Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 22 March 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- Reuters reports Internet phone services are attracting identity thieves looking to turn stolen credit cards into cash; the scams underline the lower level of security protecting Voice Over Internet Protocol. (See item 8)
- The Associated Press reports Union Pacific Corp. and the Texas state government have agreed to work toward moving freight rails out of Texas' urban areas to try to reduce accidents and keep hazardous materials out of major cities. (See item 10)
- Federal Computer Week reports Florida agencies seek federal funding to complete the statewide rollout of the Florida Integrated Network for Data Exchange and Retrieval, that law enforcement officials say could be the basis for a national information sharing strategy. (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://esisac.com]

1. *March 21, Reuters* — **Nuclear energy may be back in vogue.** Expectations of a sharp rise in energy demand and the risk of climate change are pushing many countries to return to the idea of nuclear power, the head of the United Nations nuclear watchdog said Monday, March 21. Even the most conservative estimates predict at least a doubling of energy usage by

mid−century, Mohamed ElBaradei, director general of the International Atomic Energy Agency (IAEA), told a conference on nuclear energy in the 21st century. He said any discussion of the energy sector "must begin by acknowledging the expected substantial growth in energy demand in the coming decades." It was unclear what role nuclear power would play, though it appeared to be an increasingly important one, he said. "All indicators show that an increased level of emphasis on subjects such as fast growing energy demands, security of energy supply, and the risk of climate change are driving a reconsideration, in some quarters, of the need for greater investment in nuclear power," ElBaradei said. Conference: http://www−pub.iaea.org/MTCD/Meetings/Announcements.asp?Conf ID=122
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050321/sc_nm/energy_nuclear_dc_2

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *March 18, KITV (HI)* — **Ammonia leak forces warehouse evacuation.** A potentially dangerous ammonia leak Friday, March 18, forced the evacuation of a grocery distribution warehouse at Campbell Industrial Park in Honolulu, HI, and the Honolulu Fire Department's hazardous materials teams were called into action. Four employees complained of dizziness and nausea. Two went to a hospital for observation. All 35 employees were evacuated from the building as Hazmat crews tested the air quality. Officials determined it was a small ammonia leak from a coil in the cold storage unit inside the company's large warehouse.
Source: http://www.msnbc.msn.com/id/7235232/

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *March 21, The Arizona Republic* — **Drug addicts making Arizona city a hotbed for counterfeiting.** Metropolitan Phoenix, AZ, is emerging as a national hot spot for counterfeit money thanks to the area's burgeoning population of methamphetamine addicts and access to advanced printing technology. Ken Huffer, special agent in charge of the Secret Service in Arizona, said counterfeit currency is showing up with regularity at nightclubs, convenience stores and restaurants. Huffer said 78 percent of counterfeit bills passed in Arizona are produced on modern office machinery −− inkjet printers, photocopiers, laser printers −− rather than offset printing presses. Nationally, the ratio is nearly reversed: just 13 percent of the nation's fake currency is manufactured on office equipment, which means Arizona has spawned a new brand of counterfeiter who produces just enough bad bills to pay for a motel room and support a drug habit. The methamphetamine phenomenon is reflected in another dubious distinction: last year, Arizona led the nation in identity theft per capita, largely because of the

state's drug addict population.
Source: http://www.azcentral.com/arizonarepublic/news/articles/0321c ounterfeit21.html

4. *March 21, Yale Daily News (CT)* — **Phishing scheme targets students.** Some Yale Univeristy students recently were tricked by a Website that looked just like one from Yale. On Monday, March 14, some users received an e−mail directing them to a duplicated or "spoofed" version of the Yale Central Authentication System login Website where they were prompted to enter their NetIDs and passwords, Chief Information Officer Philip Long said. The spoof was the most advanced phishing scheme to invade University e−mail servers, he said. Now, new anti−spam software will be introduced on Yale e−mail servers. Although 28 phony messages were received by users before the hoax was reported and blocked, Long said the damage was minimal. Still, he said both the quantity and quality of such phishing scams are on the rise. Long said the spoof was considered particularly dangerous because it was the first such duplication of a Yale Website he had seen, and implied knowledge of the University's network systems. "This clearly used knowledge of Yale and was sent to individuals at Yale, so we take this as a higher concern than just general issues of phishing," Long said, adding that the spoof originated off campus.
Source: http://www.yaledailynews.com/article.asp?AID=28785

5. *March 21, ComputerWeekly* — **Businesses warned of e−terror threat.** The world is likely to face a major cyber terrorism attack within the next two years, David Lacey, director of security at the Royal Mail Group (UK) warned at a conference on business continuity recently. Lacey said developments in network technology, coupled with the growth of organized crime, pointed to a major global incident by 2006. Lacey said the risks faced by businesses would peak over the next year as key technologies start to mature. The replacement of traditional telecoms with voice over IP would leave organizations more vulnerable to electronic attack, as both voice and data run on the same networks, Lacey warned. In addition, he said the increasing connectivity of organizations would provide hackers with new routes to attack organizations. Conference Website: http://www.businesscontinuityexpo.com/
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=137426&liArticleTypeID=1&liCategoryID=6&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

