Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 26 May 2005

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

Daily Highlights

- The Boston Herald reports that fearing a catastrophic terrorist attack or chemical leak, city officials are seeking to prevent hazardous materials from traveling through Boston on rail cars. (See item 6)
- Reuters reports Interpol is warning that bioterrorism using crude biological agents is a credible threat which authorities worldwide underestimate. (See item 18)
- The Associated Press reports Montana state agencies failed to remove private information before retiring outdated state computers, risking public disclosure of Social Security and credit card numbers, medical records, and income taxes. (See item 26)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *May 25, Union Leader (NH)* — **Seabrook Station official says plant remains secure.** A spokesperson for Seabrook Station, located near Portsmouth, NH, said on Tuesday, May 24, that the nuclear power plant is secure, despite the Nuclear Regulatory Commission (NRC) identifying a problem with the security fence surrounding the facility that is intended to keep out intruders. According to Alan Griffith, plant spokesperson, the problem occurred with a portion of the Perimeter Intrusion Detection System (PIDS) −− part of the security fence. PIDS

is one of three elements of Seabrook Station's security operation. The others are a variety of physical barriers, which limit entrance options, and an armed security force. The PIDS problem was detected around May 5 during routine testing of the system during an inspection by Region 1 of the NRC. Citing security concerns, Griffith was reluctant to discuss specifics, calling the information safeguarded. He did, however, say that, "At no time would we leave any vulnerability unaddressed." "We have multiple layers of security. . . . We have many ways of doing the same thing. At no point have we ever lost our ability to protect the public's health and safety," said Griffith. Griffith said at no time have unauthorized persons ever penetrated the plant due to the PIDS problem.
Source: http://www.theunionleader.com/articles_showfast.html?article =55236

2. *May 25, The Bulletin (OR)* — **PacifiCorp purchased by MidAmerican.** MidAmerican Energy Holdings Company will purchase PacifiCorp, the parent company of Pacific Power, from Scottish Power, in a deal valued at approximately $9.4 billion, the companies announced Tuesday, May 24. The $9.4 billion sale includes $5.1 billion in cash and approximately $4.3 billion in debt assumption and preferred stock. PacifiCorp will continue operating under its current name and will remain headquartered in Portland, OR. The company operates as Pacific Power in Oregon, Wyoming, Washington and northern California, and as Utah Power in Utah and Idaho. MidAmerican's U.S. electric generation will total more than 16,000 megawatts after the acquisition. It will serve about three million electric and natural gas customers in 10 contiguous states.
Source: http://www.bendbulletin.com/news/story.cfm?story_no=16386

[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 25, IDG News Service* — **New phishing scam hits Yahoo instant messenger.** Users of the instant messaging (IM) application from Yahoo are being warned of a new threat spreading via IM. The scam is a phishing attack in which users are sent a link that leads to a fake Website, which asks for their Yahoo credentials. The link appears to be targeted at gaming enthusiasts and is rated by IMLogic, an IM software company, as a medium risk threat. Yahoo users are being warned to look out for the threat, and administrators are advised to use content filtering to guard against the scam, and to download the latest antivirus updates.
Source: http://www.infoworld.com/article/05/05/25/HNnewimphishingscam_1.html?source=rss&url=http://www.infoworld.com/article/05/

05/25/HNnewimphishingscam_1.html

4. *May 24, Canadian Press* — **Canadian federal review urges more money to fight money−laundering criminals, terrorists.** The Canadian federal government will have to spend a lot more money on new tools and training to stay ahead of well−funded criminals and terrorists involved in money−laundering, says an internal review. Over the past five years, the Canadian government has organized a multi−agency fight against organized crime and money laundering as well as tracking terrorist groups that raise money in Canada, an internal audit prepared for the federal Finance Department says. However, the agencies need more resources from the government to keep up with well−financed criminals, according to the report. The Canadian government has spent about US$137 million in the past five years on various agencies that work together to combat money laundering and organized crime. About US$72 million of the money has gone to establish the Financial Transactions and Reports Analysis Center (Fintrac), which follows large money transactions through banks, brokerage firms, real estate agents and casinos. However, since 2002−03, Fintrac hasn't had any new funding to update technology −− investment it needs to keep following the money trails that could lead back to organized criminals, says the audit.
Report: http://www.fin.gc.ca/toce/2005/nicml−incba_e.html
Source: http://news.yahoo.com/news?tmpl=story&u=/cpress/20050524/ca_pr_on_na/crime_fighting_funds_1

