Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 09 May 2005

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

Daily Highlights

- Finance Tech reports the United States is the most prone to identify theft among developed countries, because of the vulnerability of commercially available consumer data from credit bureaus and information brokers. (See item 5)
- The Associated Press reports health officials are warning of a previously unknown public health risk: pet hamsters, mice, and rats have sickened up to 30 people in at least 10 states with dangerous multidrug−resistant salmonella bacteria. (See item 18)
- The Associated Press reports researchers at Carnegie Mellon University have been working to develop a "Hazmat Hotzone," a networked, multiplayer simulator that's a virtual disaster drill for dealing with hazardous materials. (See item 21)

Energy Sector

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

1. *May 06, Associated Press* — **Idaho nuclear lab can't explain lost items.** A nuclear reactor research lab in Idaho cannot account for more than 200 missing computers and disk drives that may have contained sensitive information, the Department of Energy's inspector general says. The computers were among 998 items costing $2.2 million dollars that came up missing over the past three years at the federal Idaho National Laboratory, located in Idaho Falls, ID,

according to a new report. Lab officials told investigators that none of the 269 missing computers and disk drives had been authorized to process classified information. However, they acknowledged there was a possibility the devices contained "export controlled" information −− data about nuclear technologies applicable to both civilian and military use that federal laws prohibit being released to foreign nationals.
Inspection Report on "Property Control and Accountability at the Idaho National Laboratory": http://www.ig.doe.gov/pdf/ig−0687.pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/06/AR2005050601258.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 08, Herald and News (OR)* — **Overturned tanker truck spills diesel fuel.** A tanker truck carrying 6,000 gallons of diesel fuel overturned Friday, May 6, on Highway 140 about 14 miles east of Bly, OR. About 2,500 gallons spilled. The highway was closed temporarily. No injuries were reported. The Oregon Department of Environmental Quality (ODOT) was called to the scene, according to ODOT spokesperson Julianne Repman.
Source: http://www.heraldandnews.com/articles/2005/05/08/news/community_news/localbriefs4.txt

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 05, Australian Associated Press* — **Australian banks charge for online banking to combat fraud.** The Australian Federal Police and the Australian banking industry believe online banking fraud is the world's fastest−growing crime, and with increasingly sophisticated security regimes needed to fight cyber crime, consumers are set to pay more to bank online. Three of Australia's five biggest banks −− the Commonwealth Bank, National Australia Bank (NAB) and Westpac −− and a number of smaller financial institutions charge customers Internet fees. Banks say online banking fees are needed to fight cyber criminals. NAB recently announced it would add an additional layer of security by using mobile phone text message technology for customers completing third party payments. There are no fee increases related to NAB's initiative. However, Commonwealth Bank recently increased its online transaction fees in a $100 million next−generation online services and security overhaul. All of the bank's 1.9 million Internet bank users will be using the new system, and paying the extra fees, by the end of June.
Source: http://news.ninemsn.com.au/article.aspx?id=5011

4. *May 05, Magic City Morning Star (ME)* — **Governor signs bill increasing penalties for credit card skimming.** Criminals who skim personal data from credit, debit or charge cards will face additional penalties, under a bill signed into law on Thursday, May 5, by Maine Governor John Elias Baldacci. The legislation, LD 83, "An Act to Prohibit Credit Card Skimming," establishes criminal sanctions for use of two devices −− scanning devices and re−encoders −− if those devices are used to defraud consumers, merchants or the company that issued the card. The law, which received strong support from Maine merchants and the banking industry, creates a new Class D crime of "misuse of a scanning device or encoder." Violations are punishable by up to a year in jail and a $2,000 fine. Electronic credit card skimmers, some the size of small pagers, can be used by thieves in restaurants, stores, gas stations and even locker rooms. The machines collect and store consumer's personal and account information, which can later be downloaded and used to encode other, plain cards. Adding to the problem is that the consumer's card can be returned to the consumer, unchanged, so that the consumer does not even know that the data theft has occurred until unauthorized charges appear on the consumer's monthly statements.
   Source: http://magic−city−news.com/article_3807.shtml

