National Aeronautics and Space Administration

NASA COUNTERINTELLIGENCE

Spring 2009

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

OSPP Assistant Administrator Stresses Importance of Counterintelligence and Counterterrorism Awareness

by Jack L. Forsythe

The need for counterintelligence and counterterrorism awareness could never be more necessary than it is today. The threats posed by foreign intelligence services and terrorist groups are real and should not be underestimated. It is highly important that all of us take proactive, preventative, and responsible actions to protect ourselves and our Agency from the existing threats posed by foreign intelligence services and those that threaten acts of terrorism.

This newsletter is just one of several initiatives that NASA counterintelligence is involved in to promote awareness and prevention. You will find articles in each newsletter dealing specifically with major counterintelligence and counterterrorism issues affecting our Agency and Government.

I am a strong advocate of our counterintelligence program, and the program provides a needed and valuable service to our Agency. In order to reap the full benefits of this program, it requires all of us at NASA to be educated and aware of the threat and also be able to take the necessary preventative steps to protect ourselves. We continue to call for your involvement and I encourage all of you to read this newsletter and to reach out to your nearest Counterintelligence Office to learn more.

Space Shuttle Spy Case Results in Arrests

A former Boeing engineer, Dongfan "Greg" Chung, and three family members were arrested in February 2008 on allegations that they stole military and aerospace trade secrets on behalf of China. The investigation was led by the FBI and supported by NASA Counterintelligence (CI).

According to the FBI, Chinese aviation officials began sending Chung "tasking" letters as early as 1979. Over the years, the letters directed Chung to collect specific technological information, including data related to the Space Shuttle and various military and civilian aircraft. Between 1985 and 2003, Chung made multiple trips to China to deliver lectures on technology involving the Space Shuttle and other programs. During these trips, Chung allegedly met with officials and agents of the Chinese government, and he is said to have supplied Chinese officials with information such as details of an advanced antenna system for the Space Shuttle. Chung did not report his foreign travel to Boeing as required. The case is currently pending trial in California.

Office of Security and Program Protection

Assistant Administrator
Jack L. Forsythe
202-358-3752
jack.l.forsythe@nasa.gov

Counterintelligence Division

Director
(b) (6), (b) (7)(C)

Operations
(b) (6), (b) (7)(C)

Administrative Assistant
(b) (6), (b) (7)(C)

Counterintelligence Quote

"Foreign collectors don't wait until something is classified—they're targeting it at the R&D phase."

Tim Bereznay, Former Assistant Director, FBI Counterintelligence

Counterintelligence Awareness

Cyber Threat: Supply-Chain Attacks

United States' Government agencies have warned employees about "supply-chain attacks" as one of the latest examples of a new cyber-security threat involving seemingly innocuous hardware devices. The threat involves leaving USB memory sticks (thumb drives) in Government offices that are preloaded with software that can steal information from computer systems. The thumb drives are left where any employee or contractor can find them. If inserted into an Agency computer, the thumb drive can run code that tricks Windows into believing it is really a CD that is set to auto-run, allowing the device to download malware and secretly capture certain information and send the information to an undisclosed computer outside the Agency.

Another method of carrying out these types of attacks occurs when hackers target unsuspecting Government employees attending international and domestic conferences by offering them free USB devices. In addition to containing legitimate information, the drives are also often preloaded with Trojans or other malware that can infect systems with malicious code and/or remove sensitive data such as usernames, passwords, and encryption keys from user systems.

In addition to thumb drives, supply-chain attacks can also be carried out using other forms of hardware, such as flash drives or cards, read/write CDs, memory cards, external hard drives, Personal Digital Assistant (PDA) storage cards, digital picture frames, and cameras. For example, a U.S. aerospace engineer recently visited China and came back to discover his laptop was infected despite the fact he had not connected it to any networks or let it out of his sight. The user later found out that his computer had been infected when it was connected to a digital projector while in China. A significant number of the supply-chain attacks originate in China, which manufactures much of the hardware U.S. and other foreign companies use to produce these attacks.

NASA CI PERSPECTIVE: NASA employees should remain cognizant of developing cyber threats. Motivation behind the attacks can be economic (to commit commercial espionage) or strategic (to support foreign intelligence collections against U.S. technologies associated with developing NASA programs such as Constellation). USB drives found unattended in NASA facilities should be reported to IT security managers immediately. Thumb drives received from vendors should be scanned prior to usage to determine what is on the device. NASA employees should ensure their antivirus software is up-to-date and set to scan for viruses on any new device plugged into their system. Due to a recent Government-wide increase in the number of IT security threats originating from removable media, NASA CI Office policy prohibits the use of personally owned removable media devices in Government-owned systems, to include prohibiting the use of Government-owned removable media devices on personal machines or machines that do not belong to NASA.

