Department of Homeland Security Daily Open Source Infrastructure Report for 11 May 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- A botched delivery by a chemical company mixed Muriatic acid with sodium hypochlorite creating toxic chlorine gas that resulted in hospitalizing 13 high school swimmers and three employees at the Reno Northeast Community Center. (See item 7)

- SecureWorks says a survey of attacks against its financial customers in the past year found there were 67 percent more Internet attacks attempted against credit union clients than banking clients. (See item 10)

- The Associated Press reports authorities offered a $25,000 reward on Tuesday, May 9, for information about the theft of more than 500 pounds of explosives from a storage bunker near a California gold mine. (See item 36)

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://www.esisac.com]

1. *May 10, Guardian (UK)* — **Gas gushing from overfilled tank caused explosion at UK's Buncefield oil depot.** More than 300 tons of petrol gushed unnoticed for 40 minutes from a storage tank at the Buncefield, UK, oil depot before the spill triggered Europe's biggest fire since the second world war, a report into last December's blaze has concluded. A faulty gauge

permitted the unleaded petrol to be pumped into the already full tank at the site. Emergency safety systems failed to prevent the tank over spilling and the resulting vapor cloud ignited and injured 43 people. The investigation team's Taf Powell said "automatic shutdown did not take place" as it should have done. A crucial switch from the roof of the tank intended to trigger the alarms was recently found by investigators, but has not yet been sent for forensic analysis. Pictures show the spill created a "white mist" of vapor, which drifted across the site. Investigators are unsure what caused the vapor cloud to ignite. The investigating team does not believe that the explosion was triggered by a tanker driver or by a mobile phone.
Source: http://www.guardian.co.uk/buncefieldfueldepotblaze/story/0,, 1771358,00.html

2. *May 10, Associated Press* — **Corrosion leads to shut down of pipelines.** Two oil pipelines on Alaska‘s North Slope are being shut down because of internal corrosion. One of the lines is a 24−inch diameter, five−mile pipe at the Lisburne oil field. The other is a 14−inch diameter, nearly four−mile line at Milne Point, according to BP. Together, the pipelines account for 22,000 barrels of the approximately 825,000 barrels that flows each day down the trans−Alaska pipeline to Valdez, and then to West Coast refineries. Both pipes had a history of corrosion and were being treated with corrosion inhibitor, said Maureen Johnson of BP. It became increasingly apparent corrosion inhibitor was not doing the trick. "We started to conclude last year that corrosion inhibitor alone might not stop this problem," she said. BP is leaning toward replacing both pipelines, Johnson said. The earliest that work could be done would be in 2007.
Additional information reported from:
http://www.thenewstribune.com/news/nationworld/story/5728231 p−5127739c.html
Source: http://www.localnewswatch.com/skyvalley/stories/index.php?action=fullnews&id=185548

3. *May 09, Times−Dispatch (VA)* — **New transmission line from West Virginia to New Jersey dedicated by AEP.** American Electric Power crews yesterday finished connecting a 765,000−volt power line from Wyoming, WV, to Jacksons Ferry, VA, that federal officials consider critical to preventing East Coast blackouts. The 90−mile line was 16 years in the making. Company President Michael G. Harris said AEP is now turning its attention to building a $3 billion power line that would run more than 500 miles from West Virginia to New Jersey as the utility tries to keep pace with the nation's surging energy demand. The Wyoming−Jacksons Ferry line will be energized June 30. The new line will reinforce what AEP refers to as an "overloaded system" that delivers power to about one million customers in West Virginia and Virginia.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1137835948218&path=!business&s=1045855934855

4. *May 09, Associated Press* — **U.S. troops crack down on fuel smuggling.** U.S. troops in the oil refining center of Beiji, Iraq, are cracking down on a vast fuel theft and smuggling operation that robs from Iraq's economy and helps finance the insurgency. The troops are chasing the smugglers and closely monitoring refinery workers. Before the crackdown began in recent weeks, fuel smuggling from Beiji was so extensive and flagrant that dozens of truck drivers would congregate just outside the refinery's gates. In plain sight, they would swap counterfeit export documents or transfer fuel to unauthorized trucks. In a report last month, the inspector general of the oil ministry, Ali al−Alaak, estimated about $4 billion worth of petroleum

products were smuggled out of Iraq last year, including gasoline and crude oil siphoned from pipelines. The Finance Ministry estimates that up to half of the profits from oil smuggling end up in the hands of insurgents. Smuggling is lucrative in Iraq because fuel prices are heavily subsidized by the government. A gallon of regular gasoline costs less than 70 cents. Smugglers make a substantial profit by shipping fuel to Syria or Turkey, where prices are much higher.
Source: http://www.chron.com/disp/story.mpl/ap/fn/3851132.html

