



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 18 March 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- TechWeb News reports more than 100,000 alumni of Boston College in Massachusetts are being informed that a computer hacker broke into a computer containing their addresses and Social Security numbers. (See item [8](#))
- The Associated Press reports the Federal Aviation Administration issued an advisory saying pilots have been straying from their flight paths on takeoff from New Jersey's Teterboro Airport, causing a potential threat in a very busy airspace. (See item [15](#))
- The Washington Post reports the recent anthrax scare at the Pentagon exposed gaps between the military's procedures in handling biohazards and those of the rest of the federal government, which could increase the threat to public health in the event of an actual contamination. (See item [23](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [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. *March 17, The Register (UK)* — **Power plants need anti-virus protection.** Utility companies are being urged to review cyber security risks as the industry moves over from proprietary technologies to cheaper Windows-based systems. Attendees at an Industrial Cyber Security Conference in London on Tuesday, March 15, were told that the control systems of utilities are

becoming open to the kinds of attacks that bedevil corporate systems, such as computer worms and Distributed Denial of Service attacks, as power and water companies embrace the net. Supervisory Control And Data Acquisition (SCADA) systems lie at the heart of systems that control water, sewage and electricity systems. These devices allow utilities to remotely control and monitor generation equipment and substations over phone lines, radio links and, increasingly, IP networks. Gary Sevounts, director of industry solutions for Symantec, said these systems had been disconnected for decades but this is changing as utilities connect their control systems to corporate networks. "The problem is that IT people don't understand SCADA and SCADA people don't understand security," he said. Interconnection between SCADA environments and corporate networks introduce specific security needs around protocols and applications used that are not addressed by the majority of existing cyber security products, and power systems have different requirements in terms of reliability and availability to corporate systems. Conference: <http://www.emea.symantec.com/icseventuk/>
Source: http://www.theregister.co.uk/2005/03/17/industrial_cyber-security/

2. **March 16, Government Accountability Office — GAO-05-414T: Meeting Energy Demand in the 21st Century: Many Challenges and Key Questions (Testimony).** Plentiful, relatively inexpensive energy has been the backbone of much of modern America's economic prosperity and the activities that essentially define our way of life. The energy systems that have made this possible, however, are showing increasing signs of strain and instability, and the consequences of our energy choices on the natural environment are becoming more apparent. As a nation, we have witnessed profound growth in the use of energy over the past 50 years — nearly tripling our energy use in that time. Although the United States accounts for only five percent of the world's population, we now consume about 25 percent of the energy used each year worldwide. Looking into the future, the Energy Information Administration estimates that U.S. energy demand could increase by about another 30 percent over the next 20 years. To aid the subcommittee as it evaluates U.S. energy policies, Government Accountability Office (GAO) agreed to provide its views on energy supplies and energy demand as well as observations that have emerged from its energy work. Highlights:
<http://www.gao.gov/highlights/d05414thigh.pdf>
Source: <http://www.gao.gov/new.items/d05414t.pdf>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

3. **March 17, Houston Chronicle (TX) — Carbon monoxide fumes sicken dozens of dollar-store shoppers.** At least 48 people were treated at area hospitals Thursday, March 17, for exposure to dangerous levels of carbon monoxide after becoming ill at a Family Dollar Store in southwest Houston, TX. The problem was reported about 9:50 a.m., and firefighters arrived at the scene to find people complaining of headaches, nausea and vomiting, a Houston Fire Department official said. Fire officials said carbon monoxide levels were measured at 129 parts per million (ppm) when firefighters and paramedics arrived, and within 30 minutes levels were measured at 400 ppm. Fifty ppm is considered dangerous.
Source: <http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/3089994>

[\[Return to top\]](#)