6. *March 21, eWeek* — **New phishing attacks offer cash.** A new kind of phishing attack made its debut over the weekend, and experts say this is the first time that online scammers have offered cash to entice recipients into responding to their ploys. The new e−mail is designed to look like a solicitation from Citizens Bank. The message asks recipients to complete an online survey, and in return, recipients will supposedly get $5 credited to their accounts. However, in order to receive the credit, each user must enter his ATM card number and PIN, something that no legitimate bank mailing would ever require. Experts who have seen the messages and analyzed the code behind them say that the scam is being hosted by ISPs in England and the Netherlands. This attack is one of the few times that phishers have strayed from their tried−and−true method of trying to scare recipients into falling for their scams with messages saying that users' accounts have been compromised or need to be updated to avoid cancellation. Offering a cash incentive for responding to a message takes the scams to an entirely new level, and experts predict that such attacks will likely meet with tremendous success.
Source: http://www.eweek.com/article2/0,1759,1777928,00.asp

7. *March 20, United News of Bangladesh* — **Symposium focuses on terrorist financing.** Terrorists receive financing from charitable organizations throughout the world, according to leaders from Asia and the U.S. who discussed terrorist financing and money laundering at a symposium in New York. Sponsored by the U.S. State Department, the symposium was organized by an investigations and security firm. International delegates expressed concern that the U.S. is too focused on al Qaeda and groups directly linked to al Qaeda, noting that the Tamil Tigers of Sri Lanka and the Maoist insurgents in Nepal as two groups of concern. Panelists discussed that a greater sharing of information is imperative and is necessary for better understanding of the constantly changing and innovative methods of terrorists. The use of charitable organizations as a vehicle for laundering money to terrorists has become a major problem. Delegates were told that individuals and businesses need to be more vigilant in scrutinizing exactly to whom they are donating.
   Source: http://www.bangladesh−web.com/news/view.php?hidDate=2005−03−20&hidType=LOC&hidRecord=00000000000000000038162

8. *March 18, Reuters* — **Internet phones possibly an identity theft risk.** Internet phone services have drawn millions of users looking for rock−bottom rates. Now they're also attracting identity thieves looking to turn stolen credit cards into cash. Some Internet phone services allow scam artists to make it appear that they are calling from another phone number −− a useful trick that enables them to drain credit accounts and pose as banks or other trusted authorities, online fraud experts say. The emerging scams underline the lower level of security protecting Voice Over Internet Protocol, or VOIP. Traditional phone networks operate over dedicated equipment that is difficult for outsiders to penetrate. Because VOIP calls travel over the Internet, they are vulnerable to the same security problems that plague e−mail and the Web. Criminals can use caller−ID spoofing to make it appear that they are calling from a bank or other financial institution, said Dave Jevans, who chairs the Anti−Phishing Working Group, a banking industry task force. That helps them convince consumers to divulge account numbers, passwords and other sensitive information in a scam that echoes the "phishing" e−mails that have become common, he said.
   Source: http://money.cnn.com/2005/03/18/technology/personaltech/scam_phones.reut/index.htm?cnn=yes

[Return to top]

Transportation Sector

9. *March 21, Associated Press* — **Officials investigating death of man who was restrained on airliner.** Prosecutors are investigating the death of a man who was subdued by several fellow airline passengers after he became disruptive on a New York−bound flight. William Lee was pronounced dead late Friday, March 18, after he was removed from the American Airlines flight at Kennedy International Airport. The cause of death had not yet been determined and was under investigation. Lee, 48, of New York, stood up in his seat on American's Flight 4 from Los Angeles and "loudly demanded another beer," airline spokesperson Tim Smith said. Flight attendants asked him to wait until they reached his row, Smith said, but the man "got very, very belligerent and loud and disruptive and was told he would not be served any more alcohol." Seven male passengers restrained Lee, who was a very large man, and they and the

flight crew put flexible handcuffs on him and put him back in his seat, Smith said. Lee got out of his seat again and the seven passengers held him on his back on the galley floor until the plane landed, Smith said. After the landing, New York Port Authority police boarded the plane and administered CPR to Lee, who "was in some kind of distress," Smith said.
Source: http://www.usatoday.com/travel/news/2005−03−21−passenger−dea th_x.htm

