460th Space Wing Information Protection Office, Buckley AFB CO

Classified Matters @ Buckley

460th Space Wing Information Protection Office, Buckley AFB CO

Potential Espionage Indicators (PEI): Detecting Actions Outside The Norm

Activities, behavior, or circumstances that may, unless satisfactorily explained, be indicative of potential espionage activity by an individual who may be acting as a witting espionage agent or spy. PEI are observable traits of the Insider Threat. Key to stopping some espionage activities is to be able to recognize a pattern of suspicious activity.

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.

Historically, espionage and terrorism subjects have exhibited one or more of the following indicators:

Foreign Contacts (FCON)

- Unreported FCON
- Attempts to conceal FCON
- First line foreign relatives associated with a foreign government
- Foreign government or military service
- Significant foreign business connections
- Contact with Foreign Intelligence Entities

Foreign Preference or Allegiance

- Maintains dual or multiple citizenships
- Use of a foreign passport for travel
- Use of a foreign national identification card for travel
- Foreign bank accounts for financial interests
- Expresses an affinity, bias, or favor for a foreign nation

Suspicious Foreign Travel (FTVL)

- Frequent or unexplained trips of short duration
- Attempts to conceal FTVL
- Inconsistencies with reported FTVL and passport entries

Security Violations

- Pattern of behavior inconsistent with security policies
- Mishandling classified information
- Misusing automated information systems

INSIDE THIS EDITION:

QUARTERLY DEFINITIONS:

Operations Security (OPSEC):

A process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if info obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

OPSEC Indicator:

Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.

OPSEC Critical Information:

Specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

OPSEC Countermeasure:

Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Summer 2018 Edition

Security Violations (con't)

- Misusing automated information systems
- Removing classified information from the workspace
- Attempting to enter areas not granted access, or 'need-to-know' violations on information systems

Financial Concerns

- Unexplained affluence
- Suspicious financial activity
- Unreasonable financial capabilities
- Personal financial statement (PFS) does not match subject's financial situation

Negative Polygraph

- Polygraph is inconclusive or indicates deception
- Polygraph interview provides information inconsistent with Personnel Security Interview and Personnel Security Investigation

Employment Behaviors

- Long hours
- Working early mornings, late evenings, or weekends
- Frequently alone in the office
- Extensive use of copier/, fax, etc. to transmit or reproduce classified or sensitive info
- Interest in matters outside scope of official duties
- Excessively disgruntled or 'revenge' complex

Exploitable Personal Conduct

- Sexual deviance
- Adultery
- Drug or alcohol abuse
- Excessive gambling

Stand-Alone PEI

- Unofficial contact with Foreign Intelligence Entities
- Membership in subversive groups/orgs

PEI Applied to Real Espionage Case Studies

Case Study: Brian Patrick Regan

- ➢ Former AF intel analyst & NRO contractor
- ➢ Asked Saddam Hussein for $13 million for info about U.S. reconnaissance satellites

Potential Espionage Indicators

- ✓ Deeply in debt
- ✓ Works odd hours
- ✓ Foreign national spouse
- ✓ Late nights in copy room
- ✓ Failure to report foreign travel
- ✓ Alcohol abuse
- ✓ Inappropriately obtained classified information not related to work duties

Outcome

- ✓ Aug 2001 – Arrested on charges of marketing highly classified documents & gathering national defense information
- ✓ Mar 2003 – Sentenced to life in prison for attempting to sell info to Iraq/ China & gathering national security information

Case Study - Noshir Gowadia

- ➢ Principal design engineer of B-2 stealth technology
- ➢ Denied TS/SCI access twice
- ➢ Provided China with technology information valued at hundreds of millions of dollars for a sum of $2M

Potential Espionage Indicators

- ✓ Unexplained affluence
- ✓ Pattern of suspect financial transactions
- ✓ Pattern of suspicious foreign travel location
- ✓ Pattern of suspicious foreign travel frequency

Outcome

✓ Oct 2005 – Arrested on charges of marketing & disclosing classified B-2 stealth technology

✓ Aug 2010 – Convicted of unlawfully exporting technical information, illegally retaining defense information & filing false tax returns. Received a 32-year prison sentence.

