Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 25 May 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Department of Homeland Security Secretary Chertoff, speaking before the German Marshall Fund and the European Policy Center in Brussels, Belgium, elaborated on his ideas for a technologically−based system of worldwide security envelopes. (See item 16)
- The Michigan Department of Information Technology recently announced the creation of a new Website that provides critical information for cyber security in Michigan government, businesses, and private households. (See item 18)

DHS/IAIP Update *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/IAIP Products &Contact Information

Energy Sector

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

1. *May 24, Associated Press* — **Storm creates service challenge for NStar amid strike.** As a nor'easter bore down on the Boston region Tuesday, May 24, a depleted NStar prepared for potential power outages without the help of 1,900 striking workers. The Boston−based electric and gas utility was keeping an unspecified number of contract workers on alert in case they are needed to help repair overhead lines downed by high winds. NStar was also prepared to shift workers to areas that receive the worst of the nor'easter, which was expected to bring driving rain and strong winds from Tuesday evening into Wednesday. Nearly two−thirds of NStar's workers went on strike May 16 after an old contract expired and talks toward a new agreement collapsed. The utility is relying on managers and outside contractors to continue service to 1.1

million electric customers and 300,000 natural gas customers in eastern and central Massachusetts.
Source: http://www.boston.com/news/local/massachusetts/articles/2005/05/24/storm_creates_service_challenge_for_nstar_amid_strike /

2. *May 13, Government Accountability Office* — **GAO−05−459: Department of Energy: Improved Oversight Could Better Ensure Opportunities for Small Business Subcontracting (Report).** Federal policy requires that small businesses receive the maximum practicable subcontracting opportunity for providing goods and services to large businesses that contract directly with federal agencies. The Department of Energy (DOE) annually directs almost $20 billion to the 34 “facility management contractors” of which $3.3 billion was redirected to small business subcontractors in fiscal year 2004. DOE negotiates annual small business subcontracting goals with individual contractors and monitors their achievements. The Government Accountability Office (GAO) was asked to (1) determine the usefulness of the data that DOE uses to monitor subcontracting performance and (2) discuss the actions that DOE has taken to address any problems with the contractors’ subcontracting efforts. GAO recommends that DOE (1) ensure that facility management contractors are following federal guidelines for reporting subcontracting achievements; (2) for internal management purposes, calculate contractors’ achievements as a percent of the annual contract funding; and (3) issue guidance to clarify oversight responsibilities. In commenting on the report, DOE agreed with ensuring that reporting guidelines are being followed and clarifying oversight responsibilities. DOE disagreed with calculating the achievement data as a percent of contract funding, but GAO believes doing so would improve oversight.
Highlights: http://www.gao.gov/highlights/d05459high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−459

[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

3. *May 24, Associated Press* — **Web infection holds computer files hostage.** Security researchers at Websense Inc., report that hackers have found a way to lock up electronic documents on a target computer and then demand $200 over the Internet to get them back. Websense uncovered the unusual extortion plot when a corporate customer they would not identify fell victim to the infection, which encrypted files that included documents, photographs and spreadsheets. A ransom note left behind included an e−mail address, and the attacker using

the address later demanded $200 for the digital keys to unlock the files. The FBI said the scheme, which appears isolated, was unlike other Internet extortion crimes. FBI spokesperson Paul Bresson said more familiar Internet extortion schemes involve hackers demanding tens of thousands of dollars and threatening to attack commercial Websites. Leading security and antivirus firms this week were updating protective software for companies and consumers to guard against this type of attack, which experts dubbed "ransom−ware." Experts said there were no widespread reports the new threat was spreading, and the Website was already shut down where the infection originally spread. They also said the hacker's demand for payment might be his weakness, since bank transactions can be traced easily.
Websense Advisory: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID 194
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/24/AR2005052400094.html

4. *May 23, Associated Press* — **Hacker may have stolen Social Security numbers from Jackson Community College.** A hacker who broke into the computer system at Jackson Community College in Jackson, MI, may have accessed as many as 8,000 Social Security numbers, the college said Monday, May 23. The hacker broke into the system Wednesday, May 18. College officials are still investigating but say the hacker may have downloaded employee and student passwords. The college has long used Social Security numbers as default passwords for setting up computer accounts. Jim Jones, the college's director of information technology services, said people are encouraged to change their passwords but often continue to use their Social Security numbers.
Source: http://www.freep.com/news/statewire/sw116169_20050523.htm

