increase capacity, and putting new procedures in place," Blakey said. Lawmakers and aviation advocates are more concerned Building is not keeping up with the increase in passengers, said David Stempler, president of the Air Travelers Association. "That just spells congestion and delays for passengers." Already, flights have been limited at Chicago's O'Hare International Airport because too many planes were trying to take off and land, causing delays throughout the country. Ruth Marlin, executive vice president of the air traffic controllers union, said many passengers will do a lot of waiting in 2015 if things do not change.
Source: http://www.cnn.com/2005/TRAVEL/03/17/billion.passengers.ap/i ndex.html

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

15. *March 18, Sun−Sentinel (FL)* — **Dogs could be used to detect citrus canker.** Government agricultural researchers are scrambling to find new ways of grappling with citrus canker, a plant disease that is threatening the Florida's citrus industry. The only way canker is found is by inspectors going step−by−step through miles of groves, using their eyes to spot canker that may only be on a few leaves. That can take days and weeks. Neither satellite nor aerial surveillance systems have been developed to find canker. Dogs have already been successfully trained to sniff out canker in laboratory conditions. They are part of the U.S. Department of Agriculture's National Detector Dog Training Center. Within two years, the dogs might be ready to head into groves. Researchers are also looking into hyperspectral imagery: finding canker by changes in lightwaves reflected off canker on a plant's surface.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pcanker news18mar18,0,2090626.story?coll=sfla−news−palm

16. *March 18, Animal and Plant Health Inspection Service* — **Regulations finalized on agricultural select agents and toxins.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) Friday, March 18, announced the publication of a final rule that, among other things, removes plum pox and Asian soybean rust from the list of select agents and toxins. The list of select agents and toxins was developed by USDA in conjunction with regulations governing the possession, use, and transfer of these agents and toxins, which have the potential to pose a severe threat to public health and safety, to animal or plant health, or to animal or plant products. This final rule revises the format and content of USDA's regulations, which prescribe registration, biocontainment/biosafety, incident response, and security measures for facilities handling these agents and toxins to protect against the use of such agents or toxins in domestic or international terrorism. Asian soybean rust has been removed from the list of select agents and toxins to facilitate timely research on effective means to manage the disease. Plum pox has been removed from the list of select agents and toxins because it does not spread easily by natural means and it would be difficult to spread intentionally.
Source: http://www.aphis.usda.gov/lpa/news/2005/03/slctagnt_ppq.html

17. *March 17, Economic Times* — **Disease threat to wheat.** Nobel Laureate Norman Borlaug has warned against the threat to world's wheat economy from diseases that could affect countries like India and Pakistan. "Global collaborative research programs are necessary for integrated efforts for disease screening. There are genes available that can be transferred to wheat to provide it protection against diseases like stem rust that can wipe out millions of acres of crop," Borlaug said. He was delivering the annual Coromandel Lecture at the Indian Agricultural Research Institute on Wednesday, March 16. "Some of you young scientists can take the gene out of rice and put it into wheat to provide it protection against diseases like stem rust for a long time," he said. Stem rust, one of the most destructive diseases for cereals, was responsible for millions of dollars in losses before the introduction of resistant varieties. Besides rice, other genes can also be used for providing better protection to wheat against diseases, Borlaug said.
Source: http://economictimes.indiatimes.com/articleshow/1055034.cms

[Return to top]

Food Sector

18. *March 18, Reuters* — **Japan readies mad cow policy.** Japan appears on track to approve a more lenient mad cow policy, but that is not likely to lead to an immediate lifting of a ban on U.S. beef in place for over a year, a government official said on Friday, March 18. Japan's Food Safety Commission said that a subcommittee on mad cow disease would meet on March 28 to approve the government's proposed policy of excluding cattle aged less than 21 months from blanket testing. Japan is under mounting pressure from the U.S. to end the 15−month−old ban on American beef imports. Finalizing a domestic policy based on scientific evidence is a crucial step towards ending the ban. A Commission official said, however, there were still hurdles that needed to be cleared before Japan could resume U.S. beef imports, saying that after the domestic policy is approved, the government would then look at U.S. policy.
Source: http://www.alertnet.org/thenews/newsdesk/T12443.htm

