Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 17 May 2005

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- CNET News reports there is a new sophisticated form of phishing threat that attempts to use stolen consumer data to steal from individual account holders at specific banks. (See item 3)
- The Federal Emergency Management Agency announces the beginning of National Hurricane Preparedness Week, encouraging individuals in hurricane−prone areas to take safety preparedness measures in anticipation of the upcoming 2005 hurricane season. (See item 18)
- US−CERT has issued Technical Cyber Security Alert TA05−136A: Apple Mac OS X is affected by multiple vulnerabilities. (See item 22)

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. *May 16, Associated Press* — **Workers at Boston utility go on strike.** About 2,000 linemen and engineers at electric and gas utility NStar went on strike early Monday, May 16, after negotiators failed to reach a new contract agreement. Utility Workers Union of America Local 369 struck at 12:01 a.m. when its contract expired, said President Gary Sullivan. The union said it had set up pickets Monday morning at seven locations, including NStar's corporate headquarters in Boston's Back Bay section. NStar said it has assigned managers and contractors to ensure service to its 1.1 million electric customers and 300,000 natural gas customers. The

investor−owned utility has about 3,000 employees. Both sides said they were willing to return to the table to reach an agreement.
Source: http://www.nytimes.com/aponline/business/AP−NStar−Labor.html ?

2. *May 16, North American Electric Reliability Council* — **North American Electric Reliability Council issues 2005 summer reliability assessment.** The North American Electric Reliability Council (NERC) released its 2005 Summer Assessment on Monday, May 16, which provides an assessment of projected electricity supply and demand in North America for the upcoming summer season. “NERC expects generating resources to be adequate to meet projected demand for electricity in North America this summer,” said Michehl R. Gent, NERC President and CEO. “If all operating entities comply with NERC reliability standards, even under extreme conditions, the system can be operated reliably,” he added. The assessment states that transmission systems are expected to perform reliably, although transmission congestion is expected to occur in some areas of North America this summer. Fuel supplies, inventories, and deliveries are also expected to be adequate. Even in areas where resources are expected to be adequate to serve all customer demand, unanticipated equipment problems and extremely hot weather can combine to produce situations in which demands temporarily exceed available generation and transmission capacity. The 2005 peak demand for electricity is projected to increase 5.9 percent in total compared to the actual 2004 non−coincident summer peak, although projected demand growth varies widely among the regions.
2005 Summer Reliability Assessment: http://www.nerc.com/~filez/rasreports.html
Source: http://www.nerc.com/

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 15, CNET News* — **New phishing attack uses real identity to lure victims.** Security researchers are reporting a new brand of phishing attack that attempts to use stolen consumer data to steal from individual account holders at specific banks. Workers at hosted security services company Cyota are sharing the details of this more sophisticated form of phishing threat, which forsakes the mass−targeting approach traditionally used in the fraud schemes in favor of taking aim at individual consumers. According to Cyota, the phishing e−mails arrive at bank customers' in−boxes featuring accurate account information, including the customer's name, e−mail address and full account number. The messages are crafted to appear as if they have been sent by the banks in order to verify other account information, such as an ATM

personal−identification number or a credit card CVD code, a series of digits printed on the back of most cards as an extra form of identification. Cyota co−founder Amir Orad said he believes that the criminals responsible for the personalized phishing attacks have purchased stolen consumer data from other individuals and are trying to get information that's even more sensitive to sell to someone else at a premium.
Source: http://news.com.com/New+phishing+attack+uses+real+ID+hooks/2100−7349_3−5706305.html?tag=nefd.top

4. *May 15, San Francisco Chronicle* — **California patients' medical data stolen.** A former branch manager at a San Jose, CA, medical group has been charged with stealing the confidential records of nearly 185,000 patients −− mostly South Bay residents, authorities reported. The U.S. attorney's office charged Joseph Nathaniel Harris on Friday, May 13, with stealing two computers and a compact disc that contained patient records from the San Jose Medical Group on March 28, according to a complaint filed in U.S. District Court in San Jose. San Jose Medical Group CEO Ernie Wallerstein in April notified at least 185,000 patients that their data was compromised. The missing disc contained a wealth of patient data, including names, addresses, Social Security numbers, dates of birth, insurance data, bill records and detailed medical histories. Harris worked as the branch manager of the San Jose Medical Group's McKee clinic in August and September of last year, court records said.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/05/15/THEF T.TMP