10. *March 21, Associated Press* — **Railroad agrees to move freight lines.** Union Pacific Corp. and Texas have agreed to work toward moving freight rails out of Texas' urban areas to try to reduce accidents and keep hazardous materials out of major cities, Governor Rick Perry announced Friday, March 18. Moving the rails could also open up space for new roads and speed deliveries because trains wouldn't have to slow down while passing through congested areas, Perry said. Dick Davidson, chief executive officer of the Omaha, NE−based railroad, called the agreement a blueprint for an expensive and probably long process. Union Pacific spokesperson John Bromley said bypassing a city the size of Houston is unrealistic and that bridges and tunnels might be used there instead. Since 1984, more than 5,500 people have been killed or injured in vehicle−train collisions in Texas, Perry's office said. Last month, about 200 San Marcos residents had to be evacuated after the derailment of a Union Pacific train carrying sulfuric acid. And late last year, federal regulators added 10 inspectors in San Antonio after six train accidents in the area left four dead and released toxic chemicals.
Source: http://biz.yahoo.com/ap/050318/rail_safety_1.html

11. *March 21, Associated Press* — **Port security a major concern on Gulf Coast.** U.S. ports are still trying to achieve compliance with the Maritime Transportation Security Act (MTSA) of 2002's new standards for waterside surveillance, cargo screening, personnel improvements and regional planning. Meanwhile, lawmakers, ports and the Department of Homeland Security (DHS) are debating whether there is enough funding to cover every shoreline and how best to determine the danger to each individual port. "We share the concerns about the way this (new) program's been proposed," said Mark McAndrews, director of the Port of Pascagoula, MS. McAndrews said his port, which ranked 23rd in the nation for cargo volume in 2003, has received nearly $800,000 from DHS since the grant program began. That has been enough, he added, to cover the cost of compliance with the MTSA. As for the new security standards DHS continues to issue, "we'll address those as they emerge. We have upgraded our security personnel, let me just put it that way." Officials have agreed a port's size, the type of cargo it handles and special features such as the military training base that adjoins the Port of Pascagoula are all deemed crucial. But small container ports −− such as Gulfport −− are not, even though cargo containers are considered an ideal target for terrorists. MTSA Website: http://www.uscg.mil/hq/g−m/mp/mtsa.shtml
Source: http://www.securityinfowatch.com/article/article.jsp?id=3416 &siteSection=306

12. *March 21, Dayton Business Journal (OH)* — **Comair, flight attendants reach tentative deal.** Comair Inc., which flies out of Ohio's Dayton International Airport, and its flight attendants' union have reached a tentative agreement to reduce labor costs for the airline. The airline and the International Brotherhood of Teamsters, which represents about 1,000 flight attendants, jointly issued a memo to Comair flight attendants on March 18. The memo stated that the proposed agreement "would modify the flight attendant working agreement and help the airline achieve cost reductions, protect job security and bid for growth aircraft." The union will conduct meetings with its members on March 22, March 24 and March 28 so that flight

attendants can review the proposed agreement's details. The company also has resumed negotiations with the mechanics union −− the International Association of Machinists and Aerospace Workers. Those talks are progressing. Comair is a wholly owned subsidiary of Atlanta−based Delta Air Lines, which is the largest airline flying out of Dayton International Airport.
Source: http://dayton.bizjournals.com/dayton/stories/2005/03/21/dail y4.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *March 21, Agri News* — **Brazil project could help detect soybean rust.** Early detection of soybean rust is difficult. Its symptoms can easily be confused with other soybean diseases. And farmers now must physically get in their fields, sometimes on their hands and knees, to scout their plants for infection. They have to review possibly hundreds of plants, conducting such intensive scouting at least twice a week. But new technology now being developed in Brazil could make detecting soybean rust much easier. Brazilian researchers are working on tools to help growers determine when conditions are favorable for soybean rust. Their “Projecto Radar,” which now is being tested on about 40 farms across Brazil, uses a weather station that monitors leaf wetness, temperature, humidity, and rainfall. Measurements are collected in a data logger attached to the monitors and later are downloaded from the loggers to a computer. Similar technology now is being developed in the U.S., where University of California scientists are creating equipment to monitor the probability of grape powdery mildew in vineyards. In Brazil, researchers are fine−tuning their risk index for soybean rust, determining at which level farmers should apply a fungicide.
Source: http://www.agrinewspubs.com/Main.asp?SectionID=1&SubSectionID=207&ArticleID=8278