19. *March 17, Food Safety and Inspection Service* — **Chicken strips recalled.** Perdue Farms, Inc., a Concord, NC, establishment, is voluntarily recalling approximately 230,700 pounds of fully cooked chicken breast strips due to possible under processing, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, March 17. The chicken strips were produced in February and March and were shipped to centers in Alabama, Florida, Massachusetts, North Carolina, Pennsylvania, and Virginia for further distribution. The problem was discovered by the company. FSIS has received no reports of illnesses from consumption of the product.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_011_2005_Relea se/index.asp

20. *March 16, Johns Hopkins University* — **Drug resistant bacteria on poultry products differ by brand.** The presence of drug resistant, pathogenic bacteria on uncooked poultry products varies by commercial brand and is likely related to antibiotic use in production, according to researchers at the Johns Hopkins Bloomberg School of Public Health. Their study is the first to directly compare bacterial contamination of poultry products sold in U.S. supermarkets from food producers who use antibiotics and from those who claim they do not. The study focused on antibiotic resistance, specifically fluoroquinolone−resistance in Campylobacter, a pathogen responsible for 2.4 million cases of food−borne illness per year in the U.S. Tyson Food and Perdue Farms, separately announced in 2002 that they would immediately stop using fluoroquinolones to treat poultry flocks. In 2003, researchers began a survey of Campylobacter isolates on uncooked chicken products from Tyson and Perdue and from two other producers, Eberly and Bell & Evans, who claim their production methods are completely antibiotic−free. They compared retail products purchased at grocery stores in Baltimore, MD. A high percentage of the products from the two conventional brands were contaminated with fluoroquinolone−resistant Campylobacter (96 percent from Tyson and 43 percent from Perdue) while lower proportions of "antibiotic−free" products were contaminated with fluoroquinolone−resistant Campylobacter (five percent from Eberly and 13 percent from Bell & Evans).
Source: http://www.jhsph.edu/PublicHealthNews/Press_Releases/2005/Pr ice_campylobacter_chicken.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

21. *March 18, Reuters* — **Angola says at least 77 die in acute fever outbreak.** At least 77 people, most of them children, have died in northern Angola after an outbreak of a disease the World Health Organization (WHO) suspects to be acute hemorrhagic fever, officials said on Friday, March 18. They have ruled out the Ebola virus −− a type of hemorrhagic fever −− but are urging people to avoid travel to Uige, Angola. "Most of the city has been affected, but some areas are worse hit than others," Health Ministry spokesperson Carlos Alberto said. Jose Caetano, a WHO spokesperson in Angola, said most of the victims were children with symptoms including fever, vomiting and diarrhea. He said at least 77 of the total of 83 people believed infected had died. Caetano said Angola's limited laboratory facilities had hampered identification of the disease and that samples had been sent to the U.S. Centers for Disease Control and the Pasteur Institute.
Source: http://www.alertnet.org/thenews/newsdesk/L18716816.htm

22. *March 18, Voice of America* — **Vietnamese boy contracts bird flu.** A five−year−old boy from central Vietnam has become the latest person to contract the bird flu virus that has killed at least 46 people in the region. The boy was admitted to a hospital in central Vietnam and tested positive for the H5N1 strain of the virus. His 13−year−old sister died the week of March 7 after suffering the same symptoms, but was not tested.
Source: http://www.voanews.com/english/2005−03−18−voa19.cfm

23. *March 17, Reuters* — **Tuberculosis rate falls to record low in U.S.** The tuberculosis infection rate in the U.S. fell to a record low last year, but the relatively small decline raised fears that the nation was falling behind in its battle to eliminate the disease. A total of 14,511 active TB infections, or 4.9 cases per 100,000 people, were reported to U.S. authorities in 2004, according to the Centers for Disease Control and Prevention. That compared with 14,858 cases and a rate of 5.1 cases per 100,000 in 2003. The rate last year was the lowest since national reporting of the disease began 52 years ago, but the rates of decline in the past two years −− 3.3. percent in 2004 and 2.3 percent in 2003 −− were the smallest since 1993, the CDC said. TB rates fell an average 6.6 percent between 1993 and 2002.
Source: http://www.alertnet.org/thenews/newsdesk/N17619426.htm

