Daily Highlights

• The Associated Press reports Mohammad Alavi, a former engineer at the nation's largest nuclear power plant — Palo Verde power plant west of Phoenix — has been charged with taking computer access codes and software to Iran and using it to download details of plant control rooms and reactors. (See item 1)

• The New York Times reports the Social Security numbers of tens of thousands of people who received loans or other financial assistance from two Department of Agriculture programs were disclosed for years in a publicly available database, raising concerns about identity theft and other privacy violations. (See item 17)

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

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

1. April 22, Associated Press — Ex–nuclear plant engineer allegedly took data to Iran. A former engineer at the nation's largest nuclear power plant has been charged with taking computer access codes and software to Iran and using it to download details of plant control rooms and reactors, authorities said. The FBI said there's no indication the plant employee had any terrorist connections. Mohammad Alavi, who worked at the triple–reactor Palo Verde power plant west of Phoenix, was arrested April 9 at Los Angeles International Airport when he arrived on a flight from Iran. According to court records, the software is used only for training
plant employees but allowed users access to details on the Palo Verde control rooms and the plant layout. In October, authorities alleged, the software was used to download training materials from Tehran, using a Palo Verde user identification. The FBI said there was no evidence to suggest the software access was linked to the Iranian government.
Source: http://www.knoxnews.com/kns/national/article/0,1406,KNS_350_5498078,00.html

2. April 21, Los Angeles Times — Alleged saboteur of power grid gained access despite warning. A contract technician accused of sabotaging computers at the California Independent System Operator (Cal–ISO) was able to enter the building and high-security inner rooms — allowed in by electronic card readers and a handprint scanner — even though his employer had warned days earlier that he should be denied access to the facility, authorities said. Lonnie Charles Denison, a 32–year–old computer specialist, has a “history of mental illness, drug abuse and alcohol issues,” a prosecutor said Friday, April 20. Sunday's incident has raised alarms among state and federal energy regulators. Denison was arrested by the FBI on Wednesday and charged with attempted destruction of an electrical facility. Around midnight Sunday he broke a glass seal and pushed an emergency electricity shut–off button, plunging the Cal–ISO building in Folsom into darkness and crashing computers used to communicate with the power market. The act caused no blackouts but could have disrupted the western U.S. power grid had it happened during hours of peak demand for electricity, such as a summer afternoon. Denison early Sunday night tried and failed to log on to access the Cal–ISO computer network. However, a few hours later he succeeded in gaining physical entry to the building.

3. April 20, Associated Press — Workers at BP refinery hospitalized. BP PLC said Friday, April 20, about 90 contract workers at its Texas City, TX, refinery were sent to hospitals overnight for medical observation after reporting they were feeling ill. BP spokesperson Scott Dean said Friday morning the latest information he had was that all the workers, whose complaints included eye irritation and nausea, had been released from local hospitals. The refinery, about 30 miles southeast of Houston, was the site of a 2005 explosion that killed 15 people and injured 170. Dean said the workers who fell ill were part of a group of about 400 working on a crude distillation unit that's been shut down since Hurricane Rita hit the Gulf Coast in 2005.
Source: http://biz.yahoo.com/ap/070420/bp_illness.html?v=1

4. April 19, Associated Press — Experts prepare for nuclear emergencies. Experts from around the globe gathered at a rural military facility in Austria for a training exercise aimed at boosting their performance during nuclear emergencies. The roughly 180 participants — including government agencies, institutes, companies and nuclear power plants from Australia, Canada, Germany and Iran — detected, identified and measured radiation. The session was part of a five–day training program that began Monday, April 16, and was organized by Austrian Research Centers in cooperation with the International Atomic Energy Agency. The aim was to prepare participants for emergency situations such as terrorist attacks and other scenarios involving radiation leaks.
5. **April 19, Associated Press** — Cities looking to create mini–energy districts to ensure reliable power. Mayors across the country fear aging and unreliable electric transmission systems, coupled with skyrocketing energy costs, are hurting efforts to recruit new business and keep existing ones in their cities. They are especially concerned about financial firms, such as hedge funds, where a loss of power can shut down transactions and equate to a loss of millions of dollars. That's why some are considering creating new micro grid districts, in which neighboring companies band together to produce their own electric power. The concept is already popular among communities in Europe and a similar version of it is being used in Walt Disney World in Orlando, FL. Within these special zones, sometimes referred to as "energy independence districts," businesses, government buildings and office buildings can design and create their own power source, such as a fuel cell or natural gas generator, using the electric grid only as a backup. They might also tap into underground aquifers and use that water for heating and cooling purposes, or even install solar panels to capture more energy. The entities in the district would essentially plan an electrical system that uses the energy efficiently, based on their needs.