5. *May 09, Associated Press* — **North American mining firms uneasy over Bolivia.** Bolivia's plan to nationalize its natural gas industry and exert greater state control over all of its natural resources has North American mining companies fretting over their future prospects extracting the nation's rich resources of gold, silver, and tin. Bolivia's government said last week that it would extend control over mining, forestry, and other sectors of the economy, after President Evo Morales nationalized the country's natural gas industry on May 1. Morales said his countrymen are weary of foreign exploitation of their natural resources. Vice President Alvaro Garcia Linera has emphasized that mining would not be nationalized. But he said foreign companies would face higher taxes and royalty payments and that the government would intensify enforcement of existing laws to break up big underdeveloped land holdings. This uncertainty prompted Peter Munk, chairman of Toronto−based Barrick Gold Corp., to say he now sees Pakistan as a better place to invest in, despite the presence of Islamic militants in the South Asian nation.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/09/AR2006050900872_pf.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *May 10, Tennessean* — **Tanker flips, spills fuel in Tennessee; residents evacuated.** A portion of Leipers Creek Road was closed for more than four hours Tuesday, May 9, and at least three houses were evacuated after a tanker truck transporting diesel and gasoline overturned and hit a telephone pole in Leipers Fork, TN. A portion of the truck's contents −− approximately 2,700 gallons of diesel and 1,500 gallons of gasoline −− spilled onto the ground.
Source: http://tennessean.com/apps/pbcs.dll/article?AID=/20060510/COUNTY0902/605100386/1177/COUNTY0902

7. *May 09, Reno Gazette−Journal (NV)* — **Reno lifeguard saves 13 from gas contamination.** A botched delivery by a chemical company with a history of mishaps hospitalized 13 North Valley High School swimmers and three Reno, NV, employees Monday afternoon, May 8, at the Northeast Community Center, officials said. Muriatic acid left in a tube from an earlier delivery mixed with sodium hypochlorite, which sanitizes swimming pools, and created toxic chlorine gas during a delivery by Sierra Chemical Co., Reno fire spokesperson Steve Frady said. Steve Schwade, head lifeguard at the city pool, said he noticed the strong chlorine smell in the pool area and questioned the delivery driver, who was refilling tanks outside the building. After realizing the chemicals had been mixed, Schwade then led the evacuation of the 13 high school swimmers. About 50 people were evacuated from other areas of the northeast center.
Source: http://news.rgj.com/apps/pbcs.dll/article?AID=/20060509/NEWS10/605090362/1016/NEWS

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

8. *May 10, ZDNet* — **Identity theft battle high on Australian federal agenda.** The Australian federal government Tuesday, May 9, announced it would establish identity security "strike teams" and deploy a document verification service (DVS) in an effort to combat identity fraud. Attorney−General Philip Ruddock said the measures were announced in response to indications identity theft was being targeted by "organized crime and potential terrorists." The DVS would allow agencies to check online the validity of key identity documents being presented by individuals applying for high−value benefits and services. They would be able to check passports, the health and welfare services access card, citizenship certificates, birth certificates, and drivers licenses issued in Australia. In addition, Ruddock said, three identity fraud "strike teams" led by the Australian Federal Police would be established. Ruddock also revealed that a custom−built Case Management and Information System would be deployed in overseas jurisdictions as part of efforts to enhance regional counter−terrorism capabilities.
Source: http://www.zdnet.com.au/news/security/soa/Identity_theft_battle_high_on_federal_agenda/0,2000061744,39255970,00.htm?feed =rss