5. *May 05, Finance Tech* — **U.S. most vulnerable to identity theft.** The United States is the most prone to identify theft among developed countries, says a recent report by Boston, MA−based research firm, Aite Group. Identity theft occurs seven times more frequently in the U.S. than in other industrialized regions, like the United Kingdom. Additionally, in continental Western Europe and Japan, identity theft is a non−event. According to Gwenn Bezard, research director at the Aite Group and coauthor of the report, identity theft is a far more common occurrence in the U.S. because of the vulnerability of commercially available consumer data from credit bureaus and information brokers. Financial institutions especially rely on this data to identify their customers, giving scammers a built−in incentive to misuse another person's information, credit cards or financial accounts.
   Report summary: http://www.aitegroup.com/reports/200504043.php
   Source: http://www.financetech.com/news/showArticle.jhtml?articleID= 162600200

[Return to top]

Transportation and Border Security Sector

6. *May 08, Bloomberg* — **Japan may demand rail operators use automatic brakes.** The Japanese government may force train operators to install an automatic braking system that last month could have prevented the country's deadliest railroad disaster in four decades, Transport Minister Kazuo Kitagawa said. A West Japan Railway Co. commuter train that slammed into an apartment building on April 25 killing more than 100 people was speeding to make up for a delay at a station, passengers said on the day. A 23−year−old man with 11 months' experience was driving the train when its carriages careened off the tracks during the morning rush hour in a suburb of Osaka. The government may demand operators use so−called automatic train stop technology, which detects when a train is speeding and applies the brakes, to prevent further such disasters, Kitagawa said May 8, on NHK Television's “Sunday Debate” program. “There's no doubt that speeding was one of the main reasons this accident happened,” he said. “We will consider making it mandatory that ATS or similar technologies are implemented.” West Japan Railway will have to install such safety measures before it can restart the service that crashed,

he added.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=a2_kJz2wrCuQ&refer=asia

7. *May 07, Associated Press* — **Airports in no rush to hire private screeners.** Despite discontent with federal security screeners, airports are not rushing to replace them with private workers. Only two airports −− in Sioux Falls, SD, and Elko, NV −− have applied to the government to switch back to privately employed screeners. And the management at Elko is having second thoughts. "Are the costs going to outweigh the benefits?" asked Cris Jensen, director of the Elko Regional Airport. "We're not sure." Advocates of private screeners had predicted that dozens of airports would jump at the chance to make the switch. Elaine Sanchez, spokesperson for Las Vegas McCarran International Airport, explained why most airports are sticking with the federal screeners: "In a word, liability," she said. Sanchez and other airport officials said they are concerned about potential lawsuits: People might sue an airport where private screeners failed to prevent terrorists from launching an attack.
Source: http://www.usatoday.com/travel/news/2005−05−07−airports−private−screeners_x.htm?POE=TRVISVA

8. *May 07, Associated Press* — **Popular prescreened lanes hit roadblocks at U.S.−Mexico border.** At the world's busiest border crossing, the fast lane has become a slow lane. The program unveiled in San Diego 10 years ago to speed entry for frequent border−crossers who passed a security background check has become clogged −− a victim of its own popularity and an overall spike in drug smuggling. A few months ago, motorists enrolled in SENTRI −− the Secure Electronic Network for Travelers Rapid Inspection −− rarely waited more than 15 minutes to cross from Tijuana, Mexico. Now, they sometimes idle more than an hour −− still better than other lanes at the San Ysidro Port of Entry but much longer than they had hoped for. SENTRI debuted in 1995 at San Diego's Otay Mesa Port of Entry, in El Paso in 1999, and at San Ysidro a year later. The 76,000 passholders paid up to $129 and submitted to a criminal background check. A no−fee pilot program for pedestrians at San Ysidro has enrolled 3,900 people since August. Nexus, a similar system for low−risk travelers in Detroit, Buffalo, N.Y., and other cities bordering Canada, has enrolled 76,000 people. Free And Secured Trade, or FAST −− is a program that has screened 54,000 low−risk truckers for speedier passage across the Canadian and Mexican borders.
Source: http://www.montereyherald.com/mld/montereyherald/news/11591130.htm