6. **April 16, Bloomberg** — Russia plans world’s longest undersea tunnel to Alaska. Russia plans to build the world's longest tunnel, a transport and pipeline link under the Bering Strait to Alaska, as part of a $65 billion project to supply the U.S. with oil, natural gas and electricity from Siberia. The project, which Russia is coordinating with the U.S. and Canada, would take 10 to 15 years to complete, Viktor Razbegin of the Russian Economy Ministry said, Wednesday, April 18. State organizations and private companies in partnership would build and control the route, known as TKM–World Link. A 3,700–mile transport corridor from Siberia into the U.S. will feed into the tunnel. The tunnel would run in three sections to link the two islands in the Bering Strait between Russia and the U.S. The planned undersea tunnel would contain a high–speed railway, highway and pipelines, as well as power and fiber–optic cables. The World Link will save North America and Far East Russia $20 billion a year on electricity costs, said Vasily Zubakin of Hydro OGK. The project envisions building high–voltage power lines with capacity of up to 15 gigawatts to supply the new rail links and also export to northern America.


**Chemical Industry and Hazardous Materials Sector**

7. **April 20, WTHR (IN)** — Chemical leak prompts evacuation. A chemical leak from a semi trailer caused an evacuation in downtown Marion, IN, Friday morning and early afternoon, April 20. It happened at State Roads 18 and 37. The semi was leaking anhydrous ammonia. The vehicle was moved out of downtown Marion to a more remote area along State Road 18. The two–block area around the leak was evacuated. It is primarily a business area. The roads were also closed off.

8. **April 20, Associated Press — Gas leak causes evacuations at college.** Classes resumed Friday, April 20, at Elizabethtown College, PA, a day after six classroom buildings were evacuated when a broken pipeline sent a plume of natural gas across the campus. Construction workers severed the pipe about noon Thursday at the 1,800–student private college in Lancaster County. Workers from the gas company soon arrived to repair the pipeline. 

---

**Defense Industrial Base Sector**

9. **April 20, U.S. Air Force — Air Force official testifies on UAV executive agent issue.** The deputy chief of staff for intelligence, surveillance and reconnaissance explained why Air Force leaders support the idea of creating an executive agency for unmanned aerial vehicles (UAVs) before the House Armed Services air and land forces subcommittee (HASC) Thursday, April 19. Lt. Gen. David A. Deptula joined other Department of Defense representatives in providing testimony to the HASC. The plan, originally proposed by Air Force Chief of Staff Gen. T. Michael Moseley, calls for the Air Force to oversee the fielding, integration, and operation of medium– to high–altitude UAVs. The executive agency plan would streamline acquisition, employment and overall mission effectiveness, General Deptula said. "We want to work in a unified fashion when purchasing these systems," the general said. "Doing so would be more cost–effective, freeing up funds for other programs across all the services." Without an executive agency, the services will likely continue their separate design and procurement efforts, and the Department of Defense (DoD) will have forfeited the considerable savings it could have realized. Additionally, DoD will have lost an opportunity to create and harness the interservice synergies that would result from building upon — rather than duplicating — each service's strengths, General Moseley said.

10. **April 20, Washington Post — Army contracting criticized.** A Senate panel chastised the Army Thursday, April 19, for not moving faster to award a new contract to provide logistical support to U.S. troops worldwide, even as the current contractor continued to receive critical reports from auditors, including allegations of overcharging. The Army has said it would end the current contract with KBR early and award a new contract this summer that would divide the work among three competitors. But Sen. Carl M. Levin (D–MI), chairman of the Senate Armed Services Committee, asked during a hearing yesterday: "Why didn't you do it in 2004 when we first brought this to you?" "I don't have a good answer for you," responded Claude M. Bolton Jr., assistant Army secretary for acquisitions, logistics and technology. The panel also challenged the Army on whether the military could assume the task of providing services now provided by KBR. But Bolton said KBR's more–than–50,000 contractors in Iraq would have to be replaced with a larger contingent of soldiers. KBR has been repeatedly accused of sloppy bookkeeping, and audits have found such alleged overcharges as charging for meals not served, insisting on embroidered hand towels and overpaying for trailers.
11. April 19, Government Accountability Office — GAO−07−730T: Space Acquisitions: Actions Needed to Expand and Sustain Use of Best Practices (Testimony). The Department of Defense’s (DoD) space system acquisitions have experienced problems over the past several decades that have driven up costs by hundreds of millions, even billions of dollars, stretched schedules by years, and increased performance risks. DoD has recognized the need to change its approach to developing space systems and is attempting to instill best practices in new efforts. The Government Accountability Office (GAO) was asked to testify on its findings on space acquisitions problems and steps needed to sustain and expand the use of best practices. In preparing this testimony, GAO relied on its detailed reviews of space programs as well as cross−cutting work on cost estimating and best practices. GAO does not make recommendations in this testimony. However, GAO has made recommendations on steps DoD can take to ensure better outcomes for its space acquisitions programs. These include developing an overall investment strategy for acquisition programs, addressing human capital and other shortfalls in capacity, and revising policies supporting space to incorporate best practices.
Source: http://www.gao.gov/cgi-bin/getrpt?GAO−07−730T