9. *May 09, Infoworld* — **Webroot uncovers thousands of stolen identities.** Spyware researchers at Webroot Software have uncovered a stash of tens of thousands of stolen identities from 125 countries that they believe were collected by a new variant of a Trojan horse program the company is calling Trojan−Phisher−Rebery. The FBI is investigating the stolen information, which was discovered on Tuesday, April 25, on a password−protected FTP server in the U.S. and is believed to be connected to a Trojan horse that is installed from the Website teens7(dot)com. The information, organized by country, includes names, phone numbers, social security numbers, and user log−ins and passwords for tens of thousands of Websites. The Rebery malicious software is a "banking" Trojan, which are programmed to spring to life when computer owners visit one of a number of online banking or e−commerce sites, said Gerhard Eschelbeck of Webroot. Webroot notified the FBI after it discovered the stolen information, which had been groomed and organized in folders by country where it was "ready to be sold," Eschelbeck said. Rebery is still "running wild" on the Internet, Webroot said. The company believes there are more than 12,000 systems infected with the Trojan, 1,200 of them in the U.S.
Source: http://news.yahoo.com/s/infoworld/20060509/tc_infoworld/7813 9_1

10. *May 09, Finextra* — **Hackers target credit unions.** Credit unions are now experiencing more online attacks than larger financial services firms, according to research by SecureWorks. SecureWorks says a survey of attacks against its financial customers in the past year found there were 67 percent more Internet attacks attempted against credit union clients than banking clients. On average, SecureWorks says it blocks 767 attacks per day per credit union client. Jon

Ramsey, CTO of SecureWorks, says credit unions are experiencing more Internet attacks because hackers assume that their networks are less protected than larger banks' networks. The SecureWorks report found that, on average, the firm is blocking 968 attacks per day for each bank client with $500 million to $10 billion in assets, 285 attacks per day for each client with $100 million to $500 million in assets, and 85 attacks per day for each banking client with $100 million and less in assets. An earlier study by the Anti−Phishing Working Group (APWG) also found that online scammers and phishers were increasingly targeting smaller financial institutions.
Source: http://finextra.com/fullstory.asp?id=15289

[Return to top]

Transportation and Border Security Sector

11. *May 10, Miami Herald* — **American Airlines flight forced to return to Miami after problems.** An American Airlines flight headed to New York City was forced to return to Miami International Airport on Wednesday morning, May 10, because of "possible electrical problems," said Greg Chin, spokesperson for Miami International Airport. About 127 passengers were on board the flight headed for LaGuardia International Airport. The plane landed safely and no injuries were reported, Chin said.
Source: http://www.miami.com/mld/miamiherald/14545307.htm

12. *May 10, Pittsburgh Post−Gazette* — **Pennsylvania infrastructure crumbling.** When it comes to roads, bridges, transit, and other facilities important to everyday life, Pennsylvania is nearly failing, says a nationwide engineers' group. The American Society of Civil Engineers (ASCE), in its first−ever "state report card," issued an overall "D" grade for Pennsylvania on Tuesday, May 9. It issued just one "B" −− for freight rail investments −− and no "As" in a total of nine categories. The report evaluated dams, drinking water, navigable waterways used for commercial activity, wastewater, and aviation as well as roads, bridges, rail, and transit. Although Pennsylvania fared no worse than the national average, that's "still not very good," said John Menniti, head of ASCE's Legislative Affairs Committee. He pointed to local infrastructure problems such as boil−water advisories, raw sewage backing into basements, and the collapse of a bridge beam on Interstate 70 in Washington County last December. Other organizations such as the Washington, DC−based Road Information Program and the Keystone Transportation Coalition have produced similar reports in the past.
Source: http://www.post−gazette.com/pg/06130/688850−147.stm

13. *May 10, New York Times* — **Arizona county uses new law to look for illegal immigrants.** On Wednesday, May 10, a civilian force of 300 volunteers, many of them retired deputies, fanned out over desert backcountry, watching for smugglers and the people they guide. At the same time, a small team of deputies roamed the human−trafficking routes to enforce a nine−month−old state law that makes smuggling people a felony and effectively authorizes local police forces to enforce immigration laws. Not only do deputies charge the smugglers, but many of their customers have also been jailed. Smuggling illegal immigrants is a federal crime. Arizona adopted its law last year out of frustration that Washington had not done enough to control illegal crossings. In recent years, central Arizona has emerged as a prime crossing point. Sheriff Joe Arpaio of Maricopa County sought and received an interpretation of the statute by