5. *May 23, IT−Observer* — **Consumers believe that identity theft protection needs improvement.** Despite a recent push in identity theft prevention awareness by major organizations and government agencies, 75 percent of U.S. citizens believe that their identity is no more secure than one year ago. Consumers do not believe current and traditional methods of security are good enough to protect them against identity theft. A recent survey, commissioned by Intervoice, finds that most Americans believe that technology puts them at the greatest risk for identity theft. Though, more than 60 percent of consumers are not limiting their use of technology related services in order to minimize the risk. Key findings of the survey are: Technology causes the most concern about identity theft, more so than person−to−person interactions, such as dealing with store employees, 20 percent have stopped making purchases via telephone in order to mitigate the problem of identity theft, over 40 percent of individuals in the U.S. would be willing to use national identification card as their primary means of protecting themselves from identity theft and 81 percent of consumers believed that they are personally responsible to protect themselves against identity theft.
Survey Results: http://www.intervoice.com/about/pressroom/press_releases/200 5/p1605.pdf
Source: http://www.it−observer.com/articles.php?id=735

[Return to top]

Transportation and Border Security Sector

6. *May 25, Boston Herald (MA)* — **Boston wants Hazmat ban on trains traveling into city.** Fearing a catastrophic terrorist attack or chemical leak, local and federal officials are pushing to prevent deadly toxins from going through the Boston Hub on rail cars. "In our day and age when we're trying to make the city safe from terrorist activity, I think homeland security on our rail system has to be of paramount concern," Boston City Councilor Stephen Murphy said.

Following the lead of city officials in Washington, DC, Murphy wants railroad cars hauling deadly chemicals re−routed around the city. The proposal, which cites the potential deaths of "tens of thousands" and a "catastrophic economic impact of $5 billion," would ban "ultra−hazardous" cargoes within two and one half miles of Copley Square, unless they have a Boston Fire Department permit. While the courts sort out whether cities have the power to ban railroad cars from going through their neighborhoods, U.S. Rep. Edward Markey (D−Malden) has filed federal legislation to increase rail security and ban deadly chemicals from urban areas.
Source: http://news.bostonherald.com/localPolitics/view.bg?articleid =84671

7. *May 24, U.S. Northcom* — **Aircraft warning system for the Washington, DC area.** A new warning signal for communicating with aircraft was recently deployed within the Washington, DC area. The Visual Warning System (VWS) fielded by North American Aerospace Defense Command (NORAD), in coordination with the Federal Aviation Administration and the Air Force Rapid Capabilities Office, became operational May 21. This new security measure is a communication tool to warn pilots who are violating the National Capital Region's restricted airspace −− the Air Defense Identification Zone (ADIZ), established by the Federal Aviation Administration −− and who cannot be contacted by radio. The VWS is a ground−based system that uses safety−tested, low−level beams of alternating red and green lights to alert pilots they are flying without approval in restricted airspace. "The lights are designed so that illumination is eye−safe and non−hazardous at all ranges," said Michael Perini, director of public affairs for NORAD and U.S. Northern Command. The VWS system is considered a Class One laser device, the safest class possible. It is eye safe at all distances. Only aircraft that are unauthorized, or unidentified, and unresponsive are visually warned. "The VWS is designed to prompt immediate action by the pilot to contact air traffic control and exit the restricted airspace," Perini said.
Source: http://www.northcom.mil/index.cfm?fuseaction=news.showstory&storyid=0F9ADF4A−97CD−40F8−675F45279E6798C6