9. *May 06, Arizona Republic* — **Homeland chief visits border.** During his first official visit to the U.S.−Mexican border, Department of Homeland Security Secretary Michael Chertoff, on Thursday, May 5, said the government needs more agents and technology to gain control of the Arizona border. "I'll be the first person to acknowledge we've got a lot of work to do," Chertoff said during a news conference at the U.S. Border Patrol station in Douglas, flanked by Arizona Senators John McCain and Jon Kyl, and Governor Janet Napolitano. Homeland Security officials have pledged to gain control of Arizona's 389−mile border, adding 534 Border Patrol agents and doubling the number of aircraft by October. But the state's border with Mexico, separated for miles by little more than a barbed−wire cattle fence, remains the most porous in the nation with more than 360,000 arrests in the past six months. Chertoff called concerns that a terrorist organization could penetrate the southern border "critical," warning that people planning to "wage war against us here in the United States are going to explore every possible

avenue."
Source: http://www.azcentral.com/news/articles/0506chertoff06.html

[Return to top]

Postal and Shipping Sector

10. *May 06, Argus (CA)* — **Sixteen indicted in mail thefts.** A federal grand jury has indicted 16 Bay Area men in connection with theft of mail from a San Francisco, CA, International Airport loading facility, federal prosecutors announced Thursday, May 5. The indictment was handed up Wednesday, May 4, and 13 defendants were arraigned Thursday before U.S. Magistrate Judge Elizabeth LaPorte of San Francisco on charges of conspiracy and theft of U.S. mail. The stolen mail was bound for U.S. military personnel stationed in Okinawa, Japan. A criminal complaint filed earlier claimed that since about November 2003, more than 570 incidents have been reported of mail being received by Okinawa military personnel with contents missing. The estimated losses of the reported missing mail is about $200,000. The defendants worked for Aeroground, a company providing cargo staffing to various airlines.
Source: http://www.insidebayarea.com/argus/localnews/ci_2714917

[Return to top]

Agriculture Sector

11. *May 06, Southeast Farm Press* — **Growers prepare for virus infection in tobacco.** One of several looming uncertainties for Georgia tobacco producers is how severe the incidence of tomato spotted wilt virus (TSWV) will be in 2005. In recent years, the virus has damaged as much as half of the state's crop, and most growers routinely prepare for infestation levels of at least 20 to 30 percent. It's difficult if not impossible to predict the level of TSWV incidence this year, but there are some indicators that might provide clues to growers, says J. Michael Moore, University of Georgia Extension tobacco specialist. "We had a very wet late March and early April. If that caused young thrips to drown or die because of disease, then that would be a good thing." In Georgia, tobacco thrips and Western flower thrips are the main vectors of TSWV in crops. Tobacco thrips −− insects that feed on foliage −− are the major carrier of TSWV in tobacco. "We know from weed surveys conducted in the various counties that the last round of weeds showed a very high level of TSWV," says Moore. "There already is a good presence of the virus in the field. I'd say there's a pretty good chance that we're going to have a significant amount of TSWV."
Source: http://southeastfarmpress.com/news/050605−Tobacco−virus/

12. *May 05, U.S. Department of Agriculture* — **Multi−year strategic plan for the National Animal Identification System.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Thursday, May 5, unveiled a thinking paper and timeline on the National Animal Identification System (NAIS) and called on agriculture producers, leaders, and industry partners to provide feedback. A comprehensive description of system standards will be determined over time through field trials, user experience, and the federal rulemaking process. These documents lay out in more detail projected timelines and potential avenues to achieve system milestones.