County Attorney Andrew P. Thomas, who said the illegal immigrants could face charges that they conspired with smugglers. In the eight weeks since the team of deputies formed, 146 people have been arrested, Sheriff Arpaio said, with 12 suspected of being smugglers. Four have pleaded guilty and under a deal with prosecutors received three years' probation. They will be referred to federal authorities for deportation.
Source: http://www.nytimes.com/2006/05/10/us/10smuggle.html?_r=1&ore f=slogin

14. *May 10, United Press International* — **Australia increasing cargo security.** Australia is boosting anti−terror aviation security measures for air cargo. The measures were detailed in the government's 2006−2007 budget, which was released Tuesday, May 9. The budget allocates for the first time $11 billion (U.S. $8.5 billion) to include major domestic airports in screening of cargo for explosives, something already done at international airports. Customs and other entities were also being allocated funds for other various security−enhancing airport measures. Included are base alarms, TV monitoring systems, more police, mobile x−ray screening vans, and dog detector teams.
Source: http://www.upi.com/SecurityTerrorism/view.php?StoryID=200605 09−015132−8600r

15. *May 10, Department of Transportation* — **New 'Rollover Rig' training simulator to enhance passenger rail safety.** A new rescue training simulator that can rotate a full−sized commuter rail car up to 180 degrees to teach emergency responders how to save passengers from rollover train accidents was unveiled on Wednesday, May 10, by the Federal Railroad Administration (FRA) at a demonstration in the Washington, DC area. The device, known as the Passenger Rail Vehicle Emergency Evacuation Simulator, or "Rollover Rig," can be used to simulate various passenger train derailment scenarios so first responders are able to safely practice effective passenger rail rescue techniques. The FRA developed the Emergency Evacuation Simulator at a cost of $450,000. The commuter rail car was donated by New Jersey Transit. The Washington Metropolitan Area Transit Authority has agreed to house, operate, and maintain the simulator at its emergency response training facility located in Landover, MD. The Rollover Rig is one of many projects and initiatives in the FRA's comprehensive program to improve passenger rail safety, FRA Deputy Administrator Cliff Eby stated. Other activities include: strengthening the structural composition of rail cars; designing interior features that reduce passenger injuries; and reducing hazards along rail corridors where passenger trains operate.
Source: http://www.dot.gov/affairs/fra0306.htm

16. *May 09, Associated Press* — **Wind blows freight cars off tracks, key rail link closed.** Authorities now say 16 freight cars were blown off the tracks by wind in southern Kansas early Tuesday, May 9, shutting down a key rail link. BNSF Railway says 16 of the 30 cars on the train derailed just east of Belle Plaine, KS, about 30 miles south of Wichita. The train was traveling from the Chicago area to southern California and was hauling empty containers. High winds were suspected as the cause. The National Weather Service said winds in the area reached as high as 60 miles per hour around the time of the accident.
Source: http://www.49abcnews.com/news/2006/may/09/wind_blows_freight _cars_tracks_key_rail_link_close/

17. *May 05, Transportation Security Administration* — **TSA Names Dallas/Love Field, Memphis International Airport and Milwaukee's General Mitchell International Airport as Gateway Airports.** The Transportation Security Administration (TSA) on Friday, May 5,

named Dallas/Love Field Airport, Memphis International Airport, and Milwaukee's General Mitchell International Airport as the newest "Gateway" airports, allowing certain pre−cleared general aviation operations, including corporate aircraft, charter flights, and on−demand operations, to fly directly into Ronald Reagan Washington National Airport (DCA). Currently, TSA allows those general aviation flights in accordance with the DCA Access Standard Security Program into DCA. The access program was developed in July 2005 in coordination with other Department of Homeland Security components, the Department of Transportation, the Department of Defense, and other federal agencies. The program, which allows up to 48 general aviation flights into DCA per day, addresses the special aviation security needs in the National Capitol Region by requiring all aircraft to meet security measures set forth by TSA.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01d9fcc

