Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 29 March 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Associated Press reports in the past two years, authorities have intercepted at least $7 million in funds wired through Western Union that was intended for immigrant smugglers in the Phoenix area; this is a fraction of the estimated $320 million wired to Phoenix annually to pay for the illegal services. (See item 8)
- The Associated Press reports part of Cincinnati's main airport was temporarily shut down Sunday after a passenger passed through a security checkpoint with what appeared to be a gun in a carry−on bag; the passenger was not found. (See item 10)
- The Atlanta Business Chronicle reports the Georgia Department of Human Resources plans to launch a new comprehensive and individualized bioterrorism preparedness program for as many as 150,000 hospital workers across the state. (See item 20)

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 28, Wired News* — **Silicon shortage stalls solar power.** As demand for clean energy continues to grow, the solar industry forecasts millions of photovoltaic systems will dot the landscape by the end of the decade. However, a severe shortage of the silicon used in the systems threatens to dampen solar's growth. "There is a definite shortage of silicon out there

right now," said Gary Homan, vice president of Hemlock Semiconductor, which manufactures polycrystalline silicon that is used in semiconductors and photovoltaic cells. Demand for silicon from semiconductor manufacturers and the solar industry has increased sharply and semiconductor manufacturers are able to outbid solar companies for the available silicon because the material makes up a much smaller portion of their production costs, Homan said. "The solar industry has been living off the scraps of the computer industry. This is not a recipe for success," said Ron Pernick, founder of alternative−energy consultancy Clean Edge. Increasing silicon production to meet the expected growth in solar cells would take hundreds of millions of dollars in investment, according to Pernick.
Source: http://www.wired.com/news/planet/0,2782,67013,00.html

2. *March 25, TechNewsWorld* — **World's fastest supercomputer used to simulate stockpile.** The IBM supercomputer BlueGene/L is being built by the National Nuclear Security Administration (NNSA) to help simulate the condition of the nation's nuclear stockpile. The project is halfway done and now contains 32 racks with 1,024 dual−core IBM Power chips. It is expected to be complete by July, NNSA said spokesperson Bryan Wilkes. The record−breaking performance was attained at Lawrence Livermore National Laboratory, one of three NNSA labs. The NNSA will need all the computing power BlueGene can muster when it is fully built, Wilkes said, because of the complicated calculations necessary to understand the effects of aging on the United States' nuclear weapons cache. "At the NNSA, we need certain data that we would normally get from an underground nuclear test," he said. A moratorium on nuclear testing first enacted by President George H.W. Bush and extended by Presidents Clinton and George W. Bush means that the date must come from calculations. "Our primary mission is to make sure the nuclear stockpile is safe and reliable. To do that, we have to understand what's happening with the weapons as they age," Wilkes said.
Source: http://www.technewsworld.com/story/hardware/41770.html

3. *March 25, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission issues advisory on personal security controls.** The Nuclear Regulatory Commission (NRC) said Friday, March 25, it issued an advisory Wednesday, March 23, to nuclear facility operators emphasizing the need for a heightened level of awareness in ensuring the proper identity of personnel even though they may be escorted while in the facility. In order to obtain unescorted plant access, individuals are subject to an array of additional checks. A recent incident of a foreign national using a false social security number and a false alien registration card to obtain escorted access to work at a nuclear power plant identified the need for additional checks on escorted personnel. The NRC urged licensees to check identities against a national security database. Licensees were encouraged to report promptly the fraudulent use, or attempted use of false identification information.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2005/05−0 55.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *March 28, Reuters* — **Hackers phishing for Chinese victims.** Chinese consumers are becoming increasingly popular targets of international Internet scammers, or phishers, hoping to con the country's growing ranks of Web surfers out of their money. "China reported 223 fake Websites last year, a huge increase from only one reported from 2002 to 2003," Xinhua news agency said on Monday, March 28. Bank of China and Industrial Commercial Bank of China said in December they had found fake versions of their Websites. Apparently only one consumer was duped and both banks said they had taken further Internet security precautions. Most of the fake pages had been created by foreign hackers that could manipulate Chinese host servers because they were not backed by up−to−date security software or firewalls, Xinhua said. Debit and credit card use and electronic payments are surging in the fast−developing country, making many Chinese perfect prey for phishers.
   Source: http://www.expressindia.com/fullstory.php?newsid=43954