12. April 19, Government Accountability Office — GAO−07−596T: Intelligence, Surveillance, and Reconnaissance: Preliminary Observations on DoD’s Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development (Testimony). As operations overseas continue, the Department of Defense (DoD) is experiencing a growing demand for intelligence, surveillance, and reconnaissance (ISR) assets to provide valuable information in support of military operations. While the 2006 Quadrennial Review emphasized the need for the ISR community to improve the integration and management of ISR assets, DoD plans to make significant investments in ISR capabilities for the future. Congress has been interested in DoD’s approach for managing and integrating existing assets while acquiring new systems. This testimony addresses preliminary observations based on the Government Accountability Office’s (GAO) ongoing work regarding (1) the status of DoD initiatives intended to improve the management and integration of ISR requirements and challenges DoD faces in implementing its initiatives, (2) DoD’s approach to managing current ISR assets to support military operations, and (3) the status of selected ISR programs in development and the potential for synergies between them. GAO’s ongoing work included document review, interviews with officials at relevant organizations, observations of some U.S. Central Command operations, and review of 13 airborne ISR development programs.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−596T

Banking and Finance Sector

14. April 20, Associated Press — Atlanta police recruit arrested on bank robbery warrant. An Atlanta police recruit has been arrested on a bank robbery warrant from Delaware State Police. Police spokesperson James Polite says 26-year-old Curtis Hamilton was employed as a police recruit on March 20th. He says Hamilton was assigned to administrative duties — routine for all recruits — while waiting for the start date of his Police Academy class. As part of their training, Hamilton and other recruits were required to enter personal information into a computer and the warrant appeared in a national criminal database. Polite says the warrant was for a bank robbery at a Wachovia Bank in January in Delaware. Polite says an extensive background investigation was conducted on Hamilton before he was hired and no criminal warrants were found. He says the warrant was placed in the national criminal database on April 3rd — two weeks after the recruit was hired.


15. April 20, Associated Press — Los Alamos warns workers about identity theft. Los Alamos National Laboratory warned employees about protecting themselves against identity theft after the names and Social Security numbers of 550 lab workers were posted on a Website run by a subcontractor working on a security system. An April 5 letter to the employees from Jan A. Van Prooyen, the lab’s acting deputy director, said the problem was discovered the previous week when a lab employee happened upon the Website of a software services company that had been hired years before. Clicking a link and entering a password provided online led to a table that included names, and in some cases, Social Security numbers, of people who entered certain lab sites around 1998, the letter said. Van Prooyen said the lab wasn’t aware of “this unauthorized use” of personal information until March 28, and that the former subcontractor removed the information that afternoon after the lab contacted the company.


16. April 20, Websense Security Labs — Multiple phishing alerts: Trans West Credit Union and Tri-Lakes Federal Credit Union. Websense Security Labs have received reports of a phishing attack that targets TransWest Credit Union and Tri-Lakes Federal Credit Union customers. Trans West Credit Union users receive a spoofed email message, which asks them to renew the listed services and that failure to do so will result in the suspension of the services provided. Tri–Lakes Federal Credit Union users receive a spoofed email message, which claims that due to recent changes in the Credit Union service agreement, the users need to submit additional details about their account. The email provides a link to a phishing site that attempts to collect personal and account information.


17. April 20, New York Times — U.S. database exposes Social Security numbers. The Social Security numbers of tens of thousands of people who received loans or other financial assistance from two Agriculture Department programs were disclosed for years in a publicly available database, raising concerns about identity theft and other privacy violations. Officials at the Agriculture Department and the Census Bureau, which maintains the database, were evidently unaware that the Social Security numbers were accessible in the database until they were notified last week by a farmer from Illinois, who stumbled across the database on the
Transportation and Border Security Sector

18. April 21, Boston Globe — **High-tech radios to boost subway safety in Boston.** In Boston, city, state, and Massachusetts Bay Transit Authority (MBTA) officials agreed Friday, April 20, to pay for a state-of-the-art emergency communications system in subway tunnels to fix a problem that has long been highlighted as a major gap in Boston's preparedness for a terrorist attack. The $16 million project will not only allow first responders and dispatchers to talk to one another above and below ground, but also allow incident commanders on the surface to communicate with those inside the Boston subway’s (T) 29.6 miles of tunnels. Currently, Boston's ambulance fleet can't communicate from T tunnels because old and new radio systems don't mesh or because antennas within the tunnels cannot relay their signal. Once complete, the new system will coordinate communications among Boston's Emergency Medical Services; the police and fire departments in Boston, Cambridge, and Somerville; State Police and MBTA Transit Police; and regional police and fire radio networks that support more than 100 departments. To thwart potential terrorists, the T has also installed more than 450 surveillance cameras in stations and tunnels that have also helped police identify suspects in robberies and assaults.