Counterintelligence "Indicators"

Counterintelligence indicators are signs that an individual may already be involved in espionage or other improper use of classified or sensitive information. The record of past espionage cases shows that coworkers and supervisors often overlooked or failed to report CI indicators which, had they been reported, would have permitted earlier detection of the spy. Some of the following indicators are clear evidence of improper behavior. Others may well have an innocent explanation but are sufficiently noteworthy that your security office should be informed. If you become aware that any of the following indicators apply to any of your coworkers, you are expected to report the information directly to your security office or NASA Counterintelligence Office.

The NASA Counterintelligence Office will evaluate the information in the context of all other information known about the individual. If your reporting helps stop the commission of an act of espionage against the United States, or terminates an attempt to commit an act of espionage against the U.S., you may be eligible for a reward of up to $500,000. The reward is authorized by an amendment to Title 18, U.S.C., Section 3071, which authorizes the Attorney General to make payment for information on espionage activity in any country that leads to the arrest and conviction of any person(s), or leads to the prevention of an act of espionage against the United States.

Reportable Indicators
Potential Indicators of Motivation

- Disgruntlement with one's employer or the U.S. Government strong enough to make the individual desire revenge.
- Any statement that suggests potential conflicting loyalties that may affect handling of classified or other protected information.
- Active attempt to encourage civilian, military, or contract personnel to violate laws, disobey lawful orders or regulations, or disrupt Government activities.
- Knowing membership in, or attempt to conceal membership in, any group which 1) advocates the use of force or violence to cause political change within the U.S., 2) has been identified as a front group for foreign interests, or 3) advocates loyalty to a foreign interest.
- Repeated statements or actions indicating an abnormal fascination with and strong desire to engage in "spy" work.

NASA COUNTER INTELLIGENCE

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

Spring 2009

Potential Indicators of Information Collection

- Asking others to obtain or facilitate access to classified or sensitive information to which one does not have authorized access.
- Offering extra income from an outside activity to a person with a sensitive job, in an apparent attempt to entice that person into some unspecified illegal activity.
- Having undue curiosity or requests for information about matters not within the scope of the individual's job or need-to-know.
- Conducting unauthorized removal or attempts to remove classified, export-controlled, proprietary, or other protected material from the work area.
- Retention of classified, export-controlled, proprietary, or other sensitive information obtained at a previous employment without the authorization or the knowledge of that employer.
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified, sensitive, or proprietary material which may exceed job requirements
- Taking classified or sensitive but unclassified materials home or on trips, purportedly for work reasons, without proper authorization.
- Working odd hours when others are not in the office without a logical reason, or visiting work areas after normal hours for no logical reason.
- Bringing cameras or recording devices, without approval, into areas storing classified or other protected material.

Potential Indicators of Information Transmittal

- Storing classified or sensitive material at home or any other unauthorized place.
- Taking short trips to foreign countries or within the U.S. to cities with foreign diplomatic facilities for unusual or unexplained reasons or that are inconsistent with one's apparent interests and financial means.
- Excessive and/or unexplained use of e-mail or fax.
- Failure to comply with regulations for reporting foreign contacts or foreign travel or any attempt to conceal foreign travel or to conceal close and continuing contact with a foreigner, particularly a foreign official.
- Foreign travel not reflected in the individual's passport to countries where entries would normally be stamped.
- Maintaining ongoing personal contact, without prior approval, with diplomatic or other representatives from countries with which he/she has ethnic, religious, cultural, or other emotional ties or obligations, or with employees of competing companies in those countries.

Potential Indicators of Illegal Income

- Unexplained affluence or lifestyle inconsistent with known income. Includes sudden purchase of high-value items or unusually frequent personal travel which appears to be beyond known income. Sudden repayment of large debts or loans, indicating sudden reversal of financial difficulties.
- Joking or bragging about working for a foreign intelligence service, or having a mysterious source of income.

Other Potential Indicators

- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance, searching for listening devices or cameras, and leaving "traps" to detect search of the individual's work area or home.
- Any part-time employment or other outside activity that may create a conflict of interest with one's obligation to protect classified or other sensitive information, and that has not been approved by the security office.
- Attempt to conceal any activity covered by one of these CI indicators.

NASA CI PERSPECTIVE: NASA Center Counterintelligence offices will provide CI awareness training to any office, directorate, division, or branch upon request. It is highly encouraged that managers and supervisors schedule annual CI awareness training for their personnel. Contact your local CI Office for more information.

NASA Center CI Offices

NASA Headquarters
(b) (6), (b) (7)(C)

Ames Research Center
(b) (6), (b) (7)(C)

Dryden Flight Research Center
(b) (6), (b) (7)(C)

Glenn Research Center
(b) (6), (b) (7)(C)

Goddard Space Flight Center
(b) (6), (b) (7)(C)

Jet Propulsion Laboratory
(b) (6), (b) (7)(C)

Johnson Space Center
(b) (6), (b) (7)(C)

Kennedy Space Center
(b) (6), (b) (7)(C)

Langley Research Center
(b) (6), (b) (7)(C)

Marshall Space Flight Center
(b) (6), (b) (7)(C)

Stennis Space Center
(b) (6), (b) (7)(C)