5. *March 28, BBC News (UK)* — **UK bank officials apologize for technical problems.** In the United Kingdom, Barclays Bank has apologized for a computer glitch on Sunday, March 27, which left millions of customers without cash. "It was a technical problem with the system in the south of England and we're terribly sorry it happened," said bank spokesperson Alistair Smith. About 1,500 cash machines were affected by the glitch, as well at telephone and Internet banking, which is back to normal. Barclays Bank officials said there was no impact on security −− only on "accessibility for people to their own accounts."
   Source: http://news.bbc.co.uk/1/hi/uk/4386977.stm

6. *March 28, Globes online (Israel)* — **First International Bank blackmail suspect arrested.** Detectives from the Israel Police Tel Aviv district fraud unit on Sunday, March 27, arrested a Bnei Brak resident suspected of obtaining Internet access codes to bank accounts of First International Bank of Israel customers. The man is suspected of using the codes to access four accounts and of withdrawing money without authorization. The arrested man is a relative of Dan Tiraspolsky, who was arrested Friday, March 25, on suspicion of giving access codes to criminals involved with the Russian mafia. The relative allegedly blackmailed Tiraspolsky over a debt. Tiraspolsky has worked at First International Bank's computer department for 12 years, and is responsible for information security, among other things. According to First International Bank investigators, Tiraspolsky admitted embezzling the customers' money, explaining that he was being blackmailed by members of the Russian mafia, who had threatened to harm him unless he gave them the codes.
   Source: http://new.globes.co.il/serveen/globes/docview.asp?did=89840 6&fid=942

7. *March 28, Washington Post* — **Secret Service's distributed computing project aimed at decoding encrypted evidence.** For law enforcement officials charged with stopping sophisticated financial crime and hacker rings, making arrests and seizing computers used in

the criminal activity is often the easy part. More difficult can be making the case in court, where getting a conviction often hinges on whether investigators can glean evidence off of the seized computer equipment and connect that information to specific crimes. Criminals can use widely available software to scramble evidence of their activities so thoroughly that even the most powerful supercomputers in the world would never be able to break into their codes. The Secret Service is tying together its employees' desktop computers in a network designed to crack passwords that alleged criminals have used to scramble evidence of their crimes −− everything from lists of stolen credit card numbers and Social Security numbers to records of bank transfers. To date, the Secret Service has linked 4,000 of its employees' computers into the "Distributed Networking Attack" (DNA) program. The effort started nearly three years ago to battle a surge in the number of cases in which savvy computer criminals have used commercial or free encryption software to safeguard stolen financial information, according to DNA program manager Al Lewis.
Source: http://www.washingtonpost.com/wp−dyn/articles/A6098−2005Mar2 8.html

8. *March 27, Associated Press* — **Arizona authorities intercept wire payments to smugglers.** In the past two years, authorities have intercepted at least $7 million in funds wired through Western Union that was intended for immigrant smugglers in the Phoenix, AZ, area. That's just a fraction of the estimated $320 million wired to Phoenix annually to pay for the illegal services. Authorities say that when it comes to getting paid, many people smugglers prefer Western Union because of the security it provides. Saskia Rietbroek, executive director of Miami, FL−based Association of Certified Anti−Money Laundering Specialists, said immigrants often also prefer to wire the money instead of conventional banking because of its anonymity, speed and convenience. "Sometimes when people are illegal aliens they prefer not to open a bank account because then the bank will ask for certain identification," Rietbroek said. Western Union has 220,000 locations worldwide and sends money transfers seven times a second every second of the year, according to a 2004 fourth−quarter report of its parent company, First Data Corp. Larry Flick, an agent for the Arizona Attorney General's Office, said smuggling operations use that to their advantage. The sheer volume of Western Union transactions makes it easier to hide themselves among the masses.
Source: http://www.mohavedailynews.com/articles/2005/03/28/news/stat e/state2.txt