14. *March 18, Animal and Plant Health Inspection Service* — **Animal disease exercise.** The Animal and Plant Health Inspection Service on March 21−23 will participate in Equinox 2005, an emergency response exercise based on a hypothetical foot–and–mouth disease (FMD) outbreak in North America. Equinox 2005 is part of an ongoing series of FMD exercises of the North American Animal Health Committee—an Emergency Management Working Group (EMWG) made up of the U.S., Canada, and Mexico. The intent of the North American exercise program is to provide realistic training on FMD emergency response plans, to practice the executions, and to evaluate the results. The objectives for Equinox 2005, the third series of North American exercises, will focus on U.S. and Canadian border operations in response to an FMD outbreak and international coordination among the affected states, provinces, and federal governments. The exercise will include practicing activation of the existing communications plan, as well as the North American Foot and Mouth Disease Vaccine Bank. Equinox 2005 involves emergency management facilities and state veterinarians located in Maine, Vermont,

and New Hampshire, and at several locations within Quebec and New Brunswick, Canada.
Source: http://www.aphis.usda.gov/lpa/news/2005/03/equinox_vs.html

[Return to top]

Food Sector

15. *March 18, U.S. Department of Agriculture* — **USDA announces funding to improve food safety.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Friday, March 18, announced that almost two million dollars in funding has been redirected to enhance research on bovine spongiform encephalopathy (BSE) and that five million dollars has been awarded to establish a Food Safety Research and Response Network. The BSE research funds will be used for new BSE projects. The newly funded projects include international collaborations with the Veterinary Laboratory Agency in Great Britain to study the biology of the BSE agent, the Italian BSE Reference Laboratory to evaluate present diagnostic tools for detecting atypical BSE cases, and the University of Santiago de Compostela in Spain to compare North American and European BSE strains. The Food Safety Research and Response Network will include a team of more than 50 food safety experts from 18 universities who will investigate several of the most prevalent food−related illness pathogens. Pathogens like E.coli and Salmonella will be studied to determine where they are found in the environment, how they are sustained, and how they infect herds. The group also will serve as a response team that can be mobilized to conduct focused research to control major episodes of food−related illnesses −− to include investigation of health problems associated with agricultural bioterrorism.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/03/0097.xml

16. *March 18, Food and Drug Administration* — **Sandwiches recalled in the Midwest.** Eastside Deli Supply Inc. is voluntarily recalling all of its “Eastside Deli,” “Fresh from the Deli” and “In Your Belly Deli” labeled products as a precautionary measure because of the previous recall on its “Beef and Cheese Sub” due to the presence of Listeria monocytogenes found during routine sampling in February. None of these sandwiches have been shown to be contaminated at this time. The recalled sandwiches were distributed to convenience stores in parts of Michigan, Ohio, and Indiana. No illnesses have been reported to date in connection with any of these sandwiches. Listeria monocytogenes is an uncommon organism which can cause serious and sometimes fatal infections.
Source: http://www.fda.gov/oc/po/firmrecalls/eastsidedeli03_05.html

17. *March 18, Food and Drug Administration* — **Delicatessen product recall expanded.** E.A. Sween Company announced Friday, March 18, that it is expanding its voluntary recall of Deli Express Turkey & Cheese Sandwiches, as they have the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections. As a precautionary measure, E.A. Sween Company is also withdrawing the following products; Deli Style Stacker, Turkey & Cheese, Ham & Swiss on Rye, Ham & Cheese White, Turkey Club, Classic Ham & Cheese Sub, Classic Italian Sub, Grilled Ham & Cheese, and Chopped Ham & Cheese Sub. These sandwiches were distributed in select convenience stores and vending machines nationwide.
Source: http://www.fda.gov/oc/po/firmrecalls/sween03_05.html

18. *March 18, Ohio State University* — **Choice of dairy cow bedding impacts E. coli survival, food safety.** Ohio State University researcher Jeff LeJeune has found a direct relationship between the bedding material used in dairy operations and the survival of E. coli O157:H7. LeJeune tested cattle for E. coli O157:H7 on farms that spread either sand or sawdust in stalls. A total of 3,600 fecal samples from 20 commercial Ohio farms −− 10 using sand and 10 using sawdust −− were gathered and analyzed. Results show the prevalence of E. coli O157:H7 in animals from sand−bedded herds (1.4 percent) is significantly lower than in animals from sawdust−bedded herds (3.1 percent). The total number of positive samples in sand−bedded animals (25 out of 1,800) was less than half that found in sawdust−bedded animals (56 out 1,800). LeJeune's study is the first to explore the connection between bedding and E. coli O157:H7 from a food−safety perspective. Cattle manure is considered the primary source of E. coli O157:H7 contamination in foods and the environment. "Approximately 17 percent of ground beef comes from dairy cows that go to slaughter," LeJeune said. "One cow contaminated with E. coli O157:H7 that has been sent to the slaughterhouse can contaminate many other cows, and this can result in the contamination of millions of pounds of ground beef."
Source: http://www.ag.ohio−state.edu/~news/story.php?id=3071

[Return to top]