19. April 21, Inside Bay Area (CA) — **Hearing on BART retrofit Wednesday.** Although the Bay Area Rapid Transit (BART) system survived the 1989 Loma Prieta Earthquake and provided a lineline between the East Bay and San Francisco while the damaged Bay Bridge was closed, the 35-year-old system is overdue for retrofitting. "We know that if there was an earthquake that hit the Bay Area and it's significantly closer than Loma Prieta, we're going to suffer significant damage," said BART spokesperson Linton Johnson. "We're in a race against time to get this taken care of." To that end, construction is slated to begin early next year on strengthening the 1,918 columns that support elevated tracks along 73 miles of BART's original system from the early 1970s. Wednesday, April 25, area residents will get a chance to review environmental impact information on the construction and make comments at a public hearing in Oakland at the Metropolitan Transportation Commission headquarters.


20. April 20, El Paso Times — **Border cameras lack funding, remain off.** It will be at least an additional six months before cameras on the Texas border will again broadcast over the Internet live footage of undocumented immigrants crossing into the United States, officials said this
week. The Texas Department of Public Safety sought permission months ago to spend federal grant money to get the cameras online. But because approval for that money did not come until March, said Katherine Cesinger, a spokesperson for Governor Rick Perry, the department must wait for lawmakers to approve the cash to purchase the cameras. Perry announced he would invest $5 million on an Internet-based "neighborhood watch" program for the border last June. The site went public for a 27-day test run in November. Eight to 12 cameras along Texas’ 1,200-mile border with Mexico broadcast footage from four counties: El Paso, Val Verde, Hidalgo, and Cameron. The test cost was about $200,000. State documents the El Paso Times obtained earlier this year showed millions of viewers checked out the site. Since the test, the cameras and the border watch Website have been shut down. State officials have been awaiting money to buy more cameras and continuously operate the border watch Website.


21. April 18, Government Accountability Office — GAO–07–489T: Coast Guard: Observations on the Fiscal Year 2008 Budget, Performance, Reorganization, and Related Challenges, statement for the record (Testimony). The U.S. Coast Guard is a multimission agency responsible for maritime safety, security, and stewardship. It performs these missions, relating to homeland security and non–homeland security in U.S. ports and inland waterways, along the coasts, and on international waters. The President’s budget request, including the request for the Coast Guard, was transmitted to Congress on February 5, 2007. This testimony, which is based on current and past Government Accountability Office (GAO) work, synthesizes the results of this work as it pertains to the following: • budget requests and performance goals, • organizational changes and related management initiatives, • current acquisition efforts and challenges, and • challenges related to performing traditional legacy missions. While this statement makes no recommendations, in the past GAO has made a number of recommendations on issues covered in this statement. The Coast Guard is in various stages of implementing these recommendations.


22. March 30, Government Accountability Office — GAO–06–591T: Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System (Reposted testimony). U.S. Customs and Border Protection’s (CBP) Automated Targeting System (ATS)—a computerized model that CBP officers use as a decision support tool to help them target oceangoing cargo containers for inspection—is part of CBP’s layered approach to securing oceangoing cargo. GAO reported in February 2004 on challenges CBP faced in targeting oceangoing cargo containers for inspection and testified before this subcommittee in March 2004 about the findings in that report. The report and testimony outlined recommendations aimed at (1) better incorporating recognized modeling practices into CBP’s targeting strategy, (2) periodically adjusting the targeting strategy to respond to findings that occur during the course of its operation, and (3) improving implementation of the targeting strategy. This statement for the record discusses preliminary observations from the Government Accountability Office’s (GAO) ongoing work related to ATS and GAO’s 2004 recommendations addressing the following questions: • What controls does CBP have in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of smuggled weapons of mass destruction? • How does CBP systematically analyze security inspection results and incorporate them into
What steps has CBP taken to better implement the rest of its targeting strategy at the seaports?

Postal and Shipping Sector

23. April 19, Government Accountability Office — GAO–07–685T: U.S. Postal Service: Postal Reform Law Provides Opportunities to Address Postal Challenges (Testimony). When the Government Accountability Office (GAO) originally placed the U.S. Postal Service’s (the Service) transformation efforts and long–term outlook on its high–risk list in early 2001, it was to focus urgent attention on the Service’s deteriorating financial situation. Aggressive action was needed, particularly in cutting costs, improving productivity, and enhancing financial transparency. GAO testified several times since 2001 that comprehensive postal reform legislation was needed to address the Service’s unsustainable business model, which assumed that increasing mail volume would cover rising costs and mitigate rate increases. This outdated model limited its flexibility and incentives needed to realize sufficient cost savings to offset rising costs, declining First–Class Mail volumes, unfunded obligations, and an expanding delivery network. This limitation threatened the Service’s ability to achieve its mission of providing affordable, high–quality universal postal services on a self–financing basis. This testimony will focus on (1) why GAO recently removed the Service’s transformation efforts and outlook from GAO’s high–risk list, (2) the Service’s financial condition in fiscal year 2007, (3) the opportunities and challenges facing the Service, and (4) major issues and areas for congressional oversight. This testimony is based on GAO’s past work, review of the postal reform law, and updated information on the Service’s financial condition.