24. *March 17, KABC−TV (CA)* — **West Nile virus detected in California.** Heavy rains and warm temperatures have led to the early arrival of mosquitoes and West Nile virus (WNV) in California, State Public Health Officer Richard Jackson announced Thursday, March 17. To date, WNV has been detected in 19 of California's 58 counties. No human cases have yet been reported in 2005. "This is a critical time for mosquito prevention," Jackson said. Thirty−two dead birds from the following counties have tested positive for WNV: Alameda, Contra Costa, El Dorado, Fresno, Humboldt, Kern, Kings, Los Angeles, Orange, Placer, Sacramento, Santa Clara, Santa Cruz, Solano, Sonoma, Stanislaus, Tulare, and Yolo counties. WNV has also been detected in a sentinel chicken in San Bernardino County and mosquitoes in Orange County. Source: http://abclocal.go.com/kabc/news/031705_nw_wnile_virus.html

[Return to top]

Government Sector

25. *March 17, USA TODAY* — **Federal bureaus opt against stun gun use.** The Department of Homeland Security's two largest law enforcement divisions have rejected the use of stun guns for about 20,000 agents and officers, largely because of questions about the safety of the devices that emit electrical charges to temporarily incapacitate suspects. The bans were adopted by the bureaus of Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) in internal directives that were issued during the past two years. ICE rejected the devices in December 2003, spokesperson Russ Knocke said. That was about a month after an officer with the Federal Protective Service, a part of ICE, allegedly was injured during a stun gun training session. CBP issued its own ban several months later, spokesperson Barry Morrissey said. The bureaus' acknowledgements of the bans come at a time when stun guns, which are used by more than 7,000 law enforcement agencies across the U.S., are under increasing scrutiny. The International Association of Chiefs of Police and other law enforcement groups have called for more extensive research into whether stun guns are safe. Source: http://www.usatoday.com/news/nation/2005−03−17−tasers−usat_x .htm

[Return to top]

Emergency Services Sector

26. *March 18, Newport News−Times (OR)* — **Oregon plans another mock emergency drill.** Lincoln County School District (LCSD) in Oregon will conduct a mock emergency drill involving local police and other emergency management agencies at a school in Newport, OR, sometime during Spring Break. This drill −− the second in a planned series of preparedness exercises for county emergency responders −− will feature an armed intruder scenario, according to Sue Graves, LCSD safety coordinator. Graves is withholding the exact time, date, and location for the staged event to "preserve an element of surprise" for participants, and to "add to the realism" of the scenario. Community members can hear more specific information broadcast by local radio stations at the start of the event. This drill will feature the use of "simunitions"−− non−lethal cartridges, similar to paint balls, used in firearms training. Firing the simunitions produces a sound similar to actual gunfire. Funds for the training scenario derive from a federal Emergency Responses Crisis Management grant through the Department of Education and from contributions by the participating agencies. Source: http://www.newportnewstimes.com/articles/2005/03/18/news/new s16.txt

27. *March 18, Associated Press* — **North Carolina sites to be part of summer terrorism drill.** The largest terrorism drill in North Carolina history is being planned for August and will include a mock attack on the Sunny Point Military Ocean Terminal in Brunswick County. Officials said the drill will stretch from Fort Bragg to Morehead City in the state's central coast area to Brunswick County on the southeastern coast. Emergency and law−enforcement units

from Virginia to South Carolina have been invited to participate, as have those from the seven counties that surround Fort Bragg. The exercise is thought to be the first to test the new National Response Plan that takes effect next month and requires coordination among local, state and federal officials in terrorism and emergency response. The exercise is to begin with a weapons of mass destruction drill at Fort Bragg with some of the perpetrators escaping. Other events will occur over the next three days at or near other military bases in eastern North Carolina, at the State Port in Morehead City and in the Pamlico Sound. There will be a May 17 workshop in Morehead City to help prepare those who will participate and a July exercise to test communications before the August events, said Andy Albright, an exercise facilitator.
Source: http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1031781660453