5. *May 13, ABC Alaska News* — **Increase in counterfeit money seen in Alaska.** While they usually see up to $1,200 dollars a month in counterfeit money in Alaska, over the past four months federal officials report seeing between $4,000−$6,000 a month, and some of the counterfeit is printed on genuine currency. The Secret Service says that in Alaska it started seeing fake $100 bills printed on bleached $1 bills last November. This month it started seeing $50 bills printed on bleached $5 bills. Federal officials do not know what is causing the rise in counterfeit distribution. Secret Service agent Mac Whisler says, "I think it just happens when someone gets the idea to start printing and we see a rise and that's what happened here."
Source: http://www.aksuperstation.com/artman/publish/article_669.sht ml

[Return to top]

Transportation and Border Security Sector

6. *May 16, Houston Chronicle* — **Texas governor urged to 'disinvite' Minutemen.** U.S. Rep. Sheila Jackson Lee, D−Houston, called for Governor Rick Perry to ask the Minutemen not to expand militia patrols of the U.S.−Mexico border from Arizona to Texas. Organizers have expressed an interest in recruiting in Texas and beginning patrols along the Rio Grande in October. Jackson Lee said she sees it as the "dereliction of duty" by the federal government not to have improved staffing in customs and the border patrol. She said she will advocate that money be increased to hire more workers to patrol the borders.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/politics/3183334

7. *May 16, USA TODAY* — **Backscatter X−ray machines in use this year.** The agency in charge of the nation's air security expects later this year to begin using a controversial X−ray machine

that will show airport screeners a clear picture of what's under passengers' clothes −− whether weapons or just bare skin. Screeners plan to test the "backscatter" machines at several U.S. airports, the Transportation Security Administration (TSA) says. The refrigerator−sized machines are considered a breakthrough in scanning technology but have been labeled "a virtual strip search" by the American Civil Liberties Union. Security workers using the machines can see through clothes and peer at whatever may be hidden in undergarments, shirts or pants. The images also paint a revealing picture of a person's nude body. The devices can potentially be used to screen hundreds of millions of air travelers each year, although TSA says more study is needed to determine how the devices may be used at U.S. airports. Backscatter technology has been on the sidelines for nearly four years but seems poised now to move to the forefront of aviation security. The machines are already used by U.S. Customs agents at 12 airports to screen passengers suspected of carrying drugs. They're also getting a test run at a terminal in London Heathrow Airport, the first major airport to use them.
Source: http://www.usatoday.com/travel/news/2005−05−15−airport−xray− bottomstrip_x.htm

8. *May 16, Department of Transportation* — **Secretary Mineta calls for reform of aviation trust fund.** If the nation hopes to keep up with growing demand on our aviation system, we'll need to start thinking about a better way to pay for new airport towers, runways and safety equipment, Department of Transportation Secretary Norman Y. Mineta said Monday, May 16, during a visit to General Electric's Durham Aircraft Engine Facility in North Carolina. Mineta launched a weeklong bus tour across the southeast with a call for reform of the Aviation Trust Fund, the financing mechanism used to pay for new or improved airport infrastructure projects. Mineta said the fund doesn't raise enough money to pay for needed improvements because revenues are based on a percentage of the fare each traveler pays for a plane ticket. He said ticket prices at the end of 2004 were down nine percent from their peak in 2000. The fund raised just over $9 billion in 2004, $4 billion short of the $13 billion need to make necessary improvement to the system last year.
Source: http://www.dot.gov/affairs/dot7705.htm

9. *May 13, Department of Homeland Security* — **Over $140 million in grants to secure ports announced.** The U.S. Department of Homeland Security (DHS) on Friday, May 13, announced $140,857,128 in port security grants. The FY 2005 Port Security Grant Program (PSGP) uses a risk−based formula to allocate funds to protect our ports from acts of terrorism. The program fortifies security at our nation's ports by providing funding to increase protection against potential threats from small craft, underwater attacks and vehicle borne improvised explosives, and to enhance explosive detection capabilities aboard vehicle ferries and associated facilities. The new risk−based formula considers three elements: threat, vulnerability, and consequence. As part of this risk−management approach, the port security grant program will ensure federally regulated ports, terminals, and U.S. inspected passenger vessels receiving the funds represent assets of the highest national strategic importance. Sixty−six port areas have been identified as eligible applicants for inclusion in the FY 2005 program. Successful applicants will be awarded through a competitive process. DHS designed this program in coordination with the Department of Transportation and the American Association of Port Authorities. DHS has collectively awarded $489.4 million in previous rounds.
Attachment A: Port Areas Eligible for Consideration of Funding:
http://www.dhs.gov/dhspublic/display?content=4502
Source: http://www.dhs.gov/dhspublic/display?content=4501