8. *April 26, Government Accountability Office* — **GAO−05−557: Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts (Report).** In January 2002, U.S. Customs and Border Protection (CBP) initiated the Container Security Initiative (CSI) to address the threat that terrorists might use maritime cargo containers to ship weapons of mass destruction. Under CSI, CBP is to target and inspect high−risk cargo shipments at foreign seaports before they leave for destinations in the United States. In July 2003, the Government Accountability Office (GAO) reported that CSI had management challenges that limited its effectiveness. Given these challenges and in light of plans to expand the program, GAO examined selected aspects of the program's operation, including the (1) factors that affect CBP's ability to target shipments at foreign seaports, (2) extent to which high−risk containers have actually been inspected overseas, and (3) extent to which CBP formulated and documented strategies for achieving the program's goals. GAO recommends that CBP refine its staffing model to help improve the program's ability to target shipments at foreign ports, develop minimum technical requirements for the detection capabilities of equipment used in the program, and complete development of performance measures for all program objectives. The Department of Homeland Security (DHS) generally concurred with these recommendations and described corrective actions to respond to them. The Department of State had no comments.
Highlights: http://www.gao.gov/highlights/d05557high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−557

9. *March 11, Government Accountability Office* — **GAO−05−404: Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security (Report).** This report is a publicly available version of our report on the Customs−Trade Partnership Against Terrorism (C−TPAT). The Department of Homeland Security (DHS) designated our original report as Limited Official Use because of the sensitive and specific nature of the information it contained. U.S. Customs and Border Protection (CBP) has implemented a layered approach to achieve its goals of (1) preventing terrorists and terrorist weapons from entering the United States and (2) facilitating the flow of legitimate trade and travel. One element of this approach is C−TPAT, which aims to secure the flow of goods bound for the United States by developing a strong, voluntary antiterrorism partnership with the trade community. The Government Accountability Office (GAO) examined (1) what benefits are provided to C−TPAT members, (2) how CBP determines eligibility for these benefits, (3) what process CBP uses to verify that members have implemented security measures, and (4) how well CBP manages C−TPAT. GAO recommends that CBP eliminate the weaknesses in its validation process. GAO also recommends that CBP complete its human capital plan and performance measures and put in place internal controls for the program. CBP generally concurred with these recommendations and described corrective actions to respond to them.
Highlights: http://www.gao.gov/highlights/d05404high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−404

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *May 25, Associated Press* — **Citrus canker found in Polk, Florida.** Citrus canker has been found in a grove across the street from where the disease was first discovered the week of May 16 in Polk County, the area of Florida with the most citrus trees. Agriculture officials said Tuesday, May 24, the canker was found in a grove across the street from a nursery owned by Ben Hill Griffin Inc., where the canker was first found in Polk County. The disease also was found in two groves owned by Ben Hill Griffin, one of the state's largest growers. An estimated 5,000 trees will be destroyed in the Ben Hill Griffin groves in an effort to restrict the spread of the disease, which causes fruit to drop and can cut a tree's production by half. The canker in the new grove appears to be older than canker found in the Ben Hill Griffin nursery, indicating that the disease spread from the grove to the nursery, said Denise Feiber, a spokesperson for the Florida Department of Agriculture. State protocol requires that all trees, even healthy ones, must be destroyed within 1,900 feet of an infected tree. Polk County has an estimated 11.6 million citrus trees.
Source: http://www.sun−sentinel.com/news/local/florida/sfl−fcanker25may25,0,1223650.story?coll=sfla−news−florida