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *May 10, Agricultural Research Service* — **Seed−rotting microbes sought to battle weeds.** New, integrated approaches to battling annual broadleaf weeds may enlist beneficial soil microbes that hit the plants where it hurts −− their seed banks. These banks are reserves of thousands, even millions, of weed seeds that lie dormant beneath the soil awaiting favorable conditions to germinate, according to Joanne Chee−Sanford, a microbiologist with the Agricultural Research Service (ARS). Since 2002, Chee−Sanford has been piecing together the conditions under which certain fungi and bacteria will cause decay in dormant weed seeds, killing them or diminishing their fitness. Classical biological control would call for unleashing the microbes onto a targeted weed to fight it, but Chee−Sanford has a slightly different tactic in mind. Rather than apply microbes as biological control agents, she envisions bolstering the activity of microbes that already occur in the soils naturally, possibly using an amendment of some kind.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

19. *May 09, Associated Press* — **Plants to monitor radioactive water.** The nuclear industry took

steps Tuesday, May 9, to head off a growing public relations problem, promising to closely monitor leaks of slightly radioactive water into groundwater at power plants. The issue has become particularly troublesome in Illinois where three power plants reported leaks of tritium into groundwater, including one case where six million gallons was released into soil outside the plant boundary. While the levels of contamination have been well below the health standards, the Nuclear Regulatory Commission (NRC) has formed a task force to examine the extent of such releases and why they are happening. In a meeting with NRC staff, the Nuclear Energy Institute, the industry's trade group, said it was beginning a voluntary program to closely monitor such leaks and inform state and local officials as well as the NRC when they occur even within plant boundaries. The industry is required to make such notifications only when there are offsite releases.
Source: http://www.fortwayne.com/mld/journalgazette/14536452.htm

20. *May 09, U.S. Environmental Protection Agency* — **Tools will help small drinking water utilities monitor drinking water.** The U.S. Environmental Protection Agency (EPA) has released a set of user−friendly multimedia products to help small drinking−water utilities determine federal monitoring requirements and prepare water compliance samples under the Safe Drinking Water Act. The tool kit features an interactive Rule Wizard Website that provides a complete list of all of the federal monitoring requirements for a selected type and size of public drinking water system, such as a community water system serving 3,300 people using ground water as a source of supply. A companion tool, Interactive Sampling Guide for Drinking Water Operators, features a CD−ROM with a video and a slide presentation that illustrates proper sampling procedures, which users can download to their local computer. Case studies are also presented on the CD−ROM to help public water system owners and operators work with state and local agencies when contaminants are detected.
Rule Wizard Website: http://www.rulewizard.org/
Source: http://yosemite.epa.gov/opa/admpress.nsf/74de46851771ad92852 5702100565d7d/2cd2706a3131d21185257169005277c1!OpenDocument

21. *May 08, Associated Press* — **Water now safe in part of lower ninth ward.** The Louisiana Health Department cleared the way Monday, May 8, for people to begin to return to the New Orleans neighborhood that faced Hurricane Katrina's worst fury, saying tap water in part of the Lower Ninth Ward is safe. The area encompasses the 10 blocks or so closest to the Mississippi River, where the ground is higher. In other parts of the neighborhood, people still must boil water before using it to drink, prepare food or bathe. Officials said they do not know when they'll be able to open those areas.
Source: http://abcnews.go.com/US/HurricaneKatrina/wireStory?id=19390 97

[Return to top]

Public Health Sector

22. *May 10, Agence France−Presse* — **Ivory Coast to vaccinate against polio.** Ivory Coast is planning to vaccinate more than five million children against polio on both sides of the line dividing the government−held south from the rebel−held north, the health ministry said. The campaign, which was in danger of weakening, is aimed at some 5.3 million children aged up to five years old. It will begin Friday, May 12, and last four days to ensure continued immunity

against the disease.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20060510/hl_afp/icoasthealthpoli o_060510171602

23. *May 10, International Herald Tribune* — **Birds return to Europe without virus.** The flocks of migratory birds that winged their way south to Africa last autumn and then back over Europe in recent weeks did not carry the H5N1 bird flu virus or spread it during their annual journey, scientists have concluded, defying health officials' dire predictions. International health officials had feared that the disease was likely to spread to Africa during the winter migration and return to Europe with a vengeance during the reverse migration this spring. That has not happened −− a significant finding for Europe, because it is far easier to monitor a virus that exists domestically on farms, but not in nature. In thousands of samples collected in Africa this winter, H5N1 was not detected in a single wild bird, officials and scientists said. In Europe, there have been only a handful of cases detected in wild birds since April 1, at the height of the northward migration. The number of cases in Europe has decreased so dramatically compared to February, when dozens of new cases were found daily, that experts believe the northward spring migration played no role.
Source: http://www.nytimes.com/2006/05/10/health/10cnd−flu.html?_r=1 &oref=slogin