[Return to top]

Postal and Shipping Sector

10. *May 16, Associated Press* — **UPS to purchase Overnite.** United Postal Service, Inc., (UPS), the world's biggest shipping carrier, is buying trucking company Overnite Corp. for about $1.25 billion in cash as it continues to expand its heavy freight delivery business. The deal announced Monday, May 16, marks UPS' largest single acquisition ever, and follows the Atlanta−based company's decision last week to spend $24 million to build and equip five regional freight hubs at airports around the country. The new hubs will allow UPS to ship freight weighing more than 150 pounds using more of its own planes. Similarly, the Overnite purchase will allow UPS to deliver heavy freight in its own trucks rather than solely contracting out that service as it has done in the past. UPS will still use some third−party providers, chief financial officer Scott Davis said. Richmond, Virginia−based Overnite, which serves more than 60,000 customers throughout North America, earned $63.3 million on revenue of $1.65 billion in 2004.
Source: http://biz.yahoo.com/ap/050516/ups_overnite.html?.v=8

[Return to top]

Agriculture Sector

11. *May 16, Iowa Ag Connection* — **Iowa officials announce system to help prevent spray drift.** Iowa Secretary of Agriculture Patty Judge Friday, May 13, announced that the Iowa Department of Agriculture and Land Stewardship, with the help of the Iowa Geological Survey Bureau, has created an interactive mapping system designed to help prevent chemical spray drift onto Iowa's orchards and vineyards. Ag Secretary Judge stated, "This is a fantastic new tool in our continuing efforts to help Iowa's producers and applicators prevent spray drift onto our orchards and vineyards. Producers and chemical applicators will be able to log onto our Website, click on Orchard/Vineyard GIS/IMS Map and see exactly where Iowa's orchards and vineyards are located." Iowa apple orchards and grape vineyards are both growing industries that add to Iowa's agriculture economy.
Website: http://www.agriculture.state.ia.us
Source: http://www.wisconsinagconnection.com/story−regional.cfm?tble =IA2005&ID=406

12. *May 16, Illinois Ag Connection* — **Gypsy Moth treatments to begin in Illinois.** Weather permitting, the Illinois Department of Agriculture will begin its 2005 Gypsy Moth treatment program Wednesday, May 18. The four−day, three−county treatment program has been timed to coincide with feeding by the destructive moths' caterpillars. However, the specific application dates could be affected by wind or rain. Gypsy Moths feast on the foliage of trees and shrubs, and large populations are capable of stripping plants bare. They obtained their name because the female moth cannot fly and typically lays her eggs on objects near where she is feeding, including campers, grills and backpacks. When these items are moved, the eggs ride along like a nomadic gypsy. Funding for the treatments comes from the Slow the Spread program, a joint local, state and federal effort to reduce and control the spread of the Gypsy Moth.

Maps of the specific treatment areas: http://www.urbanext.uiuc.edu/gypsymoth
Source: http://www.usagnet.com/story−regional.cfm?tble=IL2005&ID=377

13. *May 15, Agence France Presse* — **Chinese officials report two outbreaks of foot and mouth disease.** Chinese officials have confirmed two outbreaks of foot and mouth disease in a rare acknowledgement that the problem even exists inside its borders, the World Organization for Animal Health (OIE) said in a statement posted on its Website on Friday, May 13. More than 200 head of cattle were destroyed after the outbreaks were discovered, both in the eastern part of the country. China's agriculture ministry reported the two cases on Friday, according to the organization. Both outbreaks happened last month. One was in Wuxi city, Jiangsu province, where 15 cases were found and 183 animals destroyed, according to the statement. The other was in Tai'an city of Shandong province, where 17 cases were diagnosed and 40 head of cattle were destroyed, it said. Foot−and−mouth disease is a severe, highly contagious viral disease affecting cattle, pigs, sheep and other livestock. It is not usually fatal but causes severe losses in the production of meat and milk.
OIE Statement: http://www.oie.int/Messages/050513CHN.htm
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050515/hl_afp/chinafarmhealth_050515200452