[Return to top]

Transportation and Border Security Sector

5. *May 24, Washington Post* — **Plane enters restricted Maryland airspace, is diverted.** A twin−engine private plane flew into restricted airspace over Montgomery County, MD, on Monday, May 23, before being intercepted by jet fighters that fired a flare, witnesses and authorities said. The Capitol was not evacuated, but Senate Majority Leader Bill Frist (R−TN) called a recess about the time of the 6 p.m. incident. The airplane, a propeller−driven Cessna that was registered in Canada and was flying from Knoxville, TN, to Gaithersburg, MD, apparently lost its communications after being hit by lightning, according to a spokesperson for the Federal Aviation Administration. Officials did not say how close the plane came to downtown Washington, DC. Two witnesses said it appeared that it was intercepted a few miles north of the center of Wheaton, MD. A Department of Homeland Security spokesperson said there was an apparent failure of the Cessna's transponder, which provides data about the plane and its flight.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/23/AR2005052301694.html?sub=AR

6. *May 24, Associated Press* — **Immigrants die in Arizona desert heat.** A sudden onset of triple−digit heat led to a rash of deaths among illegal immigrants during the weekend in Arizona's deserts, with 12 people reported dead between Friday, May 20, and Monday, May 23. Scores more were saved in nearly 50 rescue operations, a U.S. Border Patrol spokesperson said.

The deaths were scattered along Arizona's border with Mexico, but most were west of Tucson. Under a federal border control initiative, about 200 extra agents have been brought into the region for the summer months. Heat−related deaths have become common in Arizona as immigrants have been pushed into remote and harsher terrain by agents cracking down in other border areas. The state is the busiest illegal entry point on the nation's southern border. The immigrants repeatedly told Border Patrol agents that their smugglers, known as coyotes, had instructed them to "only grab a gallon or two of water. They never said anything about walking for two or three days," Tucson sector spokesperson Luis Garza said.
Source: http://news.yahoo.com/s/ap/20050524/ap_on_re_us/border_death s

7. *May 24, 10News (CA)* — **Banned airport items may cost big bucks.** With today's tightened security, most people know they're not supposed to pack certain items when getting on a plane. If they do forget and get caught with a banned item, they simply hand it over and continue through the gate −− or, maybe not. Thanks to a little known federal safety policy, travelers may literally have to pay the price. Airport officials say they are simply aiming for safer skies. When Jon Zetterlund mistakenly packed a Swiss Army knife in a carry−on, he wasn't surprised when airport security confiscated it. But he was shocked when an official letter arrived a few weeks later, assessing a fine of $250 for bringing a weapon into the sterile environment of the airport. Zetterlund is one of nearly 10,000 passengers fined in the past year for packing banned items. Lauren Stover, the Eastern Regional Public Affairs Supervisor for the Transportation Security Administration says the fines range from $250 to $10,000 depending on the violation. But the penalties are not automatic. "We take a lot of factors into consideration," said Stover. These factors include a person's attitude with screeners, whether a person has tried to conceal the item and how dangerous it is. Zetterlund was fined because of the length of his blade but says he doesn't think he should have been a target at all.
Source: http://www.10news.com/travelgetaways/4524523/detail.html

[Return to top]

Postal and Shipping Sector

8. *May 23, Greenville News (SC)* — **Anthrax−detecting devices coming to mail facilities.** Anthrax−detecting equipment will be installed in Greenville, South Carolina's mail processing site in August 2005, the last of four sites in the state to receive the machinery. Columbia will get the equipment first, followed by Charleston, and Florence facilities in July. All mail processing facilities handle only outgoing mail. The Biohazard Detection System looks for anthrax by sampling air from around envelopes being processed in the facilities. The samples are injected into sterile water, and the mixture in analyzed by a machine that compares any DNA present to the DNA for anthrax. Any positive result triggers an alarm, evacuations and automatic notifications to postal officials. The sample would then be taken to an approved lab to confirm the presence of anthrax. In the event a positive test result is confirmed, employees will receive medications, mail trucks that received mail within two hours of the alarm will be quarantined and the mail inside the facility will be kept until it is determined safe for delivery, officials said.
Source: http://greenvilleonline.com/news/2005/05/23/2005052364921.ht m

[Return to top]