[Return to top]

Transportation Sector

9. *March 28, Government Accountability Office* — **GAO−05−356: Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed (Report).** Among its efforts to strengthen aviation security, the Transportation Security Administration (TSA) is developing a new passenger prescreening system—known as Secure Flight. As required by Congress, TSA is planning to assume, through Secure Flight, the prescreening function currently performed by the air carriers. This report assesses the (1) status of Secure Flight's development and implementation, (2) factors that could influence the effectiveness of Secure Flight, (3) processes used to oversee and manage the Secure Flight program, and (4) efforts taken to minimize the impacts on passengers and protect passenger rights. In conducting this assessment, the Government Accountability Office (GAO) addressed the 10 specific areas of congressional interest related to Secure Flight

outlined in Public Law 108−334. GAO recommends that the Department of Homeland Security (DHS) direct TSA to take several actions to mange risks associated with Secure Flight's development, including (1) finalizing requirements and test plans, privacy and redress requirements, and program cost estimates; and (2) establishing plans to achieve connectivity to obtain data, and performance goals and measures. DHS generally concurred with GAO's findings and recommendations. Highlights: http://www.gao.gov/highlights/d05356high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−356

10. *March 28, Associated Press* — **Gun scare shuts down part of Cincinnati's airport.** Part of Cincinnati's main airport was temporarily shut down Sunday, March 27, after a passenger passed through a security checkpoint with what appeared to be a gun in a carry−on bag, authorities said. Baggage screeners noticed an X−ray image that resembled a gun after the passenger had picked up the bag and left the checkpoint, said Christopher White, a Transportation Security Administration (TSA) spokesperson in Atlanta. Part of Cincinnati/Northern Kentucky International Airport, located 13 miles south of Cincinnati in northern Kentucky, was closed for about two hours as officials searched for the passenger and the weapon. Neither was found, White said. Officials do not believe the passenger boarded a plane because the affected part of the airport was closed and passengers went through security again, he said. White said the TSA is investigating why baggage screeners did not notice the image immediately.
Source: http://www.usatoday.com/news/nation/2005−03−27−gun−scare−air pot_x.htm

11. *March 28, Ironwood Daily Globe (MI)* — **Meeting to address aviation safety and security concerns.** A meeting for area general aviation aircraft owners and pilots will be held April 14 in Bessemer, MI, to address safety and security concerns. It is open to the public. "There have been many concerns for the safety and security of general aviation pilots and aircraft since the tragedy of 9−11," said Joseph Braspenick, manager of the Gogebic−Iron Airport. He pointed to recent media reports regarding the security of general aviation and the awareness that no one can be sure of the extent to which terrorists may be contemplating use of general aviation facilities or aircraft to advance their agenda. "As vulnerabilities within other areas of aviation have been reduced, general aviation may be perceived as a more attractive target, and consequently more vulnerable to misuse by terrorists, both domestic and foreign," Braspenick explained. Inspector Gregory Kranich, aviation security inspector with the Transportation Security Administration, will discuss security issues at the April 14 meeting.
Source: http://www.ironwooddailyglobe.com/0326pilt.htm

12. *March 25, Global Security Newswire* — **District of Columbia's train ban challenge could hinge on 1970 rail safety law.** The District of Columbia's bid to ban rail shipments of chlorine and other toxic gases may hinge on whether the federal government is already doing enough to address the terrorist threat against such shipments, a federal judge said Wednesday, March 23. Presiding over a U.S. District Court hearing on rail operator CSX's request for a preliminary injunction to block implementation of the city law, Judge Emmet Sullivan focused on provisions of the 1970 Federal Rail Safety Act that could be construed to allow legislation like Washington's in cases where the federal government has not addressed the threat in question. The judge opened the hearing by citing January 26 congressional testimony in which former top presidential antiterrorism adviser Richard Falkenrath said "toxic−by−inhalation industrial chemicals" are "acutely vulnerable and almost uniquely dangerous." Attorneys for CSX focused

on the possibility that the Washington law could trigger a series of similar laws across the country, rendering train shipment of hazardous materials all but impossible. District Attorney General's Office lawyer Robert Utiger retorted that future ban attempts in other cities should stand or fall on their own merits.
Source: http://www.govexec.com/dailyfed/0305/032505gsn1.htm