Water Sector

19. *March 22, Times Reporter (OH)* — **Hazmat team called after diesel fuel spill.** About 500 gallons of diesel fuel drained into Postboy Creek in Newcomerstown, OH, Sunday, March 20, after a pickup truck hit three diesel storage tanks, causing them to rupture. As of Sunday night, fuel was still was emptying into the creek, according to Jeff Shreiner, a Dover firefighter and team coordinator for Tuscarawas County Hazardous Materials Team. The fuel soaked into the ground and into a drainpipe into the creek, Shreiner said. Six Hazmat team members and ten Newcomerstown firefighters deployed containment equipment in eight areas of a one−mile stretch of the creek, he said. Shreiner said the current in the creek was very strong in places, and the fuel was floating on top of the water. He noted that all of the appropriate agencies were notified, including the Environmental Protection Agency, Ohio Department of Natural Resources and the Emergency Management Agency.
Source: http://www.timesreporter.com/left.php?ID=39633&r=0

20. *March 21, Associated Press* — **Barge runs aground in Washington state spilling diesel fuel.** on Saturday, March 19, a barge containing as much as 5,000 gallons of diesel fuel broke free of a tugboat and ran aground near Cape Disappointment State Park in Washington state, an area rich with wildlife, razor clam beds, waterfowl areas and historic landmarks. The tugboat was pulling two barges across the Columbia River in severe weather, when one broke free, drifted three miles, and ran aground, according to state ecology and Coast Guard officials. Two environmental cleanup companies were at the scene by early Monday but were unable to deploy containment booms because of high wind and waves, said Sandy Howard, a spokesperson for the state Ecology Department. Cargo holds of the oil barge Millicoma were empty, but there was diesel fuel in a double−hulled 5,000−gallon fuel tank. No injuries were reported. The cause of the accident was under investigation.

Source: http://news4colorado.com/nationalnews/BargeAground−aa/resour ces_news_html

[Return to top]

Public Health Sector

21. *March 21, Pharma Live* — **Trinity Biotech completes acquisition of Research Diagnostics.** Trinity Biotech, of Ireland, Monday, March 21, announced that it has completed the acquisition of Research Diagnostics Inc. (RDI), of Flanders, NJ. Trinity Biotech has acquired the business of RDI for $4.2 million in cash. RDI provides a comprehensive range of immunodiagnostic products to research facilities, pharmaceutical companies, reference laboratories, diagnostic manufacturers, and universities worldwide. The range of products provided by RDI is similar to that provided by Fitzgeralds, a company which Trinity acquired in April 2004. Specifically the range includes monoclonal and polyclonal antibodies, antigens, proteins, enzymes, and immunochemicals employed in the areas of cancer, cardiac, and infectious disease diagnosis. The operations of RDI will be integrated with those of Fitzgeralds and the combined entity will operate on a stand−alone basis within the Trinity group. Trinity Biotech develops, acquires, manufactures, and markets diagnostic products for the clinical laboratory and point−of−care segments of the diagnostic market. The line of over 500 test kits are used to detect infectious diseases, sexually transmitted diseases, and autoimmune diseases. Trinity is also a significant provider of raw materials to the life science industry. Trinity Biotech sells worldwide in 78 countries through its own salesforce and a network of international distributors and strategic partners.
Source: http://www.medadnews.com/News/Index.cfm?articleid=222574

22. *March 21, Canadian Press* — **Superbug endangers Canadian patients' lives.** An antibiotic−resistant superbug −− Methicillin−resistant Staphylococcus aureus (MRSA) −− has been ravaging Quebec, Canada, hospitals. In 2004 at least 5000 people were infected and 800 had serious lung or blood infections due to the bacteria. The bacteria kills one out of three patients. Over the past five years, MRSA, has progressed rapidly and is now found in almost all regions of the province and most large hospitals. MRSA is transmitted by human contact. More information about MRSA is available from the U.S. Centers for Disease Control and Prevention: http://www.cdc.gov/ncidod/hip/Aresist/ca_mrsa_public.htm
Source: http://www.canada.com/ottawa/ottawacitizen/news/story.html?id=224df1d9−5e08−405b−aff9−96a24a765074

23. *March 21, Thanh Nien News (Vietnam)* — **Vietnam province unaware of bird flu outbreak until media report.** Authorities in Vietnamese province Quang Binh became aware of a serious bird flu outbreak only after media recently uncovered a bird flu death and hundreds of suspected cases in one of the province's communes. Provincial authorities learned of the outbreak after Thanh Nien newspaper carried a news report on Sunday, March 20, saying that 195 people in Chau Hoa commune had symptoms of the bird flu. In addition, two children in the commune fell ill and were taken to a hospital in Dong Hoi town in March. The 13−year−old girl died at the hospital on March 9, testing positive for bird flu, according to health authorities. However, the Dong Hoi hospital never reported the case to provincial leaders. Local residents said families in the Chau Hoa commune continued to eat dead chickens throughout the Lunar New Year, while poultry in the rest of the country was being culled and destroyed. Tests are

being carried out with all 195 suspected patients to determine whether they are infected with bird flu. More information about avian influenza is available from the U.S. Centers for Disease Control and Prevention: http://www.cdc.gov/flu/avian/
Source: http://www.thanhniennews.com/healthy/?catid=8&newsid=5682