For example, these documents propose requiring stakeholders to identify premises and animals according to NAIS standards by January 2008. Requiring full recording of defined animal movements is proposed by January 2009. Administered by USDA's Animal and Plant Health Inspection Service, the NAIS is a cooperative state−federal−industry program being created to track animal movements from birth to death for the purpose of disease tracking. It will be established over time through the integration of three key components: premises identification, animal identification, and animal tracking. Eventually, the NAIS will allow animal health officials to identify all animals and premises that have had contact with a foreign or domestic animal disease of concern within 48 hours of an initial presumptive−positive diagnosis.
NAIS documents: http://www.usda.gov/nais
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/05/0149.xml

13. *May 04, Agricultural Research Service* — **Quarantine facility to help control invasive pests.** U.S. Department of Agriculture (USDA) officials broke ground in Sidney, MT, on Wednesday May 4, for a quarantine−greenhouse complex. The new facility will allow government scientists to develop pesticide−free ways to control invasive plants currently threatening millions of acres of native rangelands across the western U.S. The planned 2,950−square−foot quarantine facility and 4,000−square−foot greenhouse space −− estimated to cost $2.8 million dollars to construct −− will augment the existing Northern Plains Agricultural Research Laboratory (NPARL) in Sidney. Sixteen scientists and 20 support staff will use the future laboratory and greenhouse facilities to study candidate insects and plant pathogens that show promise against hardy rangeland weed invaders. Entomologists and other specialists will be able to rear imported natural enemies of weeds, extract their DNA and evaluate their potential impacts on host and nonhost plants all under one roof. This should expedite the process by which the scientists test and obtain approval to release organisms for use as biological control agents. In addition to sharing research findings with producers and the agricultural industry, NPARL also maintains close ties with regional land−grant universities, which will also benefit from the research made possible by completion of the new facilities.
Source: http://www.ars.usda.gov/is/pr/2005/050504.2.htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

14. *May 05, American Water Works Association* — **Water professionals focus on security.** As National Drinking Water Week continued Thursday, May 5, water professionals acknowledged the important strides made since the terrorist attacks of September 11, 2001, to secure North American water supplies and urged citizens to be aware of unusual activity near water facilities or sources. The American Water Works Association (AWWA) estimates water utilities throughout the United States have spent approximately two billion dollars since 2002 to

upgrade security with better fencing, cameras, locks and other physical improvements. J. Alan Roberson, AWWA director of security and regulatory affairs, said security has become part of the fabric of everyday decisions at water utilities.
Source: http://www.awwa.org/Advocacy/pressroom/pr/index.cfm?ArticleI D=434

[Return to top]

Public Health Sector

15. *May 06, Coloradoan* — **Veterinarians needed to combat public health threats.** Identifying and understanding the mysteries of diseases that jump from animals to humans and threaten millions of people might depend on teams of investigators who understand more than just the human body. It will take medical doctors, public health workers and those trained to care for animals working together to combat threats that most often start with animals and spread to people, say public health officials. Yet the number of veterinarians trained in public health is few. Of the country's 64,867 vets registered with the American Veterinary Medical Association (AVMA) at the end of 2004, only about 1,500 −− just more than two percent −− are listed in public health and preventive medicine. An additional 2,400 vets work in 15 federal agencies, but 50 percent of them are getting ready to retire, according to the AVMA. A bill introduced in Congress by former veterinarian Sen. Wayne Allard calls for $1.5 billion during the next 10 years to expand the size of vet schools and increase the number of vets trained in public health and biomedical research. For the purpose of Allard's bill, public health is defined as areas such as bioterrorism and emergency preparedness, environmental health, food safety and security, regulatory medicine, diagnostic laboratory medicine, and biomedical research.
Source: http://www.coloradoan.com/apps/pbcs.dll/article?AID=/20050506/NEWS01/505060309/1002