11. *May 24, Animal and Plant Health Inspection Service* — **Time period for interstate movement of cattle from certain bovine tuberculosis zones.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Tuesday, May 24, announced that it is amending its bovine tuberculosis (TB) regulations to reduce the amount of time between testing a herd for the disease and moving the herd interstate from six months to 60 days. Current regulations permit the interstate movement of cattle and bison from a modified accredited or accreditation preparatory state within six months after the entire herd has been tested for TB. APHIS has determined that this six month period is too long especially when considering the potential exposure of cattle in these states to TB infected wildlife. This interim rule will lower the potential risk of movement of infected animals and decrease the likelihood of TB transmission. Bovine TB is a contagious, infectious, and communicable disease caused by Mycobacterium bovis. It affects cattle, bison, deer, elk, goats, and other species, and can be fatal. APHIS classifies each state according to its level of occurrence of bovine TB.
Source: http://www.aphis.usda.gov/lpa/news/2005/05/bovinetb_vs.html

12. *May 24, U.S. Department of Agriculture* — **USDA closes border to cattle from Durango, Mexico.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Tuesday, May 24, announced that USDA's Animal and Plant Health Inspection Service (APHIS) has closed the U.S. border to cattle from the Mexican state of Durango due to inadequacies with that state's bovine tuberculosis (TB) management program. Durango is essentially divided into two sections for the purposes of exporting cattle to the U.S. with one section allowed to export and one that is not. During a review of Durango's TB management practices, APHIS found that animals from the section not allowed to export were being moved into the region that is allowed to export. This, combined with other conflicts with APHIS guidelines, led to the border closing. In order to resume trade, Durango must meet all APHIS guidelines, including the recommendations by the APHIS review team, such as: prohibiting the movement of dairy heifers from herds in the known infected region into the exporting region; requiring quarantine and tests of animals in any heifer raising operation in the exporting region that has received cattle from dairy herds in the known infected region; and requiring quarantine and tests for herds along Durango's internal regional border if one or more animal in the herd has tested positive.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/05/0180.xml

13. *May 24, Agricultural Research Service* — **Compost teas may help flowers battle blight.** Compost teas may prove helpful in protecting wholesale and retail nursery plants like rhododendrons, azaleas, viburnums, and oak saplings from what's known as ramorum blight, also called ramorum die−back or sudden oak death. That's according to Agricultural Research Service (ARS) plant pathologist Robert G. Linderman. The funguslike organism, Phytophthora ramorum, which causes these diseases, has been found in at least 20 states. To prevent spread of P. ramorum, more than one−half million otherwise−ready−to−sell plants have had to be destroyed. In a preliminary experiment, Linderman and colleagues treated rhododendron leaves indoors with a helpful bacterium, Paenibacillus polymyxa, taken from compost. The researchers then inoculated the leaves with the ramorum organism. The scientists found that P. polymyxa did not protect the foliage, but they plan to test it again −− and other potentially protective microbes −− using slightly different procedures. Compost teas are made from compost

"brewed" for at least 24 hours with all−natural ingredients that boost growth of beneficial microbes living in the compost.
Source: http://www.ars.usda.gov/is/pr/2005/050524.htm

14. *May 17, Government Accountability Office* — **GAO−05−668R: USDA's Preparation for Asian Soybean Rust.** Congress asked the Government Accountability Office (GAO) to determine the U.S. Department of Agriculture's (USDA) efforts to develop and implement an Asian soybean rust (ASR) surveillance strategy to identify and protect against ASR's entry into the U.S. and to test and verify suspect cases; USDA's strategy for minimizing the effects of ASR; and the progress that USDA, EPA, and others have made in developing, testing, and licensing fungicides to treat ASR and in identifying and breeding ASR−resistant or −tolerant soybeans. Since the initial discovery of ASR in the U.S., USDA and others have increased efforts to inform growers about how to identify and minimize the effects of the disease. In April 2005, USDA issued A Coordinated Framework for Soybean Rust Surveillance, Reporting, Prediction, Management, and Outreach. The framework includes a surveillance and monitoring network, a Web−based information management system, decision criteria for fungicide application, predictive modeling, and outreach efforts. GAO surveyed 31 states to obtain information about their efforts, in coordination with USDA, to prepare for and manage ASR. The states generally responded positively when discussing efforts to educate growers and others on ASR and in setting up sentinel plot monitoring programs. However, some of the states reported that their diagnostic laboratories may have insufficient funding and/or staff to test suspected samples for ASR. In addition, most states indicated that they were either uncertain or did not believe they would have enough equipment available to apply fungicides to treat the disease.
Source: http://www.gao.gov/new.items/d05668r.pdf