Agriculture Sector

24. April 20, Agence France–Presse — Netherlands reports mad cow case. The Dutch ministry of Agriculture announced on Friday, April 20, that it has discovered mad cow disease in a seven–year–old cow. It is the 83rd case of mad cow disease, or Bovine Spongiform Encephalopathy (BSE) in the Netherlands since 1997 but the first since March 2006. Netherlands authorities do routine checks on all slaughtered bovines for BSE. One cow from the same farm and another six from other farms believed to be at risk for mad cow disease, because they received the same feed or were descendants of the sick cow, were also culled.
Source: http://news.yahoo.com/s/afp/20070420/hl_afp/netherlandshealt h_070420174437;_ylt=Au40sVsmY1.toLxT9Dkb9SwCJOrgF

25. April 19, Animal and Plant Health Inspection Service — Additional funding to eradicate potato cyst nematode. U.S. Department of Agriculture Secretary Mike Johanns Thursday, April 19, announced the availability of nearly $11 million in additional Commodity Credit
Corporation (CCC) funds to implement an eradication strategy for potato cyst nematode (PCN) in Idaho. USDA's Animal and Plant Health Inspection Service (APHIS), in coordination with the Idaho State Department of Agriculture (ISDA), confirmed the first U.S detection of PCN in a soil sample collected from a potato processing facility in Idaho last April. Following the August 2006 transfer of $12.9 million in CCC funds, state and federal agricultural officials began an extensive survey of Idaho production and seed potato fields, packing facilities and storage sheds. The survey, which included testing more than 34,000 soil samples from 800 fields and facilities, determined that PCN is confined to seven fields within a one-mile radius. The PCN eradication program in Idaho is projected to last five years. APHIS and ISDA will use this latest infusion of funding for intensive surveys, soil fumigation and strict enforcement of quarantine regulations to prevent PCN from spreading. PCN, Globodera pallida, is a major pest of potato crops in cool–temperate areas. If left uncontrolled, nematodes can cause up to 80 percent yield loss.

Source: [http://www.usda.gov/wps/portal/ut/p/_s.7_0_A/7_0_1OB/cm...](http://www.usda.gov/wps/portal/ut/p/_s.7_0_A/7_0_1OB/cm...)

26. April 11, North American Plant Protection Organization — First report of sweet potato chlorotic stunt virus in North Carolina. Sweet potato chlorotic stunt virus (SPCSV) was detected for the first time in North Carolina. SPCSV when found in association with Sweet potato feathery mottle virus (SPFMV) causes Sweet potato virus disease (SPVD), a serious disease originally described in Africa in the 1970’s. Sweet potato chlorotic stunt virus is the whitefly transmitted component of the disease. Sweet potato feathery mottle virus is transmitted by aphids. The only other U.S. report of SPCSV was from a single accession in the U.S. Department of Agriculture Sweet Potato Germplasm Repository. No other detections of SPCSV have been reported in the U.S. In both cases of U.S. SPCSV detection, SPFMV was also present.


Food Sector

27. April 20, Associated Press — FDA asks if pet food tainted on purpose. Imported ingredients used in recalled pet food may have been intentionally spiked with an industrial chemical to boost their apparent protein content, federal officials said Thursday, April 19. That's one theory being pursued by the U.S. Food and Drug Administration (FDA) as it investigates how the chemical, melamine, contaminated at least two ingredients used to make more than 100 brands of dog and cat foods. So far, melamine's been found in both wheat gluten and rice protein concentrate imported from China. Media reports from South Africa suggest a third pet food ingredient, corn gluten, used in that country also was contaminated with melamine. That tainted ingredient has not been found in the U.S., the FDA said. FDA investigators were awaiting visas that would allow them to visit the Chinese plants where the vegetable protein ingredients were produced. Chinese authorities have told the FDA that the wheat gluten was an industrial product not meant for pet food, Sundlof said. Still, melamine can skew test results to make a
product appear more protein-rich than it really is, he added. That raises the possibility the contamination was deliberate.