Agriculture Sector

9. *May 24, Dominion Post (New Zealand)* — **Analysts to tally cost of foot−and−mouth disease hoax.** The last veterinarians stationed on Waiheke Island, New Zealand, as a precaution after the foot−and−mouth hoax can now go home, as the incubation period for the disease has passed. A letter claiming the economy−crippling disease had been released on Waiheke was sent to Prime Minister Helen Clark two weeks ago, sparking a biosecurity alert. Police are still looking for the author. With the physical operation all but over, the analysis phase begins, including working out the exact cost of the multimillion−dollar hoax. Analysis could take a month to six weeks. In the analysis, the cost of the foot−and−mouth disease hoax on Waiheke could include indirect costs such as wages for staff from the Agriculture and Forestry Ministry and their contractors, police, and foreign affairs workers who were diverted to efforts to detect any outbreak and to reassure trade partners.
Source: http://www.stuff.co.nz/stuff/0,2106,3290047a7693,00.html

10. *May 24, Ohio State University* — **Researchers find gene that may be at root of potato blight.** Researchers have found a gene they suspect plays an important role in triggering late blight −− the pathogen that causes massive amounts of agricultural damage throughout the world, on the order of billions of dollars each year. Avr3a is the first avirulence gene identified from late blight. Avirulence genes can either facilitate disease or trigger resistance. Avr3a scouts a potato plant on the cellular level to determine whether the plant is a likely victim. “This avirulence gene is kind of like a weapon that triggers a metal detector,” said Sophien Kamoun, an associate professor of plant pathology at Ohio State University. “If you take a gun through the metal detector at an airport, the alarms go off,” he said. “This gene (Avr3a) sends a signal alerting the plant that it is infected by the pathogen.” For decades, controlling this disease has involved regular applications of agrochemicals, Kamoun said. “This study is a big step forward in late blight research. Current strategies for managing late blight in potato and tomato crops are unsustainable and costly. In the U.S. and other developed countries, the chronic use of chemicals to manage late blight reduces the profit margins of farmers and is not always successful."
Source: http://researchnews.osu.edu/archive/tatrblit.htm

11. *May 23, CBC News (Canada)* — **China fights foot−and−mouth disease.** Chinese authorities are reported to have slaughtered at least 2,000 cows as they try to stop the spread of foot−and−mouth disease. The cull has been taking place on dairy farms in two villages in Yanqing district, northwest of Beijing. Police have sealed off roads to the main affected area for the past two weeks, a resident in the town of Jiuxuan said. Residents said many knew the animals were being killed but they didn't know why. An official with China's Office of Animal Husbandry and Veterinary Medicine denied there were any undisclosed cases of foot−and−mouth disease. Earlier this month, China reported outbreaks of foot and mouth in the eastern cities of Tai'an and Wuxi, but none near Beijing in the country's north.
Source: http://www.cbc.ca/storyview/MSN/world/national/2005/05/23/footandmouth050523.html

[Return to top]

Food Sector

12. *May 24, Associated Press* — **Japan moves toward resuming U.S. beef imports.** Japan took another step toward easing a 17−month−old ban on U.S. beef imports Tuesday, May 24, when the government asked food regulators to study the feasibility of partially lifting the prohibition. The Agriculture and Health ministries told the Food Safety Commission to start examining whether it is safe to reopen Japan's market to American beef for the first time since the December 2003 discovery of the first U.S. case of mad cow disease, said Agriculture Ministry official Katsuhiro Saka. The commission recommended earlier this month that the government waive mad cow disease tests for domestic cattle younger than 21 months, seen as a move to lay groundwork toward resumption of imports of beef from younger American cattle. The commission's mad cow panel is expected to start deliberation as early as this week on whether American beef is as safe as Japanese beef, Saka said. Saka did not give any timetable, but Kyodo News agency said the import ban might be lifted as early as summer. Until its ban, Japan was U.S. beef's most lucrative overseas market.
    Source: http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN_4_3802126,00.html

13. *May 23, Information Week* — **Protecting the food chain.** Should tainted food −− whether deliberately contaminated by terrorists or accidentally by bacteria −− make its way into the nation's supermarkets and restaurants, the spreadsheet−based and manual systems that most of the industry's small and midsize companies use to track shipments mean it could be days before affected products are identified. Government regulations that go into effect by the end of next year have more companies implementing new software tools and processes to boost the safety of the food supply chain. In 2004, the Food and Drug Administration finalized section 306 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, or "Track and Trace," that requires most every business in the U.S. food supply chain to keep detailed records on receipt and shipment of goods −− where they come from, who they've been sent to, lot numbers, and more −− and to be able to supply that information four to eight hours after it's requested. Some companies have in place sophisticated enterprise−resource−planning and supply−chain systems that already help them meet the Track and Trace requirements. But as much as 75 percent of companies that touch the food supply chain still are managing their inventory with disconnected spreadsheets and paper documents.
    Source: http://www.securitypipeline.com/news/163700027