[Return to top]

Food Sector

15. *May 25, Associated Press* — **Salmonella strikes at least 71 at buffet.** At least 71 diners who ate Thursday, May 19, at the buffet−style Old South Restaurant in Camden, SC, may have become ill with salmonella, health officials say. At least 16 of those who became ill had been hospitalized by Monday, May 23, Department of Health and Environmental Control (DHEC) spokesperson Missy Reese said. It could take weeks for DHEC to determine the source of the salmonella at the restaurant, Reese said. The bacteria usually comes from undercooked poultry products and causes nausea, vomiting, diarrhea, and fever, health officials said. Inspectors gave the restaurant an "A" grade during an inspection Monday, May 23. It had the same grade Thursday, May 19, and DHEC had not reported any other problems at the restaurant, Reese said.
Source: http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/ local/11731587.htm

16. *May 25, Reuters* — **Tainted biotech maize impounded at Irish port.** A U.S. consignment of genetically modified corn gluten feed tainted with an illegal strain has been impounded upon arrival at an Irish port, the European Commission said on Wednesday, May 25. The feed was contaminated with the banned Bt−10, a genetically modified (GMO) maize made by Swiss agrochemicals group Syngenta. The shipment was tested in the U.S. and the positive results for

Bt−10 were sent to Ireland to allow Dublin to stop the cargo on arrival. In April 2005, the European Union (EU) blocked imports of maize from the U.S. unless shipments carried proof that they were free of Bt−10, which is not authorized for use either in Europe or the U.S. The curb will be reviewed at the end of October but the EU's food safety chief said last month the conditional ban may be extended if contaminated products were discovered. Syngenta said the impounding of the maize shipment in Ireland showed that the testing system for Bt−10 was working.
Source: http://abcnews.go.com/US/wireStory?id=789912

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *May 25, Associated Press* — **Rodent virus now linked to six deaths.** Health officials are asking doctors to watch for unusual illnesses in organ transplant and blood transfusion patients now that at least six deaths have been linked to a virus carried by hamsters and mice. The recent discoveries that rabies and West Nile virus could spread through donated organs has officials worried that the rodent virus might have done so undetected before now. "We don't know how commonly it occurs," said Matthew Kuehnert, assistant director of blood safety for the U.S. Centers for Disease Control and Prevention. Rhode Island and Massachusetts officials said Monday, May 23, they are investigating the deaths of three people who got infected organs from a female donor whose pet hamster tested positive for lymphocytic choriomeningitis virus (LCMV). A fourth organ recipient is recovering. On Tuesday, May 24, health officials in Wisconsin revealed that four transplant recipients died in the only previously known cases involving the virus in December 2003. The cases weren't clear−cut −− the organ donor and a woman who received a lung from him in an operation in Minnesota both tested negative for LCMV. But three other transplant patients tested positive for the virus, strongly suggesting the donor was the source.
Source: http://www.fortwayne.com/mld/journalgazette/11728158.htm

18. *May 25, Reuters* — **Interpol says world should prepare for bioterrorism.** Bioterrorism is a credible threat which authorities worldwide have underestimated, Interpol warned on Wednesday, May 25. Interpol says the world is largely unprepared for the possibility of attacks with crude biological agents that militant groups have developed a heightened interest in. "We, as police, cannot afford to be unprepared for the eventual use of biological agents by terrorist groups," Interpol president Jackie Selebi told a regional conference in Cyprus. Al Qaeda manuals on preparation of biological agents were discovered at the group's training camps in Afghanistan after the U.S. invasion in 2001. In April 2005, a British court jailed a man with suspected links to al Qaeda on charges of plotting bomb or poison attacks in London. Police believed the poison that would have been deployed was ricin, extracted from castor beans and fatal even in doses of less than a milligram. In March 2005, a U.S. presidential commission