Defense Industrial Base Sector

4. *March 16, Government Accountability Office* — **GAO-05-428T: Defense Acquisitions: Future Combat Systems Challenges and Prospects for Success (Testimony)**. Future Combat Systems (FCS) is the core of Army efforts to create a lighter, more agile, capable force: a \$108 billion investment to provide a new generation of 18 manned and unmanned ground vehicles, air vehicles, sensors, and munitions linked by an information network. Although system development and demonstration began in May 2003, the program was restructured in July 2004, including processes to make FCS capabilities available to current forces. Government Accountability Office (GAO) has been asked to assess (1) FCS technical and managerial challenges; (2) prospects for delivering FCS within cost and scheduled objectives; and (3) options for proceeding. Highlights: <http://www.gao.gov/highlights/d05428thigh.pdf>
Source: <http://www.gao.gov/new.items/d05428t.pdf>

5. *March 15, Government Accountability Office* — **GAO-05-304: Tactical Aircraft: Air Force Still Needs Business Case to Support F/A-22 Quantities and Increased Capabilities (Report)**. The Air Force is preparing a modernization plan that expands the capabilities of the F/A-22, which was first designed to serve as an air-to-air fighter aircraft with very limited ability to strike targets on the ground. The Air Force now intends to transform it by adding robust air-to-ground capabilities to attack enemy ground threats and by adding onboard intelligence data gathering capabilities. It has been in development for more than 19 years, a decade longer than originally envisioned. In the face of significant cost and schedule overruns, Congress mandates that Government Accountability Office (GAO) annually assess the F/A-22 program. In this report, GAO addresses (1) the Air Force's business case for the F/A-22 modernization plan and (2) the recently completed initial operational test and evaluation. GAO is reiterating and expanding upon a 2004 recommendation that DoD complete a new and comprehensive business case that reflects the current budget environment and justifies future investments and specific quantities needed to meet mission requirements. DoD concurred and expects to build a business case through such actions as the 2005 Quadrennial Defense Review and analysis required to support future modernization efforts as a separate program. Highlights: <http://www.gao.gov/highlights/d05304high.pdf>
Source: <http://www.gao.gov/new.items/d05304.pdf>

[\[Return to top\]](#)

Banking and Finance Sector

6. *March 17, Chico Enterprise-Record (CA)* — **Chico State computer system attacked by hackers**. More than 59,000 people connected to Chico State University in Chico, CA, will be contacted for what officials are calling the largest computer hacking incident the college has seen. Notifications to anyone whose personal information was compromised were going out Tuesday, March 15, said Joe Wills, director of public affairs at the university. That list includes current and former Chico State faculty and staff members. However, the majority of those receiving notifications are students, because the server hackers targeted held the names and Social Security numbers of current, former and prospective students. The university was made

aware of the incident about three weeks ago, after routine monitoring of its network showed that hackers illegally accessed the University Housing and Food Service server. An investigation revealed hackers installed software to store files and attempted to break into other computers.

Source: <http://www.chicoer.com/Stories/0,1413,135~25088~2765075,00.h tml>

- 7. *March 17, Ananova* — Attempted bank theft by hacking.** According to evidence, criminals used hacking methods to try and steal US\$423 million from Sumitomo bank in London. The gang used devices known as key-loggers, which allowed them to track every button pressed on the bank's computer keyboards. From that they could learn account numbers, passwords and other sensitive information. Steve Purdham, CEO of Web security company SurfControl, said, "The attempted theft depended on a type of spyware — otherwise known as 'key-logging' software — to track the passwords of Sumitomo personnel and enable the fraudsters to access secure areas of the network and to begin the process of distributing funds to a number of bank accounts around the world." It is not known whether they broke into the bank to install the hacking software or did it via the Internet. The plan was to transfer the cash electronically to 10 bank accounts around the world.

Source: http://www.ananova.com/business/story/sm_1322966.html?menu=b usiness.latestheadlines

- 8. *March 17, TechWeb News* — Boston College alumni records may have been hacked.** More than 100,000 alumni of Boston College in Massachusetts are being informed that a computer hacker broke into a computer containing their addresses and Social Security numbers. While college officials said they believe the hacker may not have been attempting to retrieve personal information — the hacker was probably planting a program to launch invasions of other computers — they decided to take no chances and inform alumni of the violation. The breached computer was operated by an outside contractor unnamed by the university.