[Return to top]

Food Sector

14. *May 13, Food and Drug Administration* — **Prime Deli Corporation recalls sandwiches.** Prime Deli Corporation of Lewisville, TX, is recalling 63,476 units of 7/Eleven Grilled Sandwich and 7/Eleven Big Eats brand sandwiches because they have the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Although healthy individuals may suffer only short−term symptoms such as high fever, severe headache, stiffness, nausea, abdominal pain and diarrhea, Listeria infection can cause miscarriages and stillbirths among pregnant women. The sandwiches are labeled with “Handmade On” codes of 0502 through 0507 located on the product label. All 7/Eleven Grilled Sandwich and 7/Eleven Big Eats brand sandwiches were sold in 7/Eleven stores in North and Central Texas. There have been no reports of illnesses associated with the recalled product.
Source: http://www.fda.gov/oc/po/firmrecalls/prime05_05.html

[Return to top]

Water Sector

15. *May 15, Associated Press* — **U.S. Drought Monitor reports no 'exceptional' drought for West.** For the first time in three years, the U.S. Drought Monitor does not show exceptional drought −− its most severe category −− anywhere in the West. But drought remains an issue for much of the region, with the weekly Drought Monitor showing varying degrees of drought in Idaho, Montana, Oregon, Washington and Wyoming. Mark Svoboda, a climatologist with the National Drought Mitigation Center at the University of Nebraska−Lincoln, said Friday, May

13, there's some cause for "guarded optimism." Recent moisture has provided some benefit to parts of Montana, where the effects of drought have been felt for years. Before this week, pockets of southwest and southeast Montana had fallen into the category of "exceptional" drought. "We're definitely pleased to see this area start to see improvement, but we have a long way to go to dig out of the drought," Svoboda said Friday. According to the Drought Monitor, extreme hydrological drought remains "firmly entrenched" in parts of Idaho, Montana and Wyoming, despite decent moisture and cooler temperatures.
U.S. Drought Monitor: http://www.drought.unl.edu/dm/monitor.html
Source: http://www.casperstartribune.net/articles/2005/05/15/news/casper/1f0d97108e565f0f8725700100086c0f.txt

[Return to top]

Public Health Sector

16. *May 15, New York Times* — **After its epidemic arrival, Severe Acute Respiratory Syndrome vanishes.** Two and a half years after Severe Acute Respiratory Syndrome (SARS) infected thousands of people around the world and brought dire predictions of recurring and deadly plague, the virus has again provided a surprise. It has disappeared, at least for the moment. Not a single case of SARS has been reported this year or in late 2004. It is the first winter without a case since the initial outbreak in late 2002. Additionally, the epidemic strain of SARS that caused at least 774 deaths worldwide by June of 2003 has not been seen outside a laboratory since then. However, health officials in China warn that SARS could still pose a threat. This caution partly reflects the lack of knowledge about the virus. Most health officials are not counting on the rosiest scenario −− that SARS has simply mutated into oblivion. "We'd be lucky to believe that, and that would be very nice, but there is no research to support that," said Dr. Julie Hall, the SARS team leader at the Beijing office of the World Health Organization. "Just because we've not seen SARS anymore this year doesn't mean it is not out in the wild this year," said Hall.
Information about SARS: http://www.cdc.gov/ncidod/sars/
Source: http://www.nytimes.com/2005/05/15/health/15sars.html?adxnnl=1&adxnnlx=1116266508−XAHADp2uEnK7a3nkX7+OhA

17. *May 13, InformationWeek* — **Massachusetts begins new health pilot.** Massachusetts on Friday, May 13, kicked off the formal launch of three large−scale regional health information technology pilots involving hospitals, physician practices, nursing homes, and other care facilities in three large communities. The projects aim to examine the effectiveness and practicality of widely implementing electronic health records in community practice settings and could serve as the model for statewide, or perhaps even nationwide, adoption of digitized medical−record systems. The three communities involved with the pilot are Brockton, a city in southeastern Massachusetts, Newburyport, a seaport district on the north shore of the state, and northern Berkshire, a region in western Massachusetts. While the three communities will individually deploy the systems −− the three regions will not be wired together during the pilots −− the aim is to create an environment that could connect them, and other regional efforts, in the future so that patient records can be electronically shared statewide. A goal of the projects is to demonstrate that digitizing and electronically sharing patient records, lab reports, pharmacy and other data, leads to better medical decisions, fewer errors, and lower costs.

Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=J2KNECSZ1UPN0QSNDBGCKHSCJUMEKJVN?articleID=163102079

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

18. *May 16, Federal Emergency Management Agency* — **National Hurricane Preparedness Week begins.** Under Secretary of Homeland Security for Emergency Preparedness and Response, Michael D. Brown, joined representatives from the National Oceanic and Atmospheric Administration (NOAA) and the director of the National Hurricane Center to kickoff National Hurricane Preparedness Week on Monday, May 16. Brown emphasized the important hurricane preparedness measures individuals should take in anticipation of the upcoming 2005 hurricane season. Brown pointed to a recent poll that found a fourth of the people in 12 east and Gulf Coast hurricane−prone states are doing nothing to prepare for the next hurricane that could hit their area. The Federal Emergency Management Agency's "Are You Ready" guide details hurricane preparedness techniques Brown spoke about for individuals to follow in preparing for the upcoming storms. The three main steps to disaster preparedness highlighted in the guide are: make a plan, make a kit, get informed. These simple steps are vital to guarding against injury to life and property that could come from the effects of a hurricane or any disaster.
FEMA's "Are You Ready" guide: http://www.FEMA.gov and http://www.ready.gov
Source: http://www.fema.gov/news/newsrelease.fema?id=17476

19. *May 15, Del Rio News−Herald (TX)* — **Cyber−terrorism exercise helps participants pinpoint vulnerabilities.** An exercise conducted by the University of Texas at San Antonio's Center for Infrastructure Assurance & Security (CIAS) on Thursday, May 12, was designed to help local law enforcement and medical personnel, elected officials and those responsible for critical infrastructure to pinpoint vulnerabilities in their operations. Exercise participants included Laughlin Air Force Base security and communications personnel, members of the Val Verde County Sheriff's Office, and the Del Rio Police Department. The exercise also included members of the local medical community. Participants in the "table−top exercise" were given a series of "what if" scenarios, then asked to discuss and complete a list of questions. In one scenario, personnel at the local public library called their computer system administrators to say that many of their Internet work stations had rebooted at roughly the same time. Participants in the exercise read the scenario, then discussed what would be done. Better communication and more knowledge were seen as keys to countering cyber−terrorists, and all of the exercise's participants committed to future training.
The University of Texas at San Antonio's Center for Infrastructure Assurance & Security: http://www.utsa.edu/cias/
Source: http://www.delrionewsherald.com/report.lasso?wcd=9068

20. *May 15, NorthJersey.com* — **New Jersey first responders attend disaster training.** The Center for National Response, a long defunct 2,800−foot highway tunnel, is now a disaster response training camp run by the National Guard in Standard, WV. For two days earlier this month, it became home to the North Jersey Urban Search and Rescue strike team, formed last year to provide emergency response at disasters. The elite squad, composed of paid North Jersey firefighters from nine departments and the Port Authority Police, was formed because of its proximity to major New Jersey/New York transportation hubs, such as the Hudson River crossings. In the event of a terrorist attack or natural catastrophe, they would be called on to look for victims until the arrival of NJ Task Force 1, a statewide response team with greater resources, such as search dogs. The center provides a free, customized setting for training in counter−terrorism training and responding to attacks by weapons of mass destruction. With federal homeland security grants, NJ Task Force 1 spent slightly over $30,000 for food, transportation and instructors for the North Jersey team. Seventy−two police officers and firefighters participated in the two−day drill. Since its inception, more than 22,000 civilian first responders, police, soldiers and emergency medical service personnel have attended hands−on exercises at the national center.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2Njk0MTU1JnlyaXJ5N2Y3MTdmN3ZxZWVFRXl5Mw==