16. *May 06, PharmaLive* — **Health and Human Services awards BioShield contract for anthrax vaccine.** The Department of Health and Human Services (HHS) Friday, May 6, awarded a $122.7 million contract to BioPort Corporation of Lansing, MI, for the manufacture and delivery of five million doses of Anthrax Vaccine Adsorbed (AVA), a licensed anthrax vaccine. This supply of AVA anthrax vaccine, which is being purchased under the Project BioShield program, will be placed in the nation's Strategic National Stockpile where it will be available for use in the event of a bioterror anthrax incident. This award represents the third contract under Project BioShield, a new program intended to accelerate the development, purchase, and availability of medical countermeasures for biological, chemical, radiological and nuclear threats.
Source: http://www.pharmalive.com/News/index.cfm?articleid=237251&ca tegoryid=10

17. *May 06, Vietnam News Agency* — **Thailand announces control of bird flu.** Thailand has announced that the bird flu outbreak in Thailand is under control for the first time since last July. The announcement was made on the basis that there have been no reports of any new outbreaks nationwide over the past 21 days from Wednesday, May 4. However, Thailand continues to urge people to be vigilant of the possibility that the virus H5N1 may return and has called for the regular examination every two weeks to be maintained. From January of 2004 to now, bird flu outbreaks in Thailand have claimed 12 lives and 60 million poultry have been culled.

Source: http://www.vnagency.com.vn/NewsA.asp?LANGUAGE_ID=2&CATEGORY_ID=33&NEWS_ID=149851

18. *May 06, Associated Press* — **Dozens contract illness from pets.** Pet hamsters, mice, and rats have sickened up to 30 people in at least 10 states with dangerous multidrug−resistant bacteria, health officials are warning. It is the first known outbreak of salmonella illness tied to such pets and reveals a previously unknown public health risk. The germ is resistant to five drugs spanning several classes of antibiotics. "This is likely an under−representation of how large the problem is," because others who were sick may not have gone to doctors and not all labs do the kind of tests that would detect this germ, said Chris Braden, an epidemiologist at the Centers for Disease Control and Prevention (CDC). The CDC started investigating last summer after Minnesota officials found the unusual infection in a five−year−old boy sickened after playing with and kissing a pet mouse that had severe diarrhea and later died. Tests showed that both had a drug−resistant strain of salmonella, a relative of the germ that causes typhoid fever. The same strain was found in a four−year−old boy hospitalized in South Carolina and in his pet hamster, which also died. Officials then checked PulseNet, a national germ−reporting database, and found 28 other cases from December 2003 to October 2004.
Source: http://news.yahoo.com/s/ap/20050506/ap_on_he_me/sick_from_pets

