Office of Intelligence and Analysis
Homeland Security

Homeland Security Assessment

(U) Foreign Travel Threat Assessment: Electronic Communications Vulnerabilities

10 June 2008

(U) Prepared by the Critical Infrastructure Threat Analysis Division. Coordinated with the FBI/Domestic Threats and Technology Cyber Intelligence Unit, the National Cyber Security Division/United States Computer Emergency Readiness Team, and the Office of the National Counterintelligence Executive.

(U) Key Findings

(U//FOUO) Foreign governments routinely target the computers and other electronic devices and media carried by U.S. corporate and government personnel traveling abroad to gather economic, military, and political information. Theft of sensitive information can occur in a foreign country at any point between a traveler's arrival and departure and can continue after returning home without the victim being aware.

(U//FOUO) Use of cell phones, laptops, and personal digital assistants (PDAs) in foreign countries exposes these devices to unauthorized access and theft of data by criminal and foreign government elements. Travelers should assume that they cannot protect electronically stored data and should not transmit sensitive government, personal, or proprietary information on the Internet or through telecommunications equipment.

(U//FOUO) Personal electronic equipment carried abroad is vulnerable to installation of malicious software that can steal or manipulate data well after the traveler returns home. Devices carried overseas should be screened thoroughly upon return for the presence of malicious software.

(U//FOUO) Risks associated with use of electronic media overseas can be reduced through proper handling techniques. The simplest of these is to leave such devices at home. Barring that, protective measures should include using designated "travel" computers, single-use cell phones, and temporary e-mail addresses as well as refraining from communicating with a home organization's information technology systems.

(U) Information Theft

(U//FOUO) Any U.S. citizen traveling abroad is a potential foreign intelligence collection target, but corporate and government leaders are most at risk because of the potentially useful information that they carry. Foreign intelligence services target the full range of U.S. economic, industrial, military, and political interests and emphasize private sector, State and local, and U.S. Government officials as potential sources of information. Many foreign governments control infrastructure to facilitate their intelligence collection efforts. Foreign government-owned telecommunications companies are particularly well postured to collect information from foreign travelers communicating within the country.

— (U//FOUO) Intelligence collection activities and information theft likely will be conducted in a nonthreatening and unobtrusive manner. Victims may not realize they have been targeted until after their information is compromised.

(U) The U.S. Department of State cautions that in certain countries, U.S. citizens should have no reasonable expectation of privacy in private or public locations.

— (U) Hotel rooms, Internet cafes, offices, and public places may be subject to on-site or remote technical monitoring.

— (U) Travelers should assume that all information processed and transmitted on fax machines, foreign computers, or telephones is subject to interception. This vulnerability extends to personal cell phones, laptops, and PDAs brought from the United States that transmit over a foreign country's networks.

— (U) Spy software, which intercepts and transmits information without a user's knowledge, can be implanted in both wired and wireless Internet portals in cafes, hotels, transportation depots, and elsewhere.

— (U) Universal Serial Bus (USB) memory sticks and similar storage devices may become infected with malicious software if used on devices in a foreign country or loaded with malicious software when they are not in the owner's possession. Such storage devices given out as advertising tokens at conferences already may be loaded with malicious software.

— (U) Customs officials in foreign countries regularly inspect laptops and luggage—often without the owners being present—to copy sensitive information.

(U) Vulnerabilities after Returning Home

(U//FOUO) Malicious software surreptitiously installed abroad can become a continuing threat after the traveler returns home and connects an unwittingly compromised electronic device to corporate, government, or personal information systems. Hackers can gain access to sensitive data networks more directly by attacking personal devices than through attacks mounted over the Internet. They can use malicious software to

hijack and control thousands of personal computers at a time through robot networks (botnets). Custom-made viruses can attack corporate and government databases to corrupt or steal data.

(U) Protective Measures

(U//FOUO) The best strategy to protect electronic devices when traveling is to leave them at home. If this is impossible, alternatives include buying a single-use cell phone locally, using a designated "travel" laptop that contains minimal sensitive information, and using temporary Internet e-mail accounts not associated with a corporate or government entity. Even with these strategies, however, travelers should assume that all communications are monitored.

(U//FOUO) When it is necessary to carry and use electronic devices and media abroad, travelers should screen them for viruses before communicating with home networks and conduct a comprehensive scan after returning home.

(U//FOUO) When in transit or separated from a computer or PDA, travelers should keep sensitive and proprietary information on removable storage media such as CD–ROMs, floppy disks, removable hard drives, and USB memory sticks continuously in their possession. Even so, travelers should check these devices for malicious software upon returning home and before connecting to corporate, government, or personal networks.

(U//FOUO) Travelers should use strong passwords on devices and encryption programs for electronic files and e-mails.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to DHS and/or the FBI. The DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Incidents involving cyber related activity or breaches, including loss of Personally Identifiable Information, should be reported to US-CERT at https://forms.us-cert.gov/report/ or emailed to soc@us-cert.gov. For additional information on cyber related topics or to sign up to receive cyber alerts from the US-CERT National Cyber Alert System, visit us-cert.gov.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) **Tracked by:** CRIM-040600-01-05, CRIM-041100-01-05, CRIM-041200-01-05, CYBR-010500-02-06, HSEC-010200-01-05, TERR-010200-01-05