Source: <http://www.techweb.com/wire/security/159901496>

- 9. *March 16, Associated Press* — Auditors find IRS employees vulnerable to hackers posing as information technology employees.** More than one-third of Internal Revenue Service (IRS) employees and managers who were contacted by Department of Treasury inspectors posing as computer technicians provided their computer login and changed their password, a government report said Wednesday, March 16. The report by the Treasury Department's inspector general for tax administration reveals a human flaw in the security system that protects taxpayer data. The auditors called 100 IRS employees and managers, portraying themselves as personnel from the information technology help desk trying to correct a network problem. They asked the employees to provide their network logon name and temporarily change their password to one they suggested. "We were able to convince 35 managers and employees to provide us their username and change their password," the report said. "With an employee's user account name and password, a hacker could gain access to that employee's access privileges," the report said. "Even more significant, a disgruntled employee could use the same social engineering tactics and obtain another employee's username and password," auditors said.

Source: Report: http://www.treas.gov/tigta/auditreports/2005reports/20052004_2fr.pdf

- 10. *March 16, Government Accountability Office* — GAO-05-223: Credit Reporting Literacy: Consumers Understood the Basics but Could Benefit from Targeted Educational Efforts**

(Report). This report responds to a mandate in the Fair and Accurate Credit Transactions Act (FACT Act) of 2003 requiring Government Accountability Office (GAO) to assess consumers' understanding of credit reporting. The FACT Act, among other things, extended provisions governing the credit reporting system and addressed ongoing concerns about inaccuracies in credit reports. For example, the act expanded access to credit information by entitling consumers to one free credit report each year. It also established the Financial Literacy and Education Commission (FLEC) to improve consumers' understanding of credit issues. This report examines consumers' understanding and use of credit reports and scores and the dispute process and looks at factors that may influence their understanding of credit reporting. GAO recommends that (1) the Secretary of Treasury, as Chairman of FLEC, working with its members, take steps to improve consumers' understanding of their rights and remedies under the FACT Act, targeting the population groups that would most benefit; and (2) the Chairman of the Federal Trade Commission, take steps to improve consumers' understanding of how credit reports and scores are used, their right to dispute inaccurate information, and how consumers' credit behavior could affect their credit history. Both agencies generally agreed with the findings. Highlights: <http://www.gao.gov/highlights/d05223high.pdf>
Source: <http://www.gao.gov/new.items/d05223.pdf>

[\[Return to top\]](#)

Transportation Sector

11. *March 17, Honolulu Advertiser (HI)* — Two years of thefts suspected at Honolulu Airport.

A Transportation Security Administration (TSA) official said on Wednesday, March 16, that federal agencies are investigating whether four federal airport screeners stole money and valuables from luggage at Honolulu International Airport over a two-year period. The TSA screeners have been suspended indefinitely, said Nico Melendez, a TSA spokesperson in San Francisco. U.S. Attorney Ed Kubo said federal authorities are continuing to investigate allegations that several Transportation Security Administration workers stole items from luggage at the airport. He said people have been questioned, but there have been no arrests and no charges have been filed. "I can confirm an investigation is ongoing into several TSA employees concerning the theft of items from luggage," Kubo said. He said it's believed that the luggage belonged to Japanese visitors, but that has not been confirmed. The investigation is being handled by the TSA's law enforcement arm, as well as special agents from the Department of Homeland Security Inspector General's Office, Kubo said. "This (the theft allegations) was brought to light by TSA screeners," TSA's Melendez said. "This re-emphasizes the need for passengers to keep valuables in their carry-on (luggage) or on their person."