19. *May 05, National Institutes of Health* — **Scientists reveal how disease bacterium survives inside immune system cell.** New research on a bacterium that can survive encounters with specific immune system cells has strengthened scientists' belief that these plentiful white blood cells, known as neutrophils, dictate whether our immune system will permit or prevent bacterial infections. Scientists analyzed how neutrophils from healthy blood donors respond to Anaplasma phagocytophilum, a tick−borne bacterium that causes granulocytic anaplasmosis in people, dogs, horses, and cows. A. phagocytophilum is carried by the same tick that transmits Lyme disease and was first identified in humans in 1996. Neutrophils, which make up about 60 percent of all white blood cells, are the largest cellular component of the human immune system. Typically, neutrophils ingest and then kill harmful bacteria by producing molecules that are toxic to cells. Once the bacteria are killed, the involved neutrophils self−destruct in a process known as apoptosis. Recent evidence suggests that this process is vital to resolving human infections. "This study has given us a global model of how bacteria can inhibit neutrophil apoptosis," researchers said. "The next step is to look at specific human genes or gene pathways within this model and try to determine which of these molecules help prolong cell life following infection." Information gathered from these and similar studies could help researchers develop therapeutics to treat or prevent bacterial infections.
Source: http://www.nih.gov/news/pr/may2005/niaid−05.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *May 07, The East Oregonian* — **Oregon County to hold annual drill.** The annual Chemical Stockpile Emergency Preparedness Program drill on Tuesday, May 10, in Umatilla County, OR, will involve emergency agencies, hospitals and schools. The exercise will start with a simulated chemical emergency at the Umatilla Chemical Depot and demonstrate emergency preparedness activities throughout the communities surrounding the depot. Sirens will sound and test exercise messages will be displayed, although the precise time of the drill is not announced beforehand. During the early stages of the exercise, Morrow and Umatilla counties in Oregon will test outdoor sirens, highway message reader boards, tone alert radios and send Emergency Alert System test messages to local radio and television stations. Highway advisory radio systems will also be tested. Participants in the drill will include first responders, emergency management personnel and volunteers from all three counties, the states of Washington and Oregon and the Confederated Tribes of the Umatilla Indian Reservation. School children in communities surrounding the depot will be involved in shelter−in−place and evacuation drills earlier in the day, before the actual drill begins. Federal, state and other evaluators will observe and evaluate the drill.
Chemical Stockpile Emergency Preparedness Program Website: http://www.csepp.net/
Source: http://www.eastoregonian.info/main.asp?FromHome=1&TypeID=1&SectionID=69&ArticleID=39148&SubSectionID=375

21. *May 06, Associated Press* — **Pittsburgh university develops Hazmat simulator for firefighters.** For the past three years, professor Jesse Schell and teams of graduate students at Carnegie Mellon University have been working on "Hazmat Hotzone," a networked, multiplayer simulator that's a virtual disaster drill for dealing with hazardous materials. It is designed to fill the gap between classroom or firehouse lectures and mock disasters. A prototype of the simulator has been tested by the Fire Department of New York and the Region 13 Task Force, a group that includes emergency officials from 13 southwestern Pennsylvania counties and Pittsburgh. When it's finished, Carnegie Mellon plans to provide the program free to firefighting training centers nationwide. Instructors set up the virtual disasters by placing victims, chemical leaks and fires throughout a factory, street corner or subway. They can also give the victims symptoms that progress over time. Instructors can also change the scenarios on the fly, adding new chemical leaks, victims or even knocking out one of the firefighters.
Hazmat Hotzone: http://www.etc.cmu.edu/projects/hazmat
Source: http://www.phillyburbs.com/pb−dyn/news/103−05062005−485702.h tml

[Return to top]

Information Technology and Telecommunications Sector

22. *May 06, Security Focus* — **RSA Authentication Agent for Web remote heap buffer overflow vulnerability.** A remote heap−based buffer overflow vulnerability exists in RSA Authentication Agent for Web. This issue is due to a failure of the application to properly bounds check user−supplied input data prior to copying it into a fixed−sized heap buffer memory region. This vulnerability allows remote attackers to execute arbitrary machine code in the context of the vulnerable server application. This reportedly occurs with 'LocalSystem' privileges, allowing the attacker to gain complete control of the targeted computer. Versions 5.0, 5.2, and 5.3 of RSA Authentication Agent for Web are vulnerable to this issue. Users of

affected packages are urged to contact the vendor for further information. Users with valid support contracts with the vendor may be able to locate fixes at: https://knowledge.rsasecurity.com There are currently no vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/13524/discussion/

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: Apple has released a security patch to correct twenty vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service or obtain elevated privileges.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 6881 (bittorrent), 135 (epmap), 41170 (−−−), 53 (domain), 1025 (−−−), 6346 (gnutella−svc), 1026 (−−−), 139 (netbios−ssn), 1433 (ms−sql−s) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

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

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

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

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

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

DHS/IAIP Disclaimer