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *May 10, Hardin County News (TX)* — **TxDOT to use EvacuLanes during hurricane evacuations.** Evacuating Southeast Texans is about to become safer. EvacuLanes are the Texas Department of Transportation's (TxDOT) effort to move motorists throughout the eight−county district in the event of a hurricane evacuation. EvacuLanes involve converting the shoulders of specific hurricane routes to handle more northbound evacuation traffic.
Source: http://www.thehardincountynews.com/news/2006/0510/Front_Page /001.html

25. *May 10, Messenger (IA)* — **Disaster drill in Iowa airport gives emergency personnel practice for the real thing.** In an emergency drill at Iowa's Fort Dodge Regional Airport Tuesday morning, May 9, airport officials and emergency responders had a chance to learn what they did well to help the "victims" and what could be improved. In the simulation, a plane just leaving the ground on takeoff is rocked by a rear explosion. Airport and city firefighters arrived on the scene and simulated extinguishing the burning plane. The Iowa Air National Guard lent its support in treating and transporting the wounded. In addition, a command center with representatives from all the agencies dealing with the disaster was set up near an airport hanger. In a post−drill review, airport Director Rhonda Chambers praised the participants' communication. She was also impressed with their attention to detail. The plane in the scenario was just topped off with 800 gallons of jet fuel. In response, firefighters called the Region V

Hazmat Team to deal with the spill and prevent it from reaching the waterways. Transportation Security Administration Director Jay Brainard said he was impressed with cooperation between the agencies.
Source: http://www.messengernews.net/top_stories_full.asp?4087

26. *May 10, Daily News (NC)* — **North Carolina hosts hurricane workshop.** In the effort to prepare for the next round of hurricanes, North Carolina officials from nearby counties, military bases and emergency agencies gathered Tuesday, May 9, in at the Onslow County Multipurpose Center to discuss ways to be prepared. Tuesday's workshop, in which officials listened to informational lectures from weather experts and participated in a federally mandated course on information sharing between agencies, was one of many events leading up to the onset of hurricane season. A large−scale exercise scheduled for Tuesday−Friday, May 23−26, will involve scenarios including response to a Category 5 hurricane as well as the arrival of a pandemic bird flu outbreak. On Wednesday, May 17, a shelter management group will review the county's shelter system to determine its readiness for hurricane season.
Source: http://www.jdnews.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=41541&Section=News

27. *May 09, Times Herald (MI)* — **U.S.−Canadian emergency workers participate in terrorism drill.** Two armed Detroit men believed to be linked to Port Huron bomb threats are dead after firing shots at St. Clair County, MI, sheriff deputies. This is the hypothetical scenario St. Clair County emergency workers began dealing with Monday, May 8, as part of a joint U.S. and Canada homeland−security exercise initiated by the U.S. Department of Defense. The mock events continued in the county through Wednesday, May 10. In conjunction with the county exercise, federal and North American agencies are dealing with other simulated events, including a hurricane in Florida and terrorist activity in New England. The objective is to give federal, state and local authorities the opportunity to work together to better prepare a response to national crises.
Source: http://www.thetimesherald.com/apps/pbcs.dll/article?AID=/20060509/NEWS01/605090306/1002

[Return to top]

Information Technology and Telecommunications Sector

28. *May 09, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−129A: Microsoft Windows and Exchange Server vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Microsoft Windows and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Systems affected: Microsoft Windows; Microsoft Exchange Server. Microsoft Security Bulletin Summary for May 2006 addresses vulnerabilities in Microsoft Windows and Exchange Server. Further information is available in the following US−CERT Vulnerability Notes:
VU#303452: http://www.kb.cert.org/vuls/id/303452
VU#945060: http://www.kb.cert.org/vuls/id/945060
VU#146284: http://www.kb.cert.org/vuls/id/146284
Solution: Microsoft has provided updates for these vulnerabilities in the Microsoft Security