[Return to top]

Postal and Shipping Sector

13. *March 28, Memphis Business Journal* — **FedEx Freight continues U.S. expansion.** FedEx Freight is continuing its aggressive nationwide expansion by opening four new service centers and expanding a fifth facility to meet growing customer demand throughout the U.S. Newly−constructed and recently−opened facilities include state−of−the−art service centers in Des Plaines, IL; Salem, OR; Texarkana, AK; and Springfield, MA. In addition, a supplemental building at the company's Long Island center in West Babylon, NY, will enhance area service and capacity capabilities. These service center openings follow other recent expansions, including the addition of a new center in Gardena, CA, and expanded facilities in Youngstown, OH, and Pocono Summit, PA. FedEx Freight also recently announced plans for a new center near Sacramento, CA, scheduled to open in 2006. FedEx Freight is poised to capitalize on the continued growth of freight transportation. The American Trucking Associations' U.S. Freight Transportation Forecast to 2015 projects total tonnage to increase from 13.2 billion tons in 2003 to 17.4 billion tons in 2015. Revenues, meanwhile, will grow from about $702 billion last year to $1.2 trillion over the next 12 years. The biggest share of this 31% increase in tonnage and 71% growth in revenue will be enjoyed by the trucking industry.
Source: http://memphis.bizjournals.com/memphis/stories/2005/03/28/da ily1.html

14. *March 26, Rochester Democrat and Chronicle (NY)* — **Mail to undergo testing in New York postal facility.** A new system designed to detect biohazardous materials such as anthrax was unveiled Friday, March 26, at the U.S. Postal Service processing and distribution center in Henrietta, NY. The Henrietta processing center handles between 400,000 and 600,000 pieces of mail a day and has about 1,000 employees. The automated detection system analyses the mail as it runs through a machine that cancels and sorts it. The air samples are processed in a machine at each station and tested for anthrax. The test is actually looking for the DNA signature of anthrax. The process takes about 90 minutes. The tests are continuous. The machine can be reconfigured to search for other biological particles. The system tests incoming mail from the district that spans from Rochester to Elmira, NY. That includes letters and postcards dropped in mailboxes, left for mail carriers, or delivered to the post office.
Source: http://www.democratandchronicle.com/apps/pbcs.dll/article?AI D=/20050326/NEWS01/503260310/1002/NEWS

[Return to top]

Agriculture Sector

15.

March 25, Animal and Plant Health Inspection Service — **USDA classifies four Mexican states free of classical swine fever.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its regulations by adding the Mexican states of Campeche, Quintana Roo, Sonora, and Yucatan to the list of regions considered free of classical swine fever (CSF). APHIS has conducted a series of risk evaluations and has determined that these four states have met the requirements for being recognized as free of this disease. This action authorizes the importation into the U.S. of pork, live swine, and swine semen from these regions as a result of the CSF status. However, import of certain commodities may be restricted because of risk from other porcine diseases endemic in Mexico.
Source: http://www.aphis.usda.gov/lpa/news/2005/03/csfimprt_vs.html

[Return to top]

Food Sector

16. *March 27, Bloomberg* — **Japan confirms 16th mad cow case.** Japan's Health Ministry confirmed the country's 16th case of mad−cow disease. A nine−year−old Holstein cow raised in Hokkaido and slaughtered on March 24 tested positive for mad cow, also known as bovine spongiform encephalopathy (BSE), the Ministry of Health, Labor and Welfare said in a statement. Japan has screened every cow slaughtered since September 2001 when it found its first mad cow case.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aVL8rtjWTI0U&refer=asia