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

14. *May 23, Associated Press* — **Transplant patients die from rodent virus.** An organ donor who was exposed to a common rodent virus, possibly from a hamster, passed the disease to four

transplant patients, three of whom died, officials said Monday, May 23. It was believed to be only the second documented case in which the viral infection lymphocytic choriomeningitis virus (LCMV) was transmitted through an organ transplant. The dead were a liver transplant recipient and a double−lung recipient from Massachusetts and a kidney transplant recipient from Rhode Island. They died in late April and early May of LCMV, which is associated with exposure to rodent waste, health officials said. Another Rhode Island patient who received a kidney from the organ donor is recovering. The infection was traced to a female donor from Rhode Island who died of unrelated causes. Officials said that at least one pet in the woman's home, a hamster, tested positive for LCMV. U.S. Centers for Disease Control and Prevention (CDC) investigators were testing the dead hamster to confirm the virus as the cause. "We believe the hamster was the source, but we can't rule out a common house mouse," said CDC spokesperson Dave Daigle. Donated organs are not routinely screened for rodent viruses.
LCMV information: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/lcmv.htm
Source: http://www.cnn.com/2005/HEALTH/05/23/transplant.deaths.ap/in dex.html

15. *May 23, Agency for Healthcare Research and Quality* — **New Web−based tool helps planners inventory resources for public health emergencies.** The U.S. Department of Health and Human Services' Agency for Healthcare Research and Quality (AHRQ) Monday, May 23, released the Emergency Preparedness Resource Inventory, a new Web−based tool to help local, regional, and state planners compile customized inventories of health care and emergency resources. The tool allows communities to assess their regional supply of critical resources, prepare for incident response, estimate gaps, and support future resource investment decisions. The new resource inventory helps first responders figure out where emergency equipment and medicines are located, how much is available, and whom to contact to obtain those resources. The Web−based tool has been pilot tested in an eight county region of rural Pennsylvania. Planners in other areas may download the free software tool from AHRQ's Website and customize the inventory structure to meet their needs.
Emergency Preparedness Resource Inventory software tool: http://www.ahrq.gov/research/epri/
Source: http://www.ahrq.gov/news/press/pr2005/epripr.htm

[Return to top]

Government Sector

16. *May 23, Department of Homeland Security* — **Secretary Chertoff outlines security envelope.** Secretary Chertoff, speaking before the German Marshall Fund and the European Policy Center in Brussels, Belgium, elaborated on his "vision of a technologically−based system of security envelopes which would not require a sacrifice of liberty or privacy in order to promote security, and uphold the civil liberties both Europeans and Americans cherish." He outlined three specific areas to develop a worldwide security envelope. First, develop a systematic approach to screening on both sides of the Atlantic. Second, maximize technology resources. Third, work to connect and network law enforcement authorities to more fully match the resources and abilities of the enemy.
Source: http://www.dhs.gov/dhspublic/interapp/speech/speech_0253.xml

[Return to top]

Emergency Services Sector

17. *May 24, KLFY (LA)* — **St. Landry Parish first responders get new radios.** Every second counts when it comes to saving lives during an emergency and communication is key. But, first responders in St. Landry Parish, LA, do not have the ability to directly talk with each other. Officials say that creates confusion and wastes time. But, that lack of communication is now changing. Monday, May 23, 38 St. Landry Parish agencies −− police and fire departments, ambulance companies, and public works departments −− received 800−megahertz portable radios. Officials say the radios will allow parish agencies to directly speak with each other. Coordinators of this program say this is only the first step. Plans are in the works to give the St. Landry Parish school system access to these radios. Cost is always an issue and organizers of this program say the radios are expensive, roughly $2500 each. Currently, the cost is being taken care of through a grant from the Office of Homeland Security and Emergency Preparedness.
Source: http://www.klfy.com/Global/story.asp?S=3381493

[Return to top]

Information Technology and Telecommunications Sector

18. *May 24, Government Technology* — **Michigan Department of Information Technology releases cyber security Website.** The Michigan Department of Information Technology (MDIT) recently announced the release of a new Website promoting cyber security in Michigan government, businesses and private households. The site provides critical information regarding IT security for work, home, government and business. This Website was developed with Department of Homeland Security grant funds in support of Michigan's security strategies and goals. In addition to educating Michigan citizens on best practices for IT security, this new Website seeks to bolster security for Michigan's businesses. MDIT Director of Enterprise Security Dan Lohrmann, hopes the site will help to improve Michigan's IT Security Arena. He says, "This new Website touches on a broad spectrum of IT security issues. From consumer privacy to corporate best practices and secure Web transactions."
Website: http://www.michigan.gov/cybersecurity
Source: http://www.govtech.net/news/news.php?id=94074

19. *May 24, Federal Trade Commission* — **FTC and partners launch campaign against spam zombies.** The Federal Trade Commission (FTC) and 35 government partners from more than 20 countries have targeted the technology trick used by illegal spammers to tap into consumers' home computers and use them to send millions of pieces of illegal spam. Spammers use hidden software that allows them to hijack consumers' home computers and route spam through them. By routing their emails through "zombie" computers, the spammers are able to hide the true origin of the spam from consumers and make it more difficult for law enforcement to find them. The FTC and its partners on Tuesday, May 24, announced "Operation Spam Zombies," an international campaign to educate Internet Service Providers and other Internet connectivity providers about hijacked, or "zombie" computers that spammers use to flood in−boxes here and abroad. Government agencies around the world who will participate in Operation Spam Zombies will send letters to more than 3,000 ISPs around the world, urging them to employ

protective measures to prevent their customers' computers from being hijacked by spammers.
FTC Website for project: http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm
Source: http://www.ftc.gov/opa/2005/05/zombies.htm

20. *May 23, SecurityFocus* — **PortailPHP ID Parameter SQL injection vulnerability.** PortailPHP is prone to an SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user supplied input before using it in an SQL query. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13708/discussion/

21. *May 23, FrSIRT* — **ZoneLabs Vet engine heap overflow vulnerability.** A critical vulnerability was identified in multiple ZoneLabs products, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to a heap overflow error in the Vet Antivirus engine (VetE.dll) when analyzing the OLE stream and processing malformed VBA macro object headers, which may be exploited by remote attackers to execute arbitrary commands by sending a specially crafted VBA project name record to a vulnerable application. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0597

22. *May 23, SecurityFocus* — **Net−SNMP fixprox insecure temporary file creation vulnerability.** A local insecure temporary file creation vulnerability affects Net−SNMP's fixproc. This issue is due to a failure of the affected utility to securely create temporary files in world writable locations. An attacker may leverage this issue to corrupt, write to or create arbitrary files, as well as execute arbitrary code with the privileges of the user or process running the vulnerable script. This may facilitate privilege escalation. There is no vendor solution at this time.
Source: http://www.securityfocus.com/bid/13715

23. *May 20, Government Accountability Office* — **GAO−05−471: Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (Letter Report).** The Internet protocol (IP) provides the addressing mechanism that defines how and where information moves across interconnected networks. Internet protocol version 4 (IPv4), which is widely used today, may not be able to accommodate the increasing number of global users and devices that are connecting to the Internet. IP version 6 (IPv6) was developed to increase the amount of available IP address space. The Government Accountability Office (GAO) was asked to describe IPv6 and determine the key planning considerations and progress made by the Department of Defense (DoD) and other major agencies to transition to IPv6. GAO recommends, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition, and that agencies act to mitigate near−term IPv6 security risks. DoD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Despite these efforts, challenges remain, including finalizing plans, enforcing policy, and monitoring for unauthorized IPv6 traffic. Unlike DoD, the majority of other major federal agencies reported not yet having initiated key planning efforts for IPv6.
Highlights: http://www.gao.gov/highlights/d05471high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−471

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 reports that a new variant of the Sober worm family, Sober.P may spread by virtue of its offer of free World Cup tickets. The payload of this variant is unknown and it may be another form of spam, like Sober.q. Sober.P has a hidden the source code making it more malicious and may cause a denial−of−service attack. Sober.p creates a time stamp like key, then uses that to generate a URL to a server on one of five different hosting services operating in Germany and Austria.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 27015 (halflife), 6881 (bittorrent), 1026 (−−−), 135 (epmap), 53 (domain), 6346 (gnutella−svc), 139 (netbios−ssn), 80 (www), 1025 (−−−) 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