Source: http://the.honoluluadvertiser.com/article/2005/Mar/17/ln/ln0_3p.html

12. *March 17, Department of Transportation* — Department of Transportation seeks research proposals from small business. The U.S. Department of Transportation (DOT) on Thursday, March 17, announced that it will make available \$3.5 million in funding for innovative research that will help to enhance the safety and efficiency of the U.S. transportation system, and asked small businesses to submit their project ideas. The Small Business Innovation Research (SBIR) program encourages small business to engage in research and development activities that have the potential to produce commercially viable applications as well as meet federal research

objectives. The program is administered by the Volpe National Transportation Systems Center, a part of DOT's newly created Research and Innovative Technology Administration (RITA). Proposals from U.S.-owned businesses of no more than 500 employees are due by May 16, 2005. Research awards will be made in October. Solicitation materials can be downloaded online from <http://www.volpe.dot.gov/sbir/sol05/download.html>. The goals of DOT's SBIR program are to build a stronger economic base for the United States through invigorating the small business technology community; and to assure that technologies that develop out of this unique program will focus on safer, simpler transportation solutions.

Source: <http://www.dot.gov/affairs/rita0105.htm>

13. *March 17, Government Accountability Office* — GAO-05-364T: Coast Guard:

Observations on Agency Priorities in Fiscal Year 2006 Budget Request (Testimony). The Government Accountability Office (GAO) has conducted reviews of many of the Coast Guard's programs in recent years, and this testimony synthesizes the results of these reviews as they pertain to three priority areas in the Coast Guard's budget: (1) implementing a maritime strategy for homeland security, (2) enhancing performance across missions, and (3) recapitalizing the Coast Guard, especially the Deepwater program—an acquisition that involves replacing or upgrading cutters and aircraft that are capable of performing missions far out at sea. GAO's observations are aimed at highlighting potential areas for ongoing congressional attention. The Deepwater program, which would receive \$966 million under the budget request, appears to merit the most ongoing attention. GAO reviews of this program have shown that the Coast Guard clearly needs new or upgraded assets, but the Coast Guard's contracting approach carries a number of inherent risks that, left unaddressed, could lead to spiraling costs and slipped schedules. The Coast Guard is taking some action in this regard, but GAO continues to regard this approach as carrying substantial risk. Some expansion of cost and slippage in schedule has already occurred. Highlights: <http://www.gao.gov/highlights/d05364thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-364T>

14. *March 17, Government Accountability Office* — GAO-05-440T: Homeland Security:

Performance of Foreign Student and Exchange Visitor Information System Continues to Improve, but Issues Remain (Testimony). The Student and Exchange Visitor Information System (SEVIS) is an Internet-based system run by the Department of Homeland Security (DHS) to collect and record information on foreign students, exchange visitors, and their dependents—before they enter the United States, when they enter, and during their stay. The Government Accountability Office (GAO) has reported (that although the system had a number of performance problems during the first year that its use was required, several SEVIS performance indicators were positive at that time (June 2004). Nonetheless, some problems were still being reported by educational organizations. In addition, concerns have been raised that the number of international students and exchange visitors coming to the United States has been negatively affected by the U.S. visa process. Accordingly, the Congress asked GAO to testify on its work on SEVIS and related issues. This testimony is based on its June 2004 report, augmented by more recent GAO work, reports that was issued in February 2004 and 2005 on student and visiting scholar visa processing, and related recent research by others. Highlights:

<http://www.gao.gov/highlights/d05440thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-440T>

15.

March 17, Associated Press — **FAA: too many pilots at Teterboro straying from flight paths.** Federal officials have advised pilots who use New Jersey's Teterboro Airport to make sure they take off at the proper altitude to help avoid the possibility of midair collisions with jets headed to Newark Liberty International Airport. The Federal Aviation Administration (FAA) issued the advisory in an e-mail sent to 155,000 pilots and others on Friday, saying too many pilots have been straying from their flight paths on takeoff. The FAA sets altitude requirements and other flight procedures to ensure that departing and arriving jets in the region maintain at least 1,000 feet of vertical distance and three miles of lateral distance between them. "The issue is, we have very busy airspace in New York and New Jersey," said Arlene Murray, an FAA spokesperson. "Pilots were going above the altitude that is set for that departure procedure." Incidents the FAA calls "pilot deviations" have happened three times in the past three months and twice in 2004. Pasquale DiFulco, a spokesperson for the Port Authority of New York and New Jersey, which operates the commercial airports in the New York area, said the agency is "supportive of any measure that will enhance increased safety in the skies."
Source: <http://www.wnbc.com/news/4293341/detail.html>