17. *March 25, Food Safety and Inspection Service* — **Chicken products recalled.** Day−Lee Foods, Inc., a Santa Fe Springs, CA, firm, is voluntarily recalling approximately 12,500 pounds of chicken products that may be contaminated with Listeria monocytogenes, the Food Safety and Inspection Service (FSIS) announced Friday, March 25. The chicken products were distributed to retail stores in Arizona, California, Nevada, New Mexico, Oregon, and Washington. 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_014_2005_Relea se/index.asp

[Return to top]

Water Sector

18. *March 28, Star Bulletin (HI)* — **Chronic spills raise scrutiny of Honolulu sewers.** Despite spending $726 million on sewer improvement projects in the past 12 years, the city of Honolulu, HI, continues to struggle with a high number of sewage spills. A little over two million gallons of raw sewage spilled between January 1 and Monday, March 21, a rate that closely mirrors the situation during the same period in 2004, when almost two and a half million gallons had been spilled by mid−March. The city faces potential fines of more than one billion dollars from the EPA and state Department of Health's Clean Water Branch, according

to Acting Director of Environmental Services, Eric Takamura. The city is under a 1995 judicial consent decree to improve its sewer system over a 20−year period. In addition to a continuing pattern of sewage spills, the city has failed to meet a number of deadlines for new facilities. Takamura said progress has been made in spill reduction: In 2003 the city sewage system had a total of 183 sewage spills of any size, down from 465 spills in 1994. But the volume of spills has been at least two million gallons a year for five of the last seven years, including every year since 2002.
Source: http://starbulletin.com/2005/03/28/news/index3.html

19. *March 28, Associated Press* — **Dioxin contamination in Michigan may not be fault of only Dow Chemical.** Possible roots of dioxin contamination in the lower Saginaw River and Saginaw Bay in Bay City, MI, may extend beyond Dow Chemical Company, according to an official with Michigan's Department of Environmental Quality (DEQ). Jim Sygo, deputy director of the DEQ, said it is likely that other facilities, including the Bay City Wastewater Treatment Plant and a General Motors Corporation plant are responsible for dioxins as well. In January, Dow Chemical and the DEQ agreed to a series of steps to address dioxin contamination. The focus includes spots in Midland and along the Tittabawassee River, as well as parts of the Saginaw River and Saginaw Bay. Dioxin is a persistent and toxic chemical that was a byproduct of chemical processes that settled into the soil and river sediment along at least 22 miles of Tittabawassee River flood plain downstream from the company's headquarters. Critics worry dioxin exposure could lead to ill health effects, including cancer.
Source: http://www.macombdaily.com/stories/032805/sta_dioxin001.shtm l

[Return to top]

Public Health Sector

20. *March 28, Atlanta Business Chronicle (GA)* — **Georgia to train 150,000 for bioterrorism.** The Georgia Department of Human Resources plans to launch a new bioterrorism preparedness program for as many as 150,000 hospital workers across the state. While public health agencies and hospitals conduct disaster training for health−care workers on a regular basis, this will be the most comprehensive and individualized training ever administered statewide. "This is the first time that it has happened at this level," said Tod Rose, risk communicator for the state's division of public health. "Each health−care worker is going to receive a packet that will give them the tools and training that they need. The plan calls for a training video, as well as printed materials on disaster preparedness and terror awareness, a brochure on the threat of bioterrorism, and a booklet on health−care worker stress. The materials would discuss everything from weapons of mass destruction to facility disaster plans and personal planning.
Source: http://www.bizjournals.com/industries/health_care/hospitals/2005/03/28/atlanta_story4.html

21. *March 28, Agence France Presse* — **Angola's Marburg virus toll rises.** Angola looks set to equal if not break the record of deaths from the Marburg virus with the number of fatalities rising to 122, just one short of the most serious outbreak ever. A severe form of hemorrhagic fever akin to Ebola, the Marburg virus was first identified in 1967. The disease can spread on contact with body fluids such as blood, urine, excrement, vomit, and saliva. It kills around one in four who contract it, and a specific treatment is unknown. Health ministry spokesperson