Bulletin Summary for May 2006:
http://www.microsoft.com/technet/security/bulletin/ms06−may. mspx
Microsoft Windows updates are also available on the Microsoft Update site:
https://update.microsoft.com/microsoftupdate/v6/muoptdefault
.aspx?ln=en&returnurl=https://update.microsoft.com/microsoft
update/v6/default.aspx?ln=en−us
Source: http://www.uscert.gov/cas/techalerts/TA06−129A.html

29. *May 09, FrSIRT* — **Sophos Anti−Virus products cabinet file handling memory corruption vulnerability.** A vulnerability has been identified in various Sophos Anti−Virus products, which could be exploited by attackers or malware to take complete control of an affected system. Analysis: This flaw is due to a heap corruption error within the unpacking of Microsoft Cabinet (".CAB") files containing invalid folder count values within the CAB header, which could be exploited by attackers to execute arbitrary commands and compromise a vulnerable system by sending an e−mail containing a malicious CAB file to a machine being protected by an affected Anti−Virus product. Refer to source advisory for a complete list of vulnerable products.
Solution: Apply patches: http://www.sophos.com/support/knowledgebase/article/4934.htm l
Source: http://www.frsirt.com/english/advisories/2006/1730

30. *May 09, SecuriTeam* — **Websense Enterprise Web filtering bypass.** A Websense Enterprise vulnerability exists primarily due to the manner in which Cisco PIX and other Cisco filtering devices handle split packets in conjunction with Websense Enterprise integration. For each HTTP request the Cisco PIX or other Cisco device forwards individual packets to Websense to determine whether or not the request should be permitted.
Vulnerable systems: Cisco PIX software version 6.3; Cisco PIX ASA version 7; Cisco FWSM software version 2.3; Cisco FWSM software version 3.1.
Proof of concept: http://www.vsecurity.com/tools/WebsenseBypassProxy.java
Source: http://www.securiteam.com/securitynews/5MP042KIKC.html

31. *May 09, Security Tracker* — **Adobe Dreamweaver may let remote users inject SQL code.** A vulnerability was reported in Adobe Dreamweaver. A remote user may be able to inject SQL commands. Analysis: Code generated by Dreamweaver server behaviors for the ColdFusion, PHP mySQL, ASP, ASP.NET, and JSP server models may not properly validate user supplied input. A remote user can supply a specially crafted parameter value to execute SQL commands on the underlying database.
Affected versions: Dreamweaver 8 and Dreamweaver MX 2004.
Solution: The vendor has issued a fix (Dreamweaver 8.0.2 updater), available at:
http://www.adobe.com/support/dreamweaver/downloads_updaters. html#dw8
The Adobe advisory is available at:
http://www.adobe.com/support/security/bulletins/apsb06−07.ht ml
Source: http://securitytracker.com/alerts/2006/May/1016050.html

32. *May 09, Security Tracker* — **Sun Solaris libike IPSec IKE processing bug lets remote users deny service.** A vulnerability was reported in the 'in.iked' daemon on Sun Solaris. A remote user can cause denial−of−service conditions. Analysis: The 'libike' library does not properly process certain Internet Key Exchange (IKE) packets. A remote user can send specially crafted

packets to the target system to cause the in.iked(1M) daemon to crash or to potentially send invalid data to a peer system, which may in turn cause the peer system's in.iked daemon to crash.
Solution: Sun has issued the following fixes:
SPARC Platform: Solaris 9 with patch 113451−11 or later; Solaris 10 with patch 118371−07 or later.
x86 Platform: Solaris 9 with patch 114435−10 or later; Solaris 10 with patch 118372−07 or later.
Sun advisory: http://sunsolve.sun.com/search/document.do?assetkey=1−26−102 246−1
Source: http://securitytracker.com/alerts/2006/May/1016043.html

33. *May 09, FrSIRT* — **Linux kernel SCTP chunks handling remote denial−of−service vulnerabilities.** Multiple vulnerabilities have been identified in Linux kernel, which could be exploited by remote attackers to cause a denial−of−service. Analysis: The first issue is due to an error in the Stream Control Transmission Protocol (SCTP) code that uses incorrect state table entries when certain ECNE chunks are received in CLOSED state, which could be exploited by attackers to cause a kernel panic via a specially crafted packet. The second flaw is due to an error when handling incoming IP−fragmented SCTP control chunks, which could be exploited by attackers to cause a kernel panic via a specially crafted packet.
Affected products: Linux kernel version 2.6.16.14 and prior.
Solution: Upgrade to Linux Kernel version 2.6.16.15: http://www.kernel.org
Source: http://www.frsirt.com/english/advisories/2006/1734