[\[Return to top\]](#)

Postal and Shipping Sector

16. *March 17, WCSH (ME)* — **Postal officials warn of money order scam.** The U.S. Postal Service is warning about a scam hitting Maine where con artists, often from foreign countries, e-mail Mainers asking them to cash a postal money order, claiming they can't cash it where they live. So far, nine Mainers from communities across the state have been detained after agreeing to cash the money orders.
Source: <http://www.wcsh6.com/home/article.asp?id=21013>

[\[Return to top\]](#)

Agriculture Sector

17. *March 17, Agricultural Research Service* — **New mobile lab to help contain exotic pests.** A new U.S. Department of Agriculture (USDA) mobile biocontainment laboratory that will allow scientists to work more safely with invasive species and other agricultural threats was unveiled Thursday, March 17, at the U.S. Horticultural Research Laboratory (USHRL). "This mobile unit will allow USDA's Agricultural Research Service (ARS) and Animal and Plant Health Inspection Service (APHIS) to continue cooperative efforts to protect American agriculture from a variety of pests and diseases," said ARS Administrator Edward B. Knipping. The innovative greenhouse lab was designed and developed by ARS plant pathologist Timothy R. Gottwald at USHRL, in collaboration with APHIS plant pathologist Paul E. Parker, director of the Mission Plant Protection Center in Mission, TX. The 48-foot-long lab has a computer-controlled greenhouse and laboratory that are sealed off from the outside. Built on a trailer-type chassis, the lab can be moved to different locations as needed.
Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

18.

March 16, Southeast Farm Press — **Meteorologist plans soybean rust forecasts.** Thomas Keever saw the telltale signs of trouble on his computer a month before it hit. A trajectory traveling northwards out of the Caribbean, curving toward the southeast picking up microscopic spores on the backside of winds from Hurricane Ivan that eventually brought Asian soybean rust to the U.S. From March through October he will provide thrice-weekly forecasts regarding the threat of soybean rust in the U.S. in 2005. The forecast gives growers and others in the industry a 24 to 72 hour heads-up regarding rust infestations. As the meteorologist at the North American Plant Disease Forecast Center on the campus of North Carolina State University in Raleigh, NC, Keever brings together information from a myriad of sources over the Internet to write forecasts in next-to-real time about the what, when, and the risk to an disease epidemic in the North American Hemisphere. The Center got its start in the summer of 1995 thanks to an outbreak of blue mold in burley tobacco in the mountains of North Carolina. Keever has been working on soybean rust with various state and federal agencies for at least two years. The forecasts are listed on the Web at <http://www.ces.ncsu.edu/edu/depts/pp/soybeanrust/>
Source: <http://southeastfarmpress.com/news/031605-rust-forecasts/>

19. *March 16, Associated Press* — **Damaging alien snail found in Georgia.** A voracious, fast-breeding South American snail that is a problem in four states and Indonesia has been discovered for the first time in Georgia, officials say. The single snail was found along the Alabama River in southeastern Georgia's Pierce County last month, wildlife officials said. It was identified as a channeled apple snail, similar to those raising environmental concerns in at least nine Florida counties. The large snails ravage many types of aquatic plants that provide food and shelter for native species. They can multiply quickly because they lay thousands of eggs and have no natural enemies. Georgia Department of Natural Resources biologists believe the snail found near Blackshear could have been dumped from an aquarium.
Source: <http://abcnews.go.com/Technology/wireStory?id=586004>

[\[Return to top\]](#)