28. **April 19, California Department of Food and Agriculture** — **California hog farm quarantined.** The American Hog Farm, a 1500-animal facility in Ceres, has been quarantined by the California Department of Food and Agriculture, and lab testing has revealed the presence of the chemical melamine in pig urine. Additional testing of tissues, serum and urine from animals at the farm is underway at the California Animal Health and Food Safety Laboratory at the University California–Davis to determine if melamine is present in meat. “Although all animals appear healthy, we are taking this action out of an abundance of caution,” said State Veterinarian Dr. Richard Breitmeyer. “It is unknown if the chemical will be detected in meat. The farm is cooperating with us to determine the disposition of all animals that have left the premises since April 3.” It is believed the melamine originated with rice protein concentrate shipped from China. Through an importer, the concentrate was distributed to Diamond Pet Foods, a pet food manufacturer which sold salvage pet food to the farm for pig feed. Tests of salvage pet food/pig feed at the farm were positive for melamine, as were tests on the pet food in question, Natural Balance — the subject of a recall announced April 16.


29. **April 19, U.S. Food and Drug Administration** — **Company announces recall of one production run of dry cat food.** The Blue Buffalo Company Thursday, April 19, announced a recall of one production run of its Spa Select Kitten dry food. The Company has taken this action because the rice protein concentrate used for this particular production run was obtained from Wilbur–Ellis, the same company who supplied this ingredient to Natural Balance. Test results received the evening of April 18th indicated that this rice protein concentrate tested positive for melamine. This was the only production run that used rice protein from Wilbur–Ellis. Of the 5,044 bags produced in this particular production run, the Company was able to prevent the majority from ever entering retail distribution.


30. **April 18, U.S. Food and Drug Administration** — **Wilbur–Ellis recalls rice protein concentrate.** Wilbur–Ellis Company is recalling all lots of the rice protein concentrate the San Francisco, CA, company’s Feed Division has shipped to pet–food manufacturers because of a risk that rice protein concentrate may have been contaminated by melamine, an industrial chemical used to make plastics and fertilizers that can lead to illness or fatalities in animals if consumed. Wilbur–Ellis noted that it obtained rice protein from a single source in China and shipped to a total of five U.S. pet–food manufacturers located in Utah, New York, Kansas, and two in Missouri. On April 15, Wilbur–Ellis notified the U.S. Food and Drug Administration (FDA) that a single bag in a recent shipment of rice protein concentrate from its Chinese supplier, Binzhou Futian Biology Technology Co. Ltd., had tested positive for melamine. Unlike the other white–colored bags in that shipment, the bag in question was pink and had the word “melamine” stenciled upon it. Wilbur–Ellis separated that bag and quarantined the entire shipment for further testing and since that time, no further deliveries of rice protein concentrate have been made. Samples from the white bags tested negative for melamine. However,
subsequent and potentially more sensitive tests by the FDA came back positive for melamine. Source: [http://www.fda.gov/oc/po/firmrecalls/wilburellis04_07.html](http://www.fda.gov/oc/po/firmrecalls/wilburellis04_07.html)

**Water Sector**

31. **April 19, Associated Press — U.S. House passes multibillion water bill.** The U.S. House of Representatives overwhelmingly approved a multibillion-dollar bill Thursday, April 19. Hundreds of projects are in the bill that was approved 394–25. Supporters say the projects are sorely needed to improve access to water supplies, restore coastal shorelines, improve flood control and navigation channels and other needs. But there is disagreement over how much those will cost. The Congressional Budget Office estimated a cost of $13.2 billion over 15 years. But the White House set the cost at at least $15 billion. Another $1.5 billion was added to the bill as it went to the House floor. Watchdog groups put the tab even higher. Source: [http://www.chron.com/disp/story.mpl/ap/tx/4732060.html](http://www.chron.com/disp/story.mpl/ap/tx/4732060.html)

32. **April 18, North County Times (CA) — Judge stands by water-supply shutdown ruling.** A Superior Court judge brushed aside objections from state water officials Wednesday, April 18, and reaffirmed his March decision ordering the California Department of Water Resources to get proper environmental permits or shut down the state water project that delivers up to two-thirds of southern California's water. State officials immediately said they would appeal Judge Frank Roesch's ruling. Regional water officials say reservoirs can sustain southern California for 12 to 18 months if the state water project is shut off. In March, Roesch ruled that state water officials did not properly seek environmental permits — and gave state officials 60 days to get them or shut the pumping station down. Regional water officials said in March that it would take the state at least a year to get the permits. Source: [http://www.nctimes.com/articles/2007/04/19/news/sandiego/28_15_364_18_07.txt](http://www.nctimes.com/articles/2007/04/19/news/sandiego/28_15_364_18_07.txt)