suggested al Qaeda had made advances in developing a virulent biological warfare agent they called Agent X. The commission also said U.S. intelligence had long believed that al Qaeda had trained its members in producing toxins obtained from venomous animals and botulinum, a toxin more commonly known for its association with improperly canned food.
Source: http://abcnews.go.com/US/wireStory?id=789225

19. *May 24, Hillsboro Argus (OR)* — **Hantavirus confirmed in Oregon.** A rare case of hantavirus pulmonary syndrome has been confirmed in a Washington County, OR, resident, public health officials in the state Department of Human Services (DHS) said. This is the Oregon's sixth reported case of hantavirus. Five cases were reported between 1993 and 1997. Rodents such as deer mice or wild mice may carry hantavirus and excrete the virus in urine, droppings, and saliva. People can be infected by inhaling concentrated virus particles that become airborne when rodent droppings or nests are disturbed. Since hantavirus was first identified in 1993, a total of 379 laboratory−confirmed cases have been reported in the U.S., including 32 retrospectively identified cases that occurred before 1993.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.oregonlive.com/news/argus/index.ssf?/base/news/1116970229165550.xml&coll=6

20. *May 24, Reuters* — **Polio spreads in Yemen, Indonesia.** A polio outbreak raging through Yemen has paralyzed 108 children and the number of confirmed cases in Indonesia has risen to 14, the World Health Organization (WHO) said on Tuesday, May 24. Mass vaccination campaigns are being conducted next week in both countries, where the virus reappeared in April 2005 for the first time in a decade, according to the WHO. Earlier this month Yemen reported 83 cases while Indonesia had eight. The viral disease of the brain and spinal cord, which mainly affects children under five, can cause irreversible paralysis in a matter of hours. Some cases are fatal. The WHO, which is campaigning to halt the spread of polio by the end of the year, has battled setbacks in the last two years since Nigeria's Muslim state of Kano banned immunization. Vaccinations resumed after a 10−month ban. But the virus spread across Africa, crossed the Red Sea into Saudi Arabia and Yemen, and reached Indonesia −− infecting 16 previously polio−free countries in all.
Source: http://www.alertnet.org/thenews/newsdesk/L24693482.htm

21. *May 24, National Institute of Allergy and Infectious Diseases* — **Scientists observe infectious prions invade and move within brain cells.** Scientists from the National Institute of Allergy and Infectious Diseases (NIAID) for the first time have watched agents of brain−wasting diseases, called transmissible spongiform encephalopathies (TSE), as they invade a nerve cell and then travel along wire−like circuits to points of contact with other cells. These findings will help scientists better understand TSE diseases and may lead to ways to prevent or minimize their effects. TSE, or prion, diseases include scrapie in sheep and goats; chronic wasting disease in deer and elk; mad cow disease in cattle; and Creutzfeldt−Jacob disease in humans. Prions branded with a fluorescent dye (pink) were added to nerve cells taken from a hamster brain. The prions initially were in the form of large clumps on the cell, but over time the clumps were broken into smaller units and transported along wire−like nerve cell projections. Prions branded with a fluorescent dye (red) were added to nerve cells taken from mice. The prions initially were in the form of large clumps on the cell, but over time the clumps were broken into smaller units and transported along wire−like nerve cell projections.