Carlos Alberto said affected parents or children usually followed each other to the grave. Three−quarters of the deaths have been children under the age of five, according to the World Health Organization (WHO), but the virus has also started to claim adult victims including at least seven medical workers. In former colonial power Portugal a senior health official said authorities were checking on the cause of death of a Portuguese citizen on Saturday, March 26, shortly after his return from Angola. A South African travel clinic on Sunday, March 27, warned travelers planning to go to Angola to stay away from the country "for at least a week."
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=1&u=/afp/20050328/hl_afp/angolahealthvirus_050328104538

22. *March 28, American Medical News* — **Outbreaks of community acquired drug−resistant staph are becoming more common.** Community−associated methicillin resistant Staphylococcus aureus (CA−MRSA) is increasingly being viewed as a public health epidemic. With more cases occurring across the country, primary care physicians are being urged to rethink how they treat it when they see it. "This raises the bar for doctors," says Robert Harrison, infectious disease pediatrician and epidemiologist. "We have to change our thinking about staph, about how we use antibiotics and about how worried we should be when we see staph." MRSA has long been associated with hospitals. But in the 1990s, doctors began seeing unusual patterns of MRSA, particularly among healthy patients without risk factors. "We began to see children from the community with MRSA," said Robert Daum, who is heading several CA−MRSA studies. Daum says the community isolates are very different from the hospital−acquired type. Genetically distinct, CA−MRSA causes a different spectrum of illness, including skin and soft tissue infections that have different antibiotic susceptibility. Often misdiagnosed, CA−MRSA is spreading at an alarming rate. The University of Chicago has seen 25 times the number of cases it did in 1998. At the Texas Children's Hospital in Houston cases doubled from 800 to 1,600 in two years.
Source: http://www.ama−assn.org/amednews/2005/04/04/hlsa0404.htm

23. *March 27, Associated Press* — **North Korea reports outbreak of bird flu.** North Korea acknowledged an outbreak of bird flu for the first time, saying Sunday, March 27, that hundreds of thousands of chickens were killed to prevent its spread, and the disease was not passed on to humans. The outbreaks occurred at a "few chicken farms," and "hundreds of thousands of infected chickens" were burned before burial, the North's official Korean Central News Agency reported. The short report said no breeders who work at the farms were known to have been infected. The report did not say which strain of the virus had been discovered. North Korea said last year it was strengthening quarantine measures against bird flu following the outbreak of the virus in Southeast Asian countries, but it had not previously acknowledged the disease was present in the country. North Korea already suffers from food shortages and relies on outside aid to feed its people, making the outbreak of bird flu a further blow to the isolated nation's food supply.
Source: http://apnews.myway.com/article/20050327/D893C6980.html

24. *March 26, National Post (Canada)* — **Clostridium Difficile spreads in Canada.** Princess Margaret Hospital, in Toronto, Canada, has confirmed the arrival of Montreal, Canada's Clostridium difficile strain, a bacterium responsible for more than a hundred deaths in Quebec last year. The Montreal strain was uncovered in 10 elderly patients at Princess Margaret dating back to last October, with one of those patients succumbing to the infection, said the University

Health Network's Michael Gardam. "Now it's actually crossed the border −− and here it is," said Gardam, director of infection prevention and control at the hospital. "I would be very surprised if we were the only place that had this." C. difficile, which is spread through hand−to−hand contact via feces, causes violent diarrhea that can result in dehydration. It normally occurs in patients using antibiotics, which wipe out healthy bacteria in the bowels and allow C. difficile to thrive. Gardam suggests hospitals connected to Montreal via highways ought to examine whether they too have encountered the virulent strain of the bacterium.
Source: http://www.canada.com/national/nationalpost/news/story.html?id=e2bf8d22−1e2b−4ce2−921f−e4faa39ad0e3