21. *May 13, Kennebec Journal (ME)* — **Mall in Maine holds homeland security drill.** A homeland security drill conducted Wednesday near the Maine Mall in South Portland, ME, highlighted strengths and weaknesses in Greater Portland's disaster response plan. The daylong event involved about 250 public safety responders throughout the region, making it the largest disaster drill held in Maine since the September 11, 2001, terrorist attacks. The drill simulated three disaster scenarios: an illegal drug laboratory with a bomb, a hazardous materials spill and a bomb in a suitcase. Problems cropped up because some radio equipment wasn't compatible, there were too few ambulances to handle mock injuries and emergency responders weren't interviewed following the drill. A lack of ambulances became a problem when a responder had to remove an injured person from the building while it was still under mock gunfire. The responder simply used the nearest available truck and was successful. Edward Googins, South Portland's police chief, also was concerned that no one interviewed responders for details that would have helped in follow up investigations of each incident. "We had some of the best witnesses around, and we didn't even talk to them," he said.
Source: http://kennebecjournal.mainetoday.com/news/local/1618619.sht ml

[Return to top]

Information Technology and Telecommunications Sector

22. *May 16, US−CERT* — **US−CERT Technical Cyber Security Alert TA05−136A: Apple Mac OS X is affected by multiple vulnerabilities.** Apple has released Security Update 2005−005 to address multiple vulnerabilities affecting Mac OS X version 10.3.9 (Panther) and Mac OS X Server version 10.3.9. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities addressed by the update include disclosure of information and denial of service.

Apple advisory and updates: http://docs.info.apple.com/article.html?artnum=301528
Source: http://www.us−cert.gov/cas/techalerts/TA05−136A.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: A new vulnerability was identified in Cisco products, which may be exploited by attackers to bypass the security restrictions. The flaw resides in the Cisco Firewall Services Module (FWSM) when configured for exceptions in content filtering, which may be exploited by attackers to bypass access−list entries intended to explicitly filter inbound TCP packets.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 27015 (halflife), 6881 (bittorrent), 135 (epmap), 80 (www), 1433 (ms−sql−s), 139 (netbios−ssn), 53 (domain), 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

23. *May 15, Issues in Focus* — **Industry takes proactive steps to fight terrorism.** Property Protection Journal, a Real Estate Media newsletter, in conjunction with the Real Estate Roundtable invited leaders in the apartment, office, and retail sectors as well as a prominent real estate attorney, terrorism insurance executive, and two senior officials from the Department of Homeland Security (DHS) to meet in executive forum on April 14, at Washington, DC's Four Seasons Hotel to discuss how commercial real estate and domestic anti−terrorism initiatives mix −− and how well the industry is doing to address this issue. The executive forum took place just after DHS wrapped up its third annual Topoff anti−terrorism exercises in New Jersey and Pennsylvania, which were conducted simultaneously from April 4 to April 8. Topoff, which stands for Top Officials, is a congressionally mandated exercise managed by DHS that tests state and local governments' abilities to respond and plan for a terrorist attack −− in this year's case with Topoff3, a biological assault. Among private businesses participating in the exercise were 65 real estate companies who helped coordinate the property owners' interaction with DHS.
Source: http://www.globest.com/issuesinfocus/issuesinfocus/

24.

May 10, Washington Post — **Defense jobs in Northern Virginia at risk.** The Department of Defense will have to move as many as 50,000 employees out of Northern Virginia office buildings if it strictly enforces new security regulations, and local lawmakers say Secretary of Defense Donald H. Rumsfeld could announce some of those relocations soon. Although Pentagon officials have declined to provide details, Rumsfeld said recently that the department wants to move workers from leased office space to buildings it owns to cut long−term costs. The department would have to begin moving those jobs anyway because of anti−terrorism regulations it adopted two years ago, which require, among other things, that buildings not on military bases be set back at least 82 feet from traffic to protect against truck bombs. The new standards, already in effect for new construction, become mandatory in October for new leases and will be phased in for all lease renewals starting in 2009. The Pentagon rents about eight million square feet of space in 140 Northern Virginia buildings −− and almost none of them can meet the new requirement, according to analysts and lawmakers.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/09/AR2005050901087.html

[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 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) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the

DHS/IAIP Daily Report Team at (703) 983−3644 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