**Public Health Sector**

33. **April 20, Reuters — Tamiflu key to treat bird flu, avoid steroids.** Bird flu patients who get early treatment with the antiviral drug Tamiflu have the best chances of surviving while using steroids can do more harm than good, the World Health Organization (WHO) said on Friday, April 20. The WHO was reporting on the preliminary conclusions of international experts who met last month in Turkey to compare notes on treatments, including the attempt by doctors in some countries to use steroids as well. "Corticosteroid therapy has failed so far to show effectiveness," the WHO warned. "Prolonged or high dose corticosteroids can result in serious adverse events." Frederick Hayden of WHO's global influenza program said some doctors, notably in Vietnam and Indonesia, had administered steroids to try to save quickly deteriorating bird flu patients. Eight of nine had died, he said, citing published research. The WHO reaffirmed that early treatment with Tamiflu, known generically as oseltamivir, was useful in reducing death from the H5N1 virus. Giving it to people with advanced symptoms was also "warranted".
34. April 19, Associated Press — Makers expect to have 132 million doses of flu vaccine for U.S. Flu vaccine manufacturers expect to have a record 132 million doses ready for the 2007–2008 flu season, and even more could be available if a fifth company joins their ranks, officials said Thursday, April 19. CSL Biotherapies, an Australian company, applied last month for federal approval to sell its flu vaccine in the U.S. this fall. Government health officials have been expanding their flu shot recommendations to cover more age groups, and they now say that more than 200 million Americans should get vaccinated each year. If approved, CSL would join four other companies providing flu vaccine in the U.S. Three make flu shots — Sanofi Pasteur Inc., which projects 50 million doses; Novartis Vaccines, which expects to make up to 40 million doses; and GlaxoSmithKline, which is planning 30 million to 35 million doses. In addition, MedImmune Vaccines Inc. plans to manufacture about seven million doses of FluMist, a nasal mist recommended only for healthy people between ages five and 49.


35. April 20, Associated Press — Many campus threats after Virginia Tech shooting. A man who allegedly threatened a school attack in Yuba City, CA, that would dwarf the Virginia Tech attacks turned himself in, ending a manhunt that prompted school districts in two cities to tighten security, authorities said. Several schools canceled classes or evacuated students Thursday, April 19, and at least a dozen people were arrested or under investigation as a wave of campus threats that started soon after the Virginia Tech shootings spread across the country. In Yuba City, a 28–year–old man told a pastor Wednesday night that "he had some sort of explosive device and he was going to make the incident at Virginia Tech look mild by comparison," Sutter County Sheriff Jim Denney said. The man surrendered without incident at the sheriff's department around 9:30 p.m. Thursday, shortly after his parents called authorities to tell them he would turn himself in, Denney said. Nationwide, many of the threats — which spread in the time it takes to make a phone call or post a message on the Internet — referred to Monday's massacre in Blacksburg, VA, in which gunman Cho Seung–Hui killed 32 people and himself, or the 1999 Columbine High School killings, authorities said. Friday was the eighth anniversary of the Columbine attacks.

Source: http://hosted.ap.org/dynamic/stories/C/CAMPUS_THREATS?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

36. April 20, CNN — Gunman, hostage dead at NASA building, police say. A gunman who took two hostages Friday, April 20, at NASA's Johnson Space Center, in Houston, TX, has apparently killed himself and one hostage, police said. Another hostage has been taken to the hospital, said Houston Police Capt. Dwayne Ready. The gunman forced the evacuation of the building and put the entire center on alert. Earlier a witness in Building 44 on the campus reported two shots fired, said Ready, who described the suspect as a white man with blond hair, 50 to 60 years old. He had a handgun, said Ready. Ready said he had barricaded himself in a room. The apparent suicide happened on the second floor of Building 44, he added.

Emergency Services Sector

37. April 20, Federal Emergency Management Agency — President declares major disaster for Maine. The head of the U.S. Department of Homeland Security’s Federal Emergency Management Agency (FEMA) announced Friday, April 20, that federal disaster aid has been made available for the state of Maine to supplement state and local recovery efforts in the area struck by flooding during the period of March 16–18, 2007. FEMA Administrator David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to state and eligible local governments and certain private nonprofit organizations on a cost–sharing basis for emergency work and the repair or replacement of facilities damaged by the flooding in the counties of Hancock, Knox, Lincoln, and Waldo.

38. April 20, Federal Emergency Management Agency — DHS awards almost $4 million to prevent fire death and injury. The U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Friday, April 20, the first round of Fiscal Year (FY) 2006 Fire Prevention and Safety (FP&S) grants, awarding 52 grants totaling almost $4 million to fire departments and fire prevention organizations throughout the United States. Under the FY 2006 program, FP&S will award approximately 300 awards totaling $27 million to fire departments and other eligible organizations to reduce losses from fire and fire–related hazards. FP&S projects focus on preventing fire–related injuries to children, seniors, firefighters, and other high–risk groups. FP&S also supports innovative fire prevention solutions and research on improving firefighter health and safety.