25. *March 21, Kitsap County Department of Emergency Management (WA)* — **Public agencies to conduct bioterrorism exercise.** Public agencies throughout Kitsap, Jefferson, and Clallam counties in Washington will test their skills during a tabletop exercise on Wednesday, March 29 and an Emergency Operations Center exercise on March 30. The tabletop scenario includes people attending a public event and becoming ill with an unknown condition over a period of five days following the event. Public health staff will work throughout the tabletop exercise to discover the agent causing the illness. The tabletop will end with public health officials requesting medications from the state and the opening of the Emergency Operations Centers throughout the region. During the Emergency Operations Center exercise volunteer patients will arrive at area hospitals seeking treatment for their illness. Meanwhile, public health will open an area clinic to dispense medication to volunteers seeking to prevent illness. Law enforcement will investigate the crime while fire/emergency medical services work to transport people to needed medical care.
Source: http://www.kitsapdem.org/news/exerciseinfo.html

26. *March 18, Journal of Infectious Diseases* — **Detection of airborne Severe Acute Respiratory Syndrome coronavirus.** Severe Acute Respiratory syndrome (SARS) is characterized by a risk of nosocomial −− hospital related −− transmission; however, the risk of airborne transmission of SARS is unknown. During the Toronto, Canada, outbreaks of SARS, researchers investigated environmental contamination in SARS units, by employing air sampling and conventional surface swabbing. Two polymerase chain reaction (PCR) positive air samples were obtained from a room occupied by a patient with SARS, indicating the presence of the virus in the air of the room. In addition, several PCR−positive swab samples were recovered from frequently touched surfaces in rooms occupied by patients with SARS (a bed table and a television remote control) and in a nurses' station used by staff (a medication refrigerator door). These data provide the first experimental confirmation of viral aerosol generation by a patient with SARS, indicating the possibility of airborne droplet transmission.
Source: http://www.journals.uchicago.edu/JID/journal/issues/v191n9/33641/brief/33641.abstract.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *March 28, Government Technology* — **Georgia governor announces projects to improve communication between emergency responders.** Georgia Governor Sonny Perdue on Sunday, March 27, announced two projects designed to improve communication between Georgia law enforcement and first responders during emergency situations. The Georgia Emergency Management Agency will coordinate the distribution of Department of Homeland Security (DHS) funding for interoperability projects. The city of Atlanta, Fulton and DeKalb Counties represent one of 50 urban areas in the nation receiving funds from the DHS Urban Area Security Initiative (UASI). With this funding, these local governments have developed a project to enhance radio communications between first responders. The project will combine state of the art equipment with the existing 800 MHz radio system. Another project, funded by the DHS Law Enforcement Terrorism Prevention Program, made $9.7 million available to law enforcement communities throughout Georgia. Utilizing existing radio infrastructure, radio interface technology will be installed in dispatch centers, bridging communications between various officials, and enhancing regional response. The project's goal is to provide agency−to−agency communications to cover 75 percent of the state's population, along with two mobile communication units which can be deployed respond to populations in the remainder of the state that are not covered.
    Source: http://govtech.net/news/news.php?id=93485

[Return to top]

Information Technology and Telecommunications Sector

28. *March 28, IDG News Service* — **Internet service providers and telecommunications companies form alliance to share detailed information on attackers.** Leading global telecommunications companies, Internet service providers (ISPs) and network operators will begin sharing information on Internet attacks as members of a new group called the Fingerprint Sharing Alliance, according to a published statement from the new group. The companies, including EarthLink, Asia Netcom, British Telecommunications and MCI, will share detailed profile information on attacks launched against their networks. Information to be shared will include the sources of attacks. The alliance will make it easier for service providers and network operators to crack down on global Internet attacks more quickly, according to Tom Schuster, president of Arbor Networks, which launched the new alliance. The alliance replaces an ad hoc system of e−mail messages and phone calls that operators of large networks have used to coordinate their response to attacks and threats, Arbor said. The alliance will make it easier for them to cooperate and will lower the threshold that attacks must surpass to get the attention of ISPs. Even attacks on small ISP customers will prompt a response from large infrastructure providers.
    Source: http://www.computerworld.com/managementtopics/outsourcing/isptelecom/story/0,10801,100695,00.html