Food Sector

20. *March 17, Agence France Presse* — **Rare form of food poisoning in Hong Kong.** Seven more people have been hit with a rare form of food poisoning after eating contaminated scallops, taking the number of reported cases to 31. The victims all suffered symptoms of phycotoxin poisoning, complaining of dizziness, blurred vision, aching limbs and cramps after eating contaminated seafood bought from market stalls across Hong Kong. Hong Kong Chamber of Seafood Merchants chairman Lee Choi-wah told media that traders believed the poisoned scallops had been imported from Vietnam.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=1&u=/afp/20050317/hl_afp/healthhongkongseafood_05031711_5922
21. *March 16, Food Safety and Inspection Service* — **Chicken dumplings recalled.** Day-Lee Foods, Inc., a Santa Fe Springs, CA, firm, is voluntarily recalling approximately 12,090 pounds of chicken dumplings that may be contaminated with *Listeria monocytogenes*, the Food Safety and Inspection Service (FSIS) announced Wednesday, March 16. The chicken dumplings were distributed to a wholesaler in North Carolina. The problem was discovered through company sampling. FSIS has received no reports of illnesses associated with consumption of these

products. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease.

Source: http://www.fsis.usda.gov/News_&_Events/Recall_010_2005_Release/index.asp

22. *March 16, Indiana State Department of Health* — **Indiana State Department of Health hosts food security tabletop exercise.** The Indiana State Department of Health (ISDH) hosted a food security tabletop exercise earlier this month. The exercise, which was conducted in Indianapolis, was the first food security tabletop exercise to focus on the food processing industry. In this exercise, participants simulated an incident involving the deliberate contamination of a food commodity, which had been committed during processing and had gone undetected. More than 100 participants from several government agencies, the private sector and academia shared plans, procedures, and ideas with each other as they worked through the scenario. They discussed how their organizations would respond during different phases of the event, from the initial threat through the recovery phase. Because this was a first-of-its kind event, plans call for the results of the exercise to eventually be made available as a training module for industry, other states, and local jurisdictions across the nation to use in heightening awareness of food security issues. Additionally, ISDH's two fulltime Food Defense Program Coordinators will continue their efforts to increase food security levels in Indiana through educational programs and assisting food industry officials in identifying and minimizing their operations' vulnerabilities.

Source: <http://www.in.gov/isdh/whatsnew/express/2005%20Express/031005.pdf>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

23. *March 17, Washington Post* — **Anthrax alarm uncovers response flaws.** The anthrax scare at the Pentagon Monday, March 14, exposed gaps between the military's procedures in handling biohazards and those of the rest of the federal government, which could increase the threat to public health in the event of an actual contamination, health experts and federal and Virginia officials said Wednesday, March 16. Health officials inside government and out said the Pentagon's reliance on detection and response systems that are isolated from those at other federal agencies delayed Virginia health officials, the U.S. Postal Service, and the Centers for Disease Control and Prevention (CDC) in moving to protect the public from a possible biohazard. Local hazardous materials teams were confused by sensor equipment that differed from equipment used by the Postal Service and Department of Homeland Security, said Robert B. Stroube, Virginia's health commissioner. State and federal officials responsible for deciding public health actions said scientists had trouble interpreting the findings from a Pentagon contract lab, which is not part of the CDC's national network of labs that respond to bioterror. Officials in Fairfax, VA, and the District of Columbia, along with members of Congress, called for a summit to discuss the federal response.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A42040-2005Mar 16.html>

24. *March 16, University of Michigan* — In emergency, flu vaccine could be made quickly in existing facilities. In an emergency such as a pandemic outbreak or 2004's vaccine shortage, the influenza vaccine could be produced twice as fast using cell cultures in existing biopharmaceutical manufacturing facilities, according to Henry Wang, a University of Michigan professor of biomedical and chemical engineering, Wang, speaking at the 229th American Chemical Society National Meeting, will propose a system for retrofitting existing biopharmaceutical buildings to produce the flu vaccine using cell cultures. In the cell culture approach, the flu virus incubates in cell cultures rather than in eggs. Several companies are trying to perfect the cell-based flu vaccines where cells are grown in large vats. It is seen as a promising approach because it's more flexible and quicker than the current egg culture method. By building a separate cell culture facility and shipping the cell to the existing biomanufacturing plants, the production cycle could be cut in half to two months, Wang said. Wang identified approximately a dozen potential facilities around the world that are large scale Food and Drug Administration approved facilities that could potentially be modified to manufacture flu vaccines in an emergency.