Information Technology and Telecommunications Sector

39. April 20, eWeek — RIM: Software upgrade caused BlackBerry failure. BlackBerry maker Research In Motion (RIM) announced late Thursday, April 19, that it has determined the apparent cause of the shutdown that stopped e–mail service to BlackBerry users throughout North America earlier in the week. According to a statement from the Waterloo, Ontario–based company, the shutdown on April 17 was related to a software upgrade that went awry, followed by a failover process that also didn't work properly. The BlackBerry blackout happened when the company introduced a new, noncritical system routine into its database, officials said. The routine, according to RIM, was designed to improve cache optimization but instead caused a series of interaction errors between the databases and the cache.
Source: http://www.eweek.com/article2/0,1895,2119111,00.asp

40. April 19, IDG News Service — Spammers, hackers seize on Virginia Tech shootings. Spammers and hackers are using the slayings at Virginia Tech as a gory lure to infect
computers with malicious software, security experts noted Thursday, April 19. While the video made by gunman Cho Seung-hui prior to the killing of 33 people on Monday was widely posted on news Websites and YouTube.com, spam e-mails were intercepted Wednesday night purporting to link to the footage on a Brazilian Website, said Graham Cluley, senior technology consultant, at security vendor Sophos. If clicked, the link caused a computer to automatically download a malicious screensaver, called TERROR_EM_VIRGINIA.scr by Sophos, which installs a Trojan horse program that collects banking details, Cluley said. It's unclear yet what banks the Trojan is engineered to exploit, Cluley said. The e-mails are unlikely to mean much to English speakers since they're written in Portuguese, Cluley said. But hackers have repeatedly used breaking news events to try to trick users into opening malicious programs.

Source: http://news.yahoo.com/s/infoworld/20070419/tc_infoworld/8784
9;_ylt=AgdXD_ihKXtAYBBKpR0f5XMjtBAF

41. *April 19, CNET News — Cyberattacks at federal agencies draw House scrutiny.* As new details emerged about cyberattacks against networks at the State and Commerce departments last year, politicians on Thursday, April 19, said they're concerned many federal agencies are ill-prepared to fend off such intrusions. Members of a U.S. House of Representatives cybersecurity subcommittee said they weren't confident that the computer systems at bureaus within the State and Commerce departments were adequately secured and scrubbed of backdoors that could allow cybercrooks to re-enter. They also questioned agency representatives on whether they could truly guarantee that sensitive information hadn't been accessed or copied. Twenty-one of 24 major federal agencies had weak or deficient information security controls in place during the last fiscal year, according to audit reports, said Gregory Wilshusen, director of information security issues for the Government Accountability Office (GAO). Pitfalls ranged from failing to replace well-known vendor-supplied passwords on systems to not encrypting sensitive information to not creating adequate audit logs to track activity on their systems, according to a new GAO report he summarized at the hearing.


42. *April 19, Government Accountability Office — GAO−07−751T: Information Security: Persistent Weaknesses Highlight Need for Further Improvement (Testimony).* For many years, the Government Accountability Office (GAO) has reported that weaknesses in information security are a widespread problem with potentially devastating consequences — such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information. In reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue. Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies. FISMA also defines responsibilities for ensuring centralized compilation and analysis of incidents that threaten information security and providing timely technical assistance in handling security incidents. In this testimony, GAO discusses the continued weaknesses in information security controls at 24 major federal agencies, the reporting and analysis of security incidents, and efforts by the Department of Homeland Security to develop a cyber threat analysis and warning capability. GAO based its testimony on its previous work in this area as well as agency and congressional reports.
43. April 19, CNET News — Bug hunter targets routers, other gadgets. Software that runs home routers, cell phones and personal digital assistants is rife with security bugs, an expert said Thursday, April 19. Barnaby Jack, a Juniper Networks security researcher, gave a tutorial at the CanSecWest conference on how bug hunters can find exploitable vulnerabilities in such devices and demonstrated an attack on a D−Link router using a yet−to−be−patched hole. "Security flaws are abundant on these devices," Jack said. "Security needs to reach further than a home PC. Insecure devices pose a threat to the entire network. Hardware vendors must take security into consideration." There hasn't yet been a large amount of security research into the type of software Jack looks at. This is code that runs gadgets equipped with ARM, MIPS, XScale and PowerPC microprocessors. However, researchers appear increasingly interested in finding ways to attack routers and other such "embedded" devices. In examining software from various devices, Jack found that there are many exploitable "null pointers" in the code. "Vulnerabilities that are near dead in the PC realm are abundant," he said. "This is a new class of attack...This is a remote attack the same way as a buffer overflow or a heap overflow, but it is more reliable." 
Source: http://news.com.com/Bug+hunter+targets+routers%2C+other+gadgets/2100−1002_3−6177754.html

Internet Alert Dashboard

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/.

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

General Sector

Nothing to report.
DHS Daily Open Source Infrastructure Report Contact Information


**DHS Daily Open Source Infrastructure Report Contact Information**

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

**Contact DHS**

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

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us–cert.gov or visit their Web page at [www.us–cert.gov](http://www.us–cert.gov).

**Department of Homeland Security Disclaimer**

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