29. *March 25, Federal Computer Week* — **Study says cybersecurity regulations would be challenging to implement.** Some lawmakers, concerned about the nation’s vulnerability to cybercrime and possible cyberterrorism, are considering whether a larger federal government

role in dealing with the problem is feasible. But a recent study by the Congressional Research Service, which conducts public policy studies, suggests that congressional leaders will face significant challenges if they try to create a regulatory framework to strengthen the nation's cyberdefenses. The report cites two possible models for greater government involvement in cybersecurity. One is the government response to the year 2000 computer crisis. The Securities and Exchange Commission set rules requiring companies to report on their Year 2000 preparedness, and Congress passed liability protections for companies that complied with the rules. The other is a food safety or environmental regulation model in which federal agencies set regulations and use inspectors to monitor compliance. But the report raises questions about the feasibility of either model. Despite being inconclusive, the report lays out several legislative options. The strongest option, according to the report, would be for Congress to provide the Department of Homeland Security or another agency with regulatory authority over cyberspace industries. Report: http://www.usembassy.it/pdf/other/RL32777.pdf
Source: http://www.fcw.com/article88407−03−25−05−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT has identified a recent increase of reported P2P incidents. P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users. As a result, the usage of P2P software may allow for sensitive data or personal information to be leaked from computer systems. Further, P2P may provide a vector for malicious code to be introduced into an enterprise environment.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 22321 (wnn6_Tw), 6346 (gnutella−svc), 1026 (−−−), 139 (netbios−ssn), 80 (www), 1025 (−−−), 1027 (icq), 7674 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *March 28, Herald News (NJ)* — **Bomb call clears mall during children's show.** A phoned−in bomb threat closed the Wayne Hills Mall in Wayne, NJ, for about 90 minutes Saturday, March 26, forcing the evacuation of employees and customers, including about 200 children attending an Easter show. No one was hurt. The mall reopened around 4 p.m., after Wayne police and the

Passaic County Sheriff's Department's K−9 unit searched the building and determined there was no bomb, said Wayne Sgt. Joe Shenekji. According to employees at the Cutting Crew, a mall hair salon, a man phoned at 2:30 p.m. and asked to speak with the salon manager. She and a co−worker reported the call to mall security, who phoned the Wayne Police Department. Within minutes, officers arrived and began telling people to "please leave the building immediately," the manager said. Police did not disclose the nature of the threat to customers, though word spread among mall employees. The threat came as parents and children watched a 2 p.m. showing of a dramatization of a classic children's book.
Source: http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkzNTcmZmdiZWw3Zjd2cWVlRUV5eTY2NzE4MDUmeXJpcnk3ZjcxN2Y3dnFlZUVFeXky

31. *March 28, News−Record (NC)* — **More bomb threats made in Greensboro.** Yet another round of bomb threats were made against Greensboro, NC, establishments, including a hospital. This time, a female caller contacted The Depot on Sunday, March 27, at 3:15 p.m., saying there was a bomb on the property, according to Greensboro police. Kimber Security evacuated the building at 234 E. Washington St. but no suspicious items were found. More than two hours later at 5:43 p.m., a female caller contacted Kindred Hospital saying there was a bomb on the property and it would detonate in 20 minutes. The hospital personnel conducted a search, but did not evacuate the building. Nothing was found. The bomb threats followed threats made to Piedmont Triad International Airport on Friday, March 25, after the airport received its second bomb threat in two days, delaying commercial flights and disrupting holiday travel plans. A threat was also made Friday against the News & Record. A female caller phoned in the threat at 3:20 p.m., saying a bomb was inside the newspaper's East Market Street office.
Source: http://vh10634.moc.gbahn.net/news/now/bombthreats_032805.htm

[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.