Source: http://www.umich.edu/news/index.html?Releases/2005/Mar05/r03_1605a

25. *March 16, Agence France Presse* — Vietnam plans reserve of one million doses of bird flu vaccine. Vietnam, which has reported the most human deaths from bird flu, wants to reserve one million doses of a vaccine against the disease once tests are complete and production begins, a top research scientist said. "We envisage a strategic reserve of one million doses of the vaccine against the H5N1 virus in Vietnam, given account the population size and the extent of the bird flu epidemic," said Hoang Thuy Nguyen, chief of research on the bird flu vaccine at Hanoi's Central Institute of Hygiene and Epidemiology. Last month, state scientists said the bird flu vaccine developed in Vietnam had shown good results in tests on chickens and mice. The vaccine would also be tested on humans before being produced in mass quantities.

Source: <http://health.news.designerz.com/vietnam-plans-reserve-of-one-million-doses-of-bird-flu-vaccine.html?d20050316>

[[Return to top](#)]

Government Sector

26. *March 17, New York Times* — Security chief signals a shift in approach to terror. The United States government cannot protect the American public from all possible terrorist attacks and instead must focus on trying to prevent more serious or catastrophic strikes, Department of Homeland Security Secretary Michael Chertoff said on Wednesday, March 16. "Threats are important, but they should not be automatic instigators of action," Chertoff said in his first extensive public comments since taking over the department a month ago. Chertoff's remarks, in an interview and a speech at George Washington University, reflected his view that the Department of Homeland Security must transform itself from an enterprise set up in reaction to the September 11 attacks to one engaged in a more focused, sustainable and reasoned battle against terrorism. "This is a marathon, not a sprint," he said. In his remarks, Chertoff also outlined some of his priorities for the sprawling two-year-old department, formed by the merger of 22 agencies after the 2001 attacks. Among his first goals is to review the way the

department, which has about 180,000 employees, is organized. For the text of his remarks see http://www.dhs.gov/dhspublic/interapp/speech/speech_0245.xml
Source: <http://www.nytimes.com/2005/03/17/politics/17home.html?hp&ex=1111122000&en=38c5838f1eccc37b&ei=5094&partner=homepage>

[\[Return to top\]](#)

Emergency Services Sector

27. *March 17, Continuity Central (UK)* — **U.S. courts told to develop disaster recovery and continuity of operations plans.** A new security blueprint for America's state courts emphasizing critical review of operating procedures and facilities, planning, funding, and new courthouse design was released recently by the National Center for State Courts (NCSC). In addition to presenting a ten–point blueprint, NCSC also announced plans for a National Summit on Court Safety and Security. The National Summit will bring together all members of the court community to provide a mechanism for reviewing current safety and security practices and needs. This effort will result in a strategic action plan that will draw from a compilation of best practices and will provide the mechanism for identifying resource and funding needs. National Center for State Courts: <http://www.ncsconline.org/>
Source: <http://continuitycentral.com/news01796.htm>
28. *March 17, Pine Bluff Commercial (AR)* — **Pine Bluff prepares with final drill.** On Wednesday, March 16, a simulated accident occurred at the Pine Bluff Arsenal in Pine Bluff, AR, during routine operations while loading nerve–agent filled rockets onto a container being moved to the Pine Bluff Chemical Agent Disposal Facility. Six Arsenal employees were reported "injured" in the mock accident and treated on base. Non–essential Arsenal personnel were evacuated while staff at the National Center for Toxicological Research were taking shelter and the disposal facility was evacuated. The Pine Bluff Arsenal is one of eight sites that house the nation's reserve of stockpile chemical weapons, which must be destroyed by a 2012 international treaty deadline. The Arsenal is preparing to begin incinerating its stock of aging weapons later this month.
Source: <http://www.pbcommercial.com/articles/2005/03/17/news/news2.t xt>
29. *March 17, The Capital (MD)* — **First responders participate in safety drill on Chesapeake Bay in Maryland.** A quarter–mile off the beaches of Sandy Point State Park in Annapolis, MD, the Harbor Queen was reporting trouble. Fire was spreading in the engine room and 18 people and a 185–pound mannequin needed help. Members of the county and city Fire Departments, as well as the Natural Resources Police and U.S. Coast Guard, responded to a simulated fire on the double–decker Annapolis tour boat about 9 a.m. Wednesday, March 16, as part of a training exercise. Officials from the Mid–Chesapeake Marine Emergency Response Group, which includes local, state and federal agencies, participated in the event. The drill took six months to plan, but those involved only had two hours to "save" 18 lives. Each department involved will review the training and determine if a more detailed exercise is needed.
Source: http://www.hometownannapolis.com/cgi-bin/read/2005/03_17-21/TOP