34. *May 09, eWeek* — **Virginia official discusses the fight against cybercrime.** Gene Fishel, assistant attorney general in the state of Virginia's Attorney General's office, delivered the keynote address during Ziff Davis' Tuesday, May 9, "Enterprise Applications Virtual Tradeshow," where he provided some prime examples of computer crime, and what IT shops can do about it. Because two of the United States' Internet powerhouses are headquartered in Virginia −− AOL and MCI −− Fishel said that about 80 percent of the traffic on the Internet passes through Virginia at some point. This little−known fact is actually what provides the Virginia Attorney General's office with jurisdiction over many criminal computer crimes. "It allows us as a state to test computer crime laws before they go federal," said Fishel. "Spam is a good example of that." The Virginia Attorney General's office was the first in the nation to criminalize spam with its anti−spam law; there's now a federal law in place modeled on Virginia's efforts.
Source: http://www.eweek.com/article2/0,1895,1959790,00.asp

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: US−CERT is aware of publicly available, working exploit code for an unpatched vulnerability in Oracle Export Extensions. Successful exploitation may allow a remote attacker with some authentication credentials to execute arbitrary SQL statements with elevated privileges. This may allow an attacker to access and modify sensitive information within an Oracle database.

More information about this vulnerability can be found in the following:

Secunia Advisory19860
http://secunia.com/advisories/19860

Security Focus Oracle Vulnerability Report
http://www.securityfocus.com/bid/17699/discuss

Red Database Security Oracle Exploit Report
http://www.red−database−security.com/exploits/oracle−sql−injection−oracle−dbms_export_extension.html

US−CERT recommends the following actions to mitigate the security risks:

Restrict access to Oracle:
Only known and trusted users should be granted access to Oracle. Additionally, user accounts should be granted only those privileges needed to perform necessary tasks.

Change login credentials for default Oracle accounts:
Oracle creates numerous default accounts when it is installed. Upon installation, accounts that are not needed should be disabled and the login credentials for needed accounts should be changed.

Oracle has released Critical Patch Update April 2006. This update addresses more than thirty vulnerabilities in different Oracle products and components.
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2 006.html

Phishing Scams

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 38566 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 41170 (−−−), 25 (smtp), 32459 (−−−), 6346 (gnutella−svc), 80 (www), 49159 (−−−) 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

35. *May 10, WOAI (TX)* — **Hazmat investigates substance at San Antonio high school.** Hazmat officials were called to Southwest High School to investigate a suspicious container Tuesday night, May 9. Hazmat found the substance to be non−hazardous. However, a firefighter experienced a problem with his breathing tank. It is unknown if the incident was caused by human error or an equipment malfunction. The city's fire department recently changed their equipment manufacturer, due to various difficulties firefighters were experiencing.
Source: http://www.woai.com/news/local/story.aspx?content_id=51E0267C−CD2B−484E−8E84−C88273FDEA6B

[Return to top]

General Sector

36. *May 09, Associated Press* — **Reward offered in California explosives theft.** Authorities offered a $25,000 reward Tuesday, May 9, for information about the theft of more than 500 pounds of explosives from a storage bunker near a gold mine. "The big concern for us is who took these explosives and why did that person take them," said John D'Angelo, spokesperson for the federal Bureau of Alcohol, Tobacco, Firearms and Explosives. The agency is investigating the theft with the San Bernardino County Sheriff's Department as well as sharing information with the FBI's Joint Terrorism Task Force and the U.S. Forest Service. The theft was reported on May 3, at Gold Mountain Mine Co. about 90 miles east of Los Angeles. Associates of the mine owner found someone had broken into the explosives storage facility and 686 sticks of dynamite and a 30−pound bag of ammonium nitrate were missing, D'Angelo said.
Source: http://news.yahoo.com/s/ap/20060510/ap_on_re_us/brf_explosiv es_theft_1

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

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.

Department of Homeland Security Disclaimer

The DHS 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.