24. *March 17, University of Wisconsin* — **Harnessing microbes.** Taking a new approach to the painstaking assembly of nanometer−sized machines, a team of scientists at the University of Wisconsin−Madison has successfully used single bacterial cells to make tiny bio−electronic circuits. The work is important because it has the potential to make building the atomic−scale machines of the nanotechnologist far easier. It also may be the basis for a new class of biological sensors capable of near−instantaneous detection of dangerous biological agents such as anthrax. The approach suggests that microbes can serve as forms for complicated nanoscale structures, perhaps obviating, in part, the need for the time−consuming construction of devices at the smallest scale. "One of the great challenges of nanotechnology remains the assembly of nanoscale objects into more complex systems," says Robert Hamers, the senior author of the new reports. "We think that bacteria and other small biological systems can be used as templates for fabricating even more complex systems." Toward that end, Hamers and his colleagues developed a system in which living microbes are guided down a channel to a pair of electrodes barely a germ's length apart. Slipping between the electrodes, the microbes, in effect, become electrical "junctions," giving researchers the ability to capture, interrogate, and release bacterial cells one by one.
Source: http://www.news.wisc.edu/releases/10831.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

25. *March 21, The Patriot−News (PA)* — **Trainees learn water rescue skills.** Fifty−nine students wearing aquatic suits, life vests and helmets assembled near the Dock Street Dam in Harrisburg, PA, Sunday, March 20, to practice the fundamentals of river rescue. They came from around the state −− and some from New York and New Jersey −− to earn Phase I certification, which covers moving water, cold water and shore−based techniques. The drill was the culmination of a three−day course created by the Pennsylvania Fish and Boat Commission and taught by the water safety and training division of LifeTeam River Rescue, an all−volunteer organization that responds to emergencies in the Harrisburg area. The students watched as two professionals in a yellow inflatable boat paddled against the current to rescue a spare tire that swirled near the 4 1/2−foot dam, which resembled a shallow waterfall. Later, half the group dropped into a fetal position in the river to experience being adrift in cold, moving water. Their classmates and trainers tossed them throwbags−−bags containing floating rope−−to reel them back to shore, where a LifeTeam Emergency Services Crew waited with an ambulance.
LifeTeam River Rescue: http://www.lifeteamriverrescue.org/wc05/wc05.html

Source: http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/1111400470287630.xml

26. *March 21, The Yuma Sun (AZ)* — **Fire departments use many tools to get to calls quickly.** In an effort to improve speed to the call, Yuma Fire Department (YFD) in Yuma, AZ, has made numerous improvements to ensure that they always know where they are going. One change was the installation of mobile data computers (MCDs) on all fire engines, rescue vehicles and battalion chief trucks. These computers give firefighters information to help them make the right decisions on getting to an emergency. To speed response, the entire city is broken up into one−quarter square mile sections, called grids. Captain Gene Tutell said that as road construction can make things difficult, firefighters try to stay informed about where the detours are in the city. In addition, it is important to keep up with new development. YFD stays in constant contact with the city's Department of Community Development and attends their meetings. When new construction is done, the Rural/Metro Ambulance and Fire Department in the suburban and urban areas receives information from the developers, said Chief Patrick Foley. Also, firefighters will go out and survey the development, so it can be added to the books. He said these surveys are done on a continuous basis.
Source: http://sun.yumasun.com/artman/publish/articles/story_15511.p hp

27. *March 20, The Sentinel (PA)* — **Counter−Terrorism Task Force hosts conference.** Being ready for a terrorist strike or natural disaster was the theme of a three−day conference last week at Harrisburg Area Community College in Pennsylvania. More than 300 representatives from police, fire and emergency services agencies as well as hospitals and critical businesses, industries and public utilities across an eight−county region attended the three−day session held to offer training and networking opportunities. Ted Wise, chairman of the South Central Pennsylvania Counter−Terrorism Task Force, said training and the opportunity to exchange information among disaster responders were two main facets of the conference. Conference seminar topics covered a range of issues from al Qaeda training, tactics and targeting to operating a dispatch center during a terrorist incident. Businesses and industries can play two vital roles in counter−terrorism by promoting public awareness and protecting their own facilities, said Wise. Participants from these groups included representatives of Three Mile Island's nuclear power plant in Harrisburg, electric companies, telecommunications industries, food supply chains and agribusiness. Wise said agriculture, electric and water lines and computer networks are considered vulnerable targets and could themselves be vital to emergency response. South Central Pennsylvania Counter−Terrorism Task Force: http://www.scpacttf.org/scpacttf/site/default.asp?scpacttfNa v=|
Source: http://www.cumberlink.com/articles/2005/03/20/news/news11.tx t