Source: http://www2.niaid.nih.gov/newsroom/Releases/prion_move.htm

[Return to top]

Government Sector

22. *April 25, Government Accountability Office* — **GAO−05−420: Electronic Government: Funding of the Office of Management and Budget's Initiatives (Report).** In accordance with the President's Management Agenda, the Office of Management and Budget (OMB) has sponsored initiatives to promote electronic government— the use of information technology, such as Web−based Internet applications, to enhance government services. Generally, these "e−gov" initiatives do not have direct appropriations but depend on a variety of funding sources, including monetary contributions from participating agencies. The Government Accountability Office (GAO) was asked to review the funding of e−gov initiatives that relied on such contributions: specifically, to determine, for fiscal years 2003 and 2004, whether agencies made contributions in the amounts planned and to determine the timing of these contributions. What GAO Recommends In order to avoid errors and to better assist managing partner agencies in obtaining funds to execute e−gov initiatives, GAO recommends that OMB ensure that it correctly reflects the funding plans of each initiative in its budget guidance to partner agencies. In commenting on a draft of this report, officials from OMB's Office of Electronic Government generally agreed with its content and the recommendation.
Highlights: http://www.gao.gov/highlights/d05420high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−420

[Return to top]

Emergency Services Sector

23. *May 25, Lincoln County News (ME)* — **Emergency drill goes smoothly.** Threatening skies provided a somber backdrop for a large−scale emergency response drill in Damariscotta, ME, on Saturday, May 21. The drill involved a scenario designed to stretch local resources to their limits. One of the drill's designers, Lincoln County Emergency Management Agency director Tim Pellerin, said he was extremely pleased with the findings produced by the exercise. As designed, the exercise involved a disgruntled customer attacking the local water utility. The disgruntled customer detonated a radioactive device, a "dirty bomb" contaminating himself, the water supply, and three children on bicycles who just happened to be in the area. More than 11 separate agencies participated including Lincoln County EMA, the Sheriff,s Office, Damariscotta Police, Maine State Environmental Protection Agency, Great Salt Bay Sanitary District and fire departments from Bristol, Newcastle, and Damariscotta. Pellerin said that inter−agency communication went well but it could be improved upon. However, emergency radios the county purchased with federal funds last year worked perfectly, he said.
Source: http://www.mainelincolncountynews.com/index.cfm?ID=12068

24. *May 25, Associated Press* — **Hundreds participate in nuclear emergency drill.** Local, state and federal officials converged on Windham County, VT, for an emergency drill involving two mock earthquakes at the Vermont Yankee nuclear plant near Battleboro, VT. It was a biennial

graded exercise in which the Federal Emergency Management Agency (FEMA) will review the activities of officials who would respond to a real emergency. FEMA will reveal its findings at a meeting in Brattleboro on June 2. Duncan Higgins, deputy director of state Division of Emergency Management, reported that hundreds of state and local officials covered their emergency posts, with 70 responding at the division's headquarters in Waterbury alone. Vermont Yankee spokesperson Robert Williams said the emergency drill was triggered by two mock earthquakes near the plant. He said a general emergency −− the most severe of four classes of emergencies at a nuclear plant −− was declared shortly after noon, and that the drill envisioned a release of radioactivity into the environment. Each of the five Vermont towns within the emergency−planning zone around Vermont Yankee −− Vernon, Brattleboro, Dummerston, Guilford and Halifax −− staffed its emergency operations center. State officials staffed an incident field office in Dummerston, while state and Vermont Yankee officials staffed a media center in Brattleboro, holding mock press briefings.
Source: http://www.fosters.com/apps/pbcs.dll/article?AID=/20050525/N EWS0103/105250018

[Return to top]

Information Technology and Telecommunications Sector

25. *May 25, SecurityFocus* — **Computer Associates Vet library remote heap overflow vulnerability.** Computer Associates Vet is susceptible to a remote heap overflow vulnerability. This is due to an integer overflow flaw in memory allocation and utilization routines. This vulnerability allows remote attackers to overwrite critical heap memory control structures. This results in the ability to cause arbitrary machine code to be executed in the context of applications that utilize the affected library. Advisory and updates available at: http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=328 96
Source: http://www.securityfocus.com/bid/13710/solution/