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

30. *March 16, Secunia* — **PHPOpenChat "sourcedir" file inclusion vulnerability.** A vulnerability in PHPOpenChat was reported, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "sourcedir" parameter in "contrib/yabbse/poc.php" is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.
Source: <http://secunia.com/advisories/14600/>
31. *March 16, Federal Computer Week* — **Sarasota County, Florida government secures wireless network.** Cautious about the security of its wireless network, the Sarasota County, FL government has installed devices in its buildings to detect and prevent wireless intrusion. By using such devices to secure about three million square feet of airspace across 15 of the county's 200 buildings, it is easier for information technology personnel to spot any unauthorized vulnerabilities or attacks on the wireless infrastructure. "We minimize the risk that occurs through these devices," said Bob Hanson, Sarasota County's chief information officer. Hanson said his government has security policies in place, but with considerable employee turnover each year, it's difficult to keep up their education. He said there are almost 5,000 employees in the area covered, and rogue wireless access points are perplexing. Sarasota IT officials can monitor their airspace using a centralized Web-based interface. Rich Swier, CEO of monitoring system company, said that although the benefits of wireless are obvious, it has also created a problem. Before, security personnel only had to worry about security within their facilities. "Now you're having your good guys, your employees and so forth bringing in devices and exposing your network outside your four walls."
Source: <http://www.fcw.com/article88313-03-16-05-Web>
32. *March 15, Symantec* — **Symantec products multiple vulnerabilities.** Multiple vulnerabilities are identified in Symantec products (Enterprise Firewall, VelociRaptor, and Gateway Security) that may be exploited by attackers to conduct DNS cache poisoning and redirection attacks. An updated hot fix was released on March 14 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>
Source: <http://securityresponse.symantec.com/avcenter/security/Content/2005.03.15.html>
33. *February 09, Government Accountability Office* — **GAO-05-151: Telecommunications: Greater Involvement Needed by FCC in the Management and Oversight of the E-Rate Program. (Report).** Since 1998, the Federal Communications Commission's (FCC) E-rate program has committed more than \$13 billion to help schools and libraries acquire Internet and telecommunications services. Recently, however, allegations of fraud, waste, and abuse by some E-rate program participants have come to light. As steward of the program, FCC must ensure that participants use E-rate funds appropriately and that there is managerial and financial accountability surrounding the funds. The Government Accountability Office (GAO) reviewed (1) the effect of the current structure of the E-rate program on FCC's management of the program, (2) FCC's development and use of E-rate performance goals and measures, and

(3) the effectiveness of FCC’s oversight mechanisms in managing the program. GAO recommends that FCC (1) determine comprehensively which federal accountability requirements apply to E–rate; (2) establish E–rate performance goals and measures; and (3) take steps to reduce the backlog of beneficiary appeals. In response, FCC stated that it does not concur with (1) because it maintains it has done this on a case–by–case basis. GAO continues to believe that major issues remain unresolved. FCC concurs with (2) and (3), noting that it is already taking steps on these issues. Highlights: <http://www.gao.gov/highlights/d05151high.pdf>
 Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-151>

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 | The Top Ten Target Port information is unavailable due to technical difficulties. Source: http://isc.incidents.org/top10.html ; Internet Storm Center |
|----------------------------|--|

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

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

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS/IAIP Products & Contact Information

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

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

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

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

DHS/IAIP Disclaimer

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