28. *March 20, The Oshkosh Northwestern (WI)* — **Citizen Corps program develops in Wisconsin county.** When the next emergency arises, planning and training that’s happening right now could prove invaluable, said Jon Lee, emergency services coordinator for the Oshkosh, WI, American Red Cross chapter. As part of Winnebago County’s homeland security plan, local law enforcement agencies, emergency personnel and a number of local agencies are working together in developing the Winnebago County Citizen Corps program. The effort is meant provide better coordination between all groups involved in emergency response, from neighborhood watch groups to police and fire departments to organizations like the Red Cross. Components of the program would allow everyday residents to get training in emergency

response. The Corps will also establish a medical reserve comprised of retired medical personnel who would become available in times of need. Residents trained in emergency response will be a tremendous asset to agencies stretched thin in the event of tornadoes, large fires or other large−scale responses. Winnebago County Citizen Corps: http://www.co.winnebago.wi.us/sheriff/USA%20Freedom%20Corps. htm
Source: http://www.wisinfo.com/northwestern/news/local/stories/local_20233058.shtml

29. *March 20, The Free Press (NC)* — **North Carolina county conducts emergency training exercise.** On Saturday, March 19, a man drove a truck containing a cylinder of hazardous chemicals into the EMS building in La Grange, NC. There were several people in the building at the time, and they were taken hostage by the armed driver. Two were shot, and a number suffered eye, skin and respiratory damage from chemical leakage before law enforcement officials freed the hostages and killed the gunman. The training exercise for Lenoir County law enforcement officers, rescue squads, firefighters and hospital personnel was geared to test how well various emergency responders would react to such a hazardous chemical emergency. Funding for the drill and training, about $15,000, came from the Department of Homeland Security. Roger Dail, Lenoir County's emergency services director, said that what the emergency responders learned during the drill will be incorporated into a countywide response plan. All those participating in the four−hour drill, from EMTs and firefighters, to hazardous waste responders, police officers, hospital personnel, Boy Scouts, and county SWAT team members, reacted to the event as if it was real.
Source: http://www.kinston.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=26374&Section=Local

30. *March 19, Southern Maryland Online* — **Emergency preparedness drill in Maryland scheduled for April.** The Charles County Department of Emergency Services, the Charles County Sheriff's Office, local volunteer fire and rescue departments, Civista Medical Center, the Washington, DC National Guard, the Maryland Institute for Emergency Medical Services Systems, and other state and local emergency response agencies, in cooperation with the St. Charles Towne Center, will conduct an emergency preparedness exercise on Sunday, April 3, at the Regional Mall in Waldorf, MD. The mall and surrounding grounds will be closed to the public during this time. A portion of the St. Charles Towne Plaza, across the street from the mall, will be used as a staging area for the exercise. Additional information: http://www.charlescounty.org/es/company_exercise_drill_form. pdf
Source: http://somd.com/news/headlines/articles/1791.shtml

[Return to top]

Information Technology and Telecommunications Sector

31. *March 21, USA TODAY* — **Cyberattacks on corporate networks rising, surveys show.** Cyberintruders have stepped up their attacks on corporate computer networks, according to two surveys released Monday, March 21. Symantec, the world's largest supplier of anti−virus software, reports a 332% spike in worms and viruses launched against Windows desktop computers and servers in the last half of 2004 compared with the year before — 7,360 variants in all. Also, in a January survey of 229 midsize and large companies, security firm Mazu Networks found 47% had networks compromised by a self−propagating worm in the past year.

Companies set up perimeter firewalls as a first defense. So intruders have begun probing the pathways corporations keep open to communicate one−on−one with employees, customers and suppliers. Areas ripe for intrusion are Web applications set up to share, create or modify data and Web tools such as instant messaging services and desktop tools to do Web searches and locate files. Tech managers are responding by banning some free tools and wireless devices. Report highlights: http://www.symantec.com/press/2005/n050321.html and http://www.mazunetworks.com/news/press_releases/article/inde x.php?id=45
Source: http://www.usatoday.com/tech/news/2005−03−20−it−attack−usat_x.htm

32. *March 19, New York Times* — **Growth of wireless Internet opens new path for thieves.** Federal and state law enforcement officials say sophisticated criminals have begun to use the unsecured Wi−Fi networks of unsuspecting consumers and businesses to help cover their tracks in cyberspace. Law enforcement officials warn that such connections are being commandeered for child pornography, fraud, death threats and identity and credit card theft. More than 10 million homes in the United States now have a Wi−Fi base station providing a wireless Internet connection, according to ABI, a technology research firm. Experts say most of those households never turn on any of the features, available in almost all Wi−Fi routers, that change the system's default settings, conceal the connection from others and encrypt the data sent over it. Failure to secure the network in those ways can allow anyone with a Wi−Fi−enabled computer within about 200 feet to tap into the base station's Internet connection. Wi−Fi connections in retail and university locations are also often left unsecured. Holly L. Hubert, the supervisory special agent in charge of the Cyber Task Force at the FBI field office in Buffalo, said the use of Wi−Fi was making it much more difficult to track down online criminals.
Source: http://www.nytimes.com/2005/03/19/technology/19wifi.html