26. *May 25, Associated Press* — **Montana leaves private information on outdated computers.** Montana state agencies failed to remove private information before retiring outdated state computers, risking public disclosure of Social Security and credit card numbers, medical records and income taxes, a new report disclosed. The legislative audit, obtained Tuesday, May 24, blamed unclear state policy for the computer hard drives not being properly "scrubbed" before the machines were donated to school districts, given to other state agencies or sold to the public. Janet Kelly, Department of Administration director, said in a written response that her agency immediately began crafting a more concise policy to ensure private information held by the government is not made public. Jeff Brandt, acting chief information officer for the state, said the new policy should be complete by mid−July. Brandt said the information discovered by the auditor's office was never divulged, so the people to whom it pertains need not be concerned. However, he acknowledged the state has no way of knowing if other data on other computers discarded by the state was disclosed over the years as the machines changed hands.
Montana Legislative Audit Division: http://leg.state.mt.us/css/audit/default.asp
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05 /25/AR2005052500975.html

27. *May 24, SecurityTracker* — **Ipswitch IMail Server multiple vulnerabilities.** A remote user can view arbitrary files on the target system and can execute arbitrary code with system

privileges. A remote authenticated user can cause the IMAP service to crash. The server does not properly process user supplied requests for nonexistent JSP files. A remote user can send a special HTTP request to view files on the target system with system level privileges. Advisory and updates available at: http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html
Source: http://www.securitytracker.com/alerts/2005/May/1014047.html

28. *May 24, SecurityTracker* — **Cisco ACNS can be crashed with specially crafted compressed DNS data.** A vulnerability was reported in Cisco CNS in the processing of DNS messages. A remote user can cause denial of service conditions. A remote user can send a DNS packet with specially crafted message compression data to cause an error on the target system. The target device may function abnormally or crash. The vendor fix matrix is available at: http://www.cisco.com/warp/public/707/cisco−sn−20050524−dns.s html
Source: http://securitytracker.com/alerts/2005/May/1014046.html

29. *May 24, Reuters* — **FBI aims to launch new computer system by 2006.** The FBI has designed a new computer system to replace a failed $170 million one aimed at helping agents share information but it will not be ready for use until the end of 2006, the FBI director said on Tuesday, May 25. The need for the system was identified after the September 11, 2001, attacks on the United States, when investigators found deficiencies in the sharing and recording of information by U.S. agencies. FBI Director Robert Mueller told a Senate Appropriations subcommittee the FBI had designed a new electronic information management system called Sentinel. The bureau expected the first phase to be deployed by the end of next year.
Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2005−05−24T212709Z_01_N24318273_RTRIDST_0_TECH−SECURITY−FBI−DC.XML

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 reports that a new variant of the Sober worm family, Sober.P may spread by virtue of its offer of free World Cup tickets. The payload of this variant is unknown and it may be another form of spam, like Sober.q. Sober.P has a hidden the source code making it more malicious and may cause a denial−of−service attack. Sober.p creates a time stamp like key, then uses that to generate a URL to a server on one of five different hosting services operating in Germany and Austria.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 1026 (−−−), 1027 (icq), 1433 (ms−sql−s), 1434 (ms−sql−m), 139 (netbios−ssn),

	15118 (dipnet [trojan]), 1025 (−−−), 1028 (−−−) 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

30. *May 26, U.S. Department of State* — **U.S. Embassy in Jakarta closed.** The U.S. Embassy and the U.S. Consulate General wish to inform all American citizens in Indonesia that the Embassy, Consulate General, and all other U.S. Government facilities in Indonesia will be closed beginning May 26, 2005 until further notice because of a security threat. Consular officers are available in Jakarta and Surabaya to provide emergency assistance to U.S. citizens even though U.S. Government facilities are closed to the public. The Embassy reminds all Americans that the terrorist threat in Indonesia remains high. Attacks could occur at any time and could be directed against any location, including those frequented by foreigners and identifiably American and other western facilities or businesses in Indonesia.
Source: http://www.usembassyjakarta.org/news/warden052605.html

[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