28. *March 17, Associated Press* — **Thousands of Arizonans assist public−safety crews in emergencies.** Citizen Corps, a nationwide volunteer movement, is quietly blossoming in cities and towns across Arizona. Citizen Corps is a network of groups organized after 9/11 based on a simple theory: Local folks have to deal with disasters, so specialized volunteer units should be run independently in each community with the assistance of federal money, coordination and information. There are 3,000 Arizonans on about 30 Community Emergency Response Teams (CERT) statewide. The Citizen Corps has an elaborate layering of oversight councils that funnel money, coordinate operations and conduct training. A state council was founded last year, and 94 percent of Arizona's population now lives within the protective Citizen Corps umbrella. Besides CERT, the corps includes four other specialized partner programs. The Medical Reserve Corps provide urgent care during plagues, disasters or attacks with weapons of mass destruction. The Volunteers in Police Service include posse members, police reserves and other private citizens who give their time at police or sheriff's departments. The Fire Corps is for private citizens who already volunteer at fire departments. The Neighborhood Watch includes an estimated 3,800 state residents enrolled in this long−standing Justice Department program who are also members of Citizen Corps.
Source: http://kvoa.com/Global/story.asp?S=3092427

[Return to top]

Information Technology and Telecommunications Sector

29. *March 21, ZDNet (United Kingdom)* — **Physical security becoming an IT problem.** The proliferation of technologies such as identity management mean more IT managers are having to take responsibility for physical security, according to a panel of leading IT security managers. Speaking at the Business Continuity Expo in London's Docklands, IT security experts from the Royal Mail Group, Proctor & Gamble and Barclaycard acknowledged that their companies are increasingly merging systems used to authenticate employees' entry to physical facilities with those used to control access to computing resources. David McCaskill, manager for global security solutions at Proctor & Gamble, explained that the pharmaceutical giant had also integrated its physical and IT authentication systems. "Before, if you forgot your passcard to access the building that wasn't a major problem, but now it is." Companies have generally treated physical security as the responsibility of the facilities department and computer security as that of IT. But employee information has increasingly become integrated, allowing businesses to link the two systems, said Steve Hunt, an analyst with Forrester

Research.
Source: http://news.zdnet.co.uk/internet/security/0,39020375,3919183 9,00.htm

30. *March 18, BBC News (United Kingdom)* — **European governments to form Internet 'terror watch' team.** Five European governments are setting up a hi−tech team to monitor how terrorists and criminals use the Internet. The group will make recommendations on shutting down Websites that break terrorism laws. The plans for the initiative came out of a meeting of the G5 interior ministers in Spain that discussed ways to tackle these threats. The five countries also agreed to make it easier to swap data about terror suspects and thefts of explosives. The interior ministers of Spain, Britain, France, Germany and Italy −− the G5 −− met in Granada, Spain last week for an anti−terrorism summit. To combat terrorism the ministers agreed to make it easier for police forces in their respective states to share data about suspects connected to international terror groups. Part of this anti−terror work will involve the creation of the technical team that will keep an eye on how organized crime groups and terrorists make of the web.
Source: http://news.bbc.co.uk/1/hi/technology/4360727.stm

31. *March 17, Computerworld* — **CTIA: Experts call for homeland security, wireless industry cooperation.** To bolster the value of wireless voice and data communications for U.S. homeland security purposes, industry and government officials need to work closer together, security experts at Cellular Telecommunications & Internet Association (CTIA) Wireless 2005 said last week. The consensus among experts from the Federal Communications Commission and Department of Homeland Security who took part in a panel discussion was that wireless technologies have improved since the September 11, 2001, terrorist attacks. But they said much remains to be done to set up effective warning systems in the event of a terrorist or natural disaster and to improve interoperability of wireless devices for emergency responders. The toughest issue for police, firefighters and other emergency responders may be the widespread lack of interoperability between public safety networks and devices, experts said. Several panelists called for development of emergency warning systems to notify a large group of people of an emergency, similar to one county officials use in Arlington, VA. That system is used by police and fire officials to call residents over wired or wireless phones, or the Internet, to warn them of traffic disasters or crimes. CTIA: http://www.ctia.org
Source: http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,100458,00.html

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: Multiple vulnerabilities are identified in Symantec products that may be exploited by attackers to conduct DNS cache poisoning and redirection attacks. An updated hot fix was released on March 14, 2005 that further hardens the DNS for protection against an additional potential vector identified by Symantec engineers. Symantec recommends customers immediately apply the latest hot fix for their affected product versions to protect against this type of threat. Product specific hot fixes are available via the Symantec Enterprise Support site http://www.symantec.com/techsupp.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 7674 (−−−), 6346 (gnutella−svc), 53 (domain), 1026 (−−−), 80 (www), 1025 (−−−) 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

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

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.