33. *March 18, K−Otik Security* — **J2SE Java Web Start client−side argument injection vulnerability.** A critical vulnerability was identified in Java Web Start, which may allow an untrusted application the ability to elevate its privileges. The flaw resides in the Java Web Start launcher ("javaws.exe" for Windows and "javaws" for Solaris and Linux) when handling a specially crafted "property" tag in a "JNLP" file, which may be exploited, via a specially crafted web page, to bypass the default "sandbox" security policy and read/write arbitrary files on a vulnerable system. Solutions available at:
http://sunsolve.sun.com/search/document.do?assetkey=1−26−577 40−1
Source: http://www.k−otik.com/english/advisories/2005/0282

34. *March 18, SecurityTracker* — **CoolForum input validation flaws permit SQL injection and cross−site scripting attacks.** Several input validation vulnerabilities were reported in CoolForum. A remote user can conduct cross−site scripting attacks and inject SQL commands. Multiple scripts do not properly validate user−supplied data. The vendor has released a fixed version (0.8.1), available at: http://www.coolforum.net/index.php?p=dlcoolforum
Source: http://www.securitytracker.com/alerts/2005/Mar/1013474.html

35. *March 18, New York Times* — **Study criticizes government on cybersecurity research.** A report released Friday, March 18, by a panel of computer experts criticizes the federal government, saying that its financing of research on computer network security is inadequate and that it is making a mistake by focusing on classified research that is inaccessible to the commercial sector. The report, commissioned by the Bush administration, calls for the

government to spend $148 million annually on Internet security research through the National Science Foundation, over the current $58 million. It also urges more research spending by the Pentagon's Defense Advanced Research Projects Agency, or Darpa, and by the Department of Homeland Security. The report, "Cybersecurity: A Crisis of Prioritization," was prepared by a subcommittee of the President's Information Technology Advisory Committee (PITAC), a group of industry and university experts. Research in Internet security is needed to protect systems that run the government and military operations, as well as other areas, including the electric power grid, the air traffic control grid and financial systems, the report said. Report: http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cyb ersecurity.pdf
Source: http://www.nytimes.com/2005/03/19/technology/19computer.html

36. *March 18, Federal Computer Week* — **Florida police agencies share data.** Florida agencies want federal funding to complete the statewide rollout of a network that local law enforcement officials say could be the basis for a national information sharing strategy. Development of the Florida Integrated Network for Data Exchange and Retrieval (FINDER) began in August 2002 with the goal of providing all 355 law enforcement agencies in the state a way to share critical information in hundreds of different police databases. Twenty−three agencies are sharing information over the network and another 22 have signed a memorandum of understanding as a prelude to participating, said Lt. Mike McKinley, a member of the Orange County Sheriff's Office and chairman of the executive committee of Florida Law Enforcement Data Sharing Consortium (FLEDSC). Without FINDER, police officers now have to make separate phone calls to other police agencies to check for information about suspects or such things as vehicle details, McKinley said. It's impossible for anyone to query every agency in the state with that method, he added. The University of Central Florida, co−developer of FINDER, has estimated combined savings through sharing over FINDER could add up to as much as $10 million a year.
Source: http://www.fcw.com/article88341−03−18−05−Web

37. *March 18, ZDNet (United Kingdom)* — **Virus writers changing focus.** Security researchers have warned that sudden impact viruses, such as the Slammer worm, which cause immediate widespread damage to IT systems are being superseded by slow−burning worms where the focus is on avoiding detection. According to F−Secure, virus writers are putting more time into making their viruses stealthy in an attempt to sneak them past antivirus software. Malware authors, many of whom now use viruses as a way of making money, are regularly testing their viruses against antivirus packages, said Mikko Hyppönen, director of antivirus research for F−Secure. Hyppönen said that no one has seen a really hard−hitting worm since May last year and believes this is because virus writers have changed their approach. Many new viruses attempt to install key loggers that can record passwords and personal details, according to Hyppönen, so by attracting less attention the viruses should be more successful.
Source: http://news.zdnet.co.uk/internet/security/0,39020375,3919184 0,00.htm

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

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

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 22321 (wnn6_Tw), 53 (domain), 80 (www), 113 (auth), 1025 (−−−), 1026 (−−−), 7674 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website:

http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer