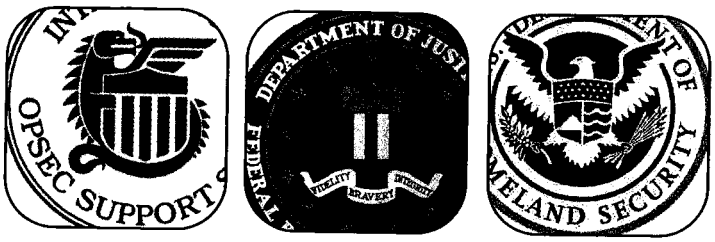


(U) Finding Information and Assistance

Any potential adversary is interested in virtually anything about U.S. military capability, law enforcement capabilities and intentions, political and economic policies, and diplomatic initiatives.

(U) Threat information about a particular operation can be postulated first by employing some common sense concerning who might be interested in critical information about the operation, why they would need the information, and how they might go about collecting it. We should assume that any potential adversary is interested in virtually anything about U.S. military capability, law enforcement capabilities and intentions, political and economic policies, and diplomatic initiatives and that any competitor is interested in anything dealing with economic, trade, and commercial endeavors.

(U) Although threat summaries and intelligence reports can provide an overall picture of the threat, this picture should be tailored to each specific operation or activity. Tailoring the threat picture involves examining both national intelligence sources as well as local sources. Threat information can be obtained through a number of the U.S. government sources, such as the Federal Bureau of Investigation, the Department of Homeland Security, the Defense Intelligence Agency, the Defense Security Service, the Department of Defense Security Institute (DODSI), the Department of Energy (DOE), the Department of State (DOS), and the National Counterintelligence Executive (NCIX). These agencies are responsible for protecting U.S. government and commercial activities, as well as executing counterintelligence programs, security education, and/or threat analysis.

(U) Federal Bureau of Investigation
(U) www.fbi.gov

(U) The FBI has primary responsibility for counterintelligence investigations within the United States and can provide a variety of support services and classified analytical products to government agencies. An integral part of the FBI's counterintelligence efforts is the Awareness of National Security Issues and Response (ANSIR) program. It is the "public voice" of the FBI for espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues. The program is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies. Information is disseminated nationwide via the ANSIR-Email and ANSIR-FAX networks. Each of the FBI's field offices has an ANSIR coordinator and is equipped to provide national security threat and awareness information on a regular basis to corporate recipients within their jurisdiction.

(U) Department of Homeland Security (DHS)
(U) www.dhs.gov

(U) One primary reason for the establishment of the Department of Homeland Security was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure the United States. DHS carries out its mission by focusing on the following elements:

- (U) **Awareness**—Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.
- (U) **Prevention**—Detect, deter and mitigate threats to our homeland.
- (U) **Protection**—Safeguard our people and their freedoms, critical infrastructure, property and the economy of our Nation from acts of terrorism, natural disasters, or other emergencies.
- (U) **Response**—Lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.
- (U) **Recovery**—Lead national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

(U) Defense Intelligence Agency

(U) **www.dia.mil**

(U) DIA is a combat support agency and the senior military component in the United States Intelligence Community. It provides intelligence in support of joint military operations in peacetime, crisis, contingency, and combat; service weapons systems acquisition; and defense policy making. DIA prepares counterintelligence (CI) risk assessments for the DOD and conducts a variety of assessments and studies on the foreign intelligence collection threat. DIA also assesses the threat posed by illegal transfers of high-tech military capabilities to adversaries of the United States.

(U) Defense Security Service

(U) **www.dss.mil**

(U) DSS provides security services to the Department of Defense through the integration of personnel security, industrial security, information systems security, and counterintelligence. Through the integration of security services, combined with intelligence threat data, DSS is uniquely able to facilitate the application of threat-appropriate security countermeasures. A counterintelligence element in DSS is responsible for providing threat data from the intelligence and counterintelligence communities to industry. As the partnership has matured, industry routinely reports security incidents to DSS for joint resolution with management officials. As an added benefit, DSS is able to share this information in a sanitized form in order to enhance the security awareness and training programs for defense industry at large. DSS refers significant incidents involving both industrial and personnel security to the FBI and the military counterintelligence elements if a counterintelligence investigation is believed to be warranted.

(U) Department of Defense Security Institute

(U) **www.dss.mil**

(U) DODSI was disestablished at the end of fiscal year 1998, and its functions were assumed by the DSS Training Office. In December 1998, DODSI became a part of the DSS. As such, it continues to develop and present courses on DOD security countermeasure programs. DODSI conducts instructional courses on industrial, personnel, and information security. Discussion of intelligence collection threats is an inherent part of the training provided by DODSI. They also publish unclassified security awareness publications. The best known of these publications is the Security Awareness Bulletin, which is distributed to 25,000 customers in government and industry. Articles often highlight foreign economic and industrial intelligence efforts, as well as methods to protect against such activities.

(U) Department of Energy Counterintelligence Division

(U) The DOE Counterintelligence Division is responsible for analyzing foreign intelligence collection threats, providing awareness training, and disseminating threat assessments to government and contract organizations. The CI Division publishes classified and unclassified threat assessments, and distributes bulletins and newsletters concerning foreign intelligence threats to DOE activities and facilities. This data can be provided to U.S. government agencies and corporations that have entered Cooperative Research and Development Agreements (CRADAs) with DOE. The DOE Counterintelligence Division can be contacted at (202) 586-5901.

(U) Department of State Bureau of Diplomatic Security

(U) **www.travel.state.gov**

(U) The Bureau of Diplomatic Security (DS) is responsible for protecting the Secretary of State and other senior leaders in the department; ensuring the security of diplomatic facilities overseas and department activities within the United States, conducting counterterrorism and antiterrorism activities; and investigating violations of U.S. passport laws. In support of its mission, DS conducts threat assessments and provides U.S. government and private entities overseas with threat assessment support through its regional security officers. DOS's Overseas Advisory Council (OSAC) is a joint DS and industry venture that cooperates on overseas security problems of mutual concern. An area of growing concern for OSAC is the intelligence collection threat faced by U.S. businesses overseas. OSAC gathers and disseminates threat information to member businesses. To exchange threat information as expeditiously as possible, the OSAC Electronic Bulletin Board (EBB) has been implemented. The EBB provides a means for businesses to exchange information among themselves and with the Department. It also provides a means for the Bureau of Diplomatic Security's Office of Intelligence and Threat Analysis to disseminate threat information. Travel advisories and other pertinent State Department security information is available on their website.

(U) National Counterintelligence Executive (NCIX)

(U) **www.ncix.gov**

(U) The NCIX was established in accordance with Presidential Decision Directive 24, United States Counterintelligence Effectiveness, issued in May 1994. The NCIX coordinates the U.S. government's efforts to identify and counter foreign intelligence threats to U.S. national and economic security. The NCIX conducts analyses of emerging collection threats, and identifies and broadly disseminates information on HUMINT and technical collection methods. As appropriate, the NCIX provides analytical products to private firms, depending on classification and dissemination caveats.

(U) Department of Commerce Bureau of Export Administration

(U) The Bureau of Export Administration has three offices available to counsel businesses and individuals on their obligations under the Export Administration Regulations and assist in determining their licensing requirements. The Bureau of Export Administration also maintains a list of firms and individuals who have been denied export and re-export privileges.

(U) **Exporter Counseling Division (Washington, DC)**
Room 2705 (for mail)
Room 1099 (for visitors)
14th Street and Pennsylvania Ave., N.W.
U.S. Department of Commerce
Washington DC 20230
Phone: (202) 482-4811 Fax: (202) 482-3617

(U) **Western Regional Office (Newport Beach, CA)**
3300 Irvine Avenue, Suite 345
Newport Beach, CA 92660
Phone: (949) 660-0144 Fax: (949) 660-9347

(U) **Western Regional Office (San Jose, CA)**
101 Park Center Plaza, Suite 1001
San Jose, CA 95113
Phone: (408) 998-7402 Fax: (408)998-7470

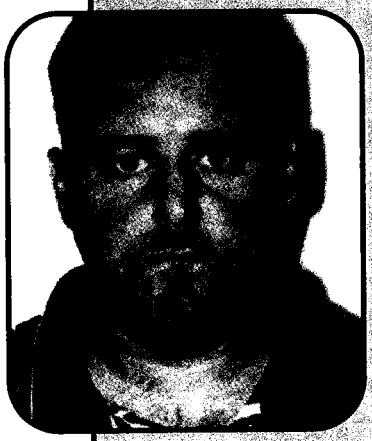
(U) The Interagency OPSEC Support Staff

(U) **www.ioss.gov**

(U) The Interagency OPSEC Support Staff (IOSS) was established in January 1989 to carry out national-level, interagency OPSEC training for executives, program and project managers, and OPSEC specialists; to act as a consultant to the executive departments and agencies in connection with the establishment of OPSEC programs and the conduct of OPSEC surveys; to perform OPSEC-related analyses; and to provide an OPSEC technical staff to the National Security Council. IOSS also conducts the Defensive Information to Counter Espionage (DICE) program to disseminate threat information to DOD contractors. DICE provides current threat information through training programs and briefings provided to DOD contractors and the presentation of threat briefings at selected classified conferences. The IOSS can provide government agencies and their supporting contractors with assistance in the following areas:

- (U) OPSEC training courses
- (U) OPSEC program development
- (U) OPSEC survey support
- (U) OPSEC publications and training materials development

The Brian Regan Case



(U) Brian Regan, a 40-year-old married father of four, owed nearly $117,000 on his credit cards when he wrote a letter in 2001 to Iraqi leader Saddam Hussein offering to sell satellite intelligence that could help Iraq hide anti-aircraft missiles. His asking price was $13 million. The letter was found on a computer at Regan's home. The computer contained a nearly identical letter to Libyan leader Moammar Gadhafi. Regan worked at the National Reconnaissance Office (NRO), which operates the government's spy satellites, first for the Air Force and then as a civilian employee for TRW, a defense contractor.

(U) Using his access to a classified government computer network, Regan looked up numerous top-secret documents, including satellite photos of Iraqi missile sites and confidential documents about Libya's biological warfare program. He printed approximately 20,000 pages of this secret material and then buried portions of the information in a series of caches in state parks in Virginia and Maryland. Regan's idea was to sell the exact location of the sites to a foreign country and let its officials or agents dig up the buried intelligence treasure, thus insulating himself from the danger of being caught while delivering the documents.

(U) Regan was arrested in August 2001 at Dulles International Airport outside Washington while boarding a flight for Zurich, Switzerland. Regan was carrying information with the coded coordinates of Iraqi and Chinese missile sites, the missiles that were stored there, and the date the information was obtained. He also had the addresses of the Chinese and Iraqi embassies in Switzerland and Austria in his wallet and tucked into his right shoe.

(U) Prosecutors sought the death penalty for Regan; but although a jury convicted him in February 2003 of espionage, it decided his crimes did not merit execution. In exchange for Regan's cooperation in debriefing, the government dropped possible charges against his wife and allowed her to collect a portion of his pension. Brian Regan was sentenced to life in prison in March 2003. Although he protested that his sentence was too harsh and that his actions were undertaken just "to protect my wife and children," the judge immediately rejected Regan's plea, observing, **"You have betrayed your nation's trust...You have joined the list of infamous spies."**