Report all suspicious activities to an appropriate security official!

NOTE: *The existence of one or more of the aforementioned PEI does not necessarily mean that a person is engaged in espionage activity. However, the risk that someone may be involved in espionage increases when these indicators are present.*

Buckley AFB is Being Watched

In the past few months, external interest in Buckley AFB has been growing.

This interest has been demonstrated by the recent "First Amendment Audits" occurring outside Buckley. These "audits" show individual activists agitators challenging military and civilian law enforcement with "tests" or "audits" of constitutional First Amendment rights. Individuals conduct First Amendment tests by taking pictures or filming U.S. government or military protected facilities. The audits are an effort to challenge and potentially provoke an aggressive response from military or civilian LE personnel.

Between August 2017 and April 2018, a local Aurora man has conducted three separate audits outside the Mississippi Gate. The audits have had the desired effect and attracted the attention of base and local LE personnel. The picture on the right is a still from one of actual films posted to the internet by the activist.

AFOSI judges these audits do not pose a direct force protection threat, however publicly uploaded footage or photographs of access points, critical infrastructure, security measures, response times, tactics, techniques and procedures (TTPs) used during LE encounters could provide nefarious actors a viable means to overtly conduct pre-operational surveillance.

There are few limitations on photography under U.S. law, in most situations, U.S. citizens and visitors may legally photograph anything they choose so long as their vantage point is located on public or private property (outside of U.S. government jurisdictional boundaries). While it is not advisable to engage or interact with activity you suspect may be related to an audit, base personnel have a responsibility to report suspicious activity inside and outside of Buckley AFB. Personnel are advised to report activity occurring inside or outside the Buckley perimeter such as: photographing or filming of personnel or assets; questioning about duties, deployments, or manning; and unsolicited contact with foreign nationals.

Det 801 AFOSI | May 2018

Protect Your Information When Using Public Wi-Fi

Here's some tips on how you can protect your information when using Public Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Don't use the same password on different websites. It could give someone who gains access to **one** accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when/how your device uses public Wi-Fi.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get VPN account from a VPN service provider.
  - Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, *Force-TLS* and *HTTPS-Everywhere* are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites — look for **https** in the URL to know a site is secure.

Reference: Federal Trade Commission | Mar 2014

Insider Threat Case Study

WHO: Gregory Justice – 50-year-old engineer at Boeing Satellite Systems

WHAT: He worked as a mechanical engineer on the night shift for Boeing since March 2000. He was frustrated with financial problems and inability to get promoted so he attempted to contact Russian intelligence officials to sell sensitive and proprietary software technology and other satellite information. Over the course of a year, he met several times with an undercover FBI agent he thought was a Russian Intelligence Officer and collected $3,500 for the information he passed. He was arrested in July 2016 on charges that he sold proprietary trade secrets such as sensitive satellite information to a man he believed was a Russian spy

INSIDER INDICATORS: He felt unappreciated at work and frustrated that he could not get promoted. His wife suffered from multiple medical problems with mounting bills. His User Activity Monitoring indicated illegal download of information on USB. He sent notes to Russian embassy and consulate. He was enamored with spy thriller. He sent gifts and over $21,000 to an "online paramour" he had never met.

IMPACT: His actions posed an imminent threat to national security. The proprietary satellite information contained technical data covered by the U.S. Munitions List and therefore was subject to controls restricting export from the U.S. under the International Traffic in Arms Regulations. The FBI and AFOSI agents were able to timely and effectively intervene to protect this critical technology

PUNISHMENT: September 18, 2017: He was sentenced to **five years in federal prison** for attempting to commit economic espionage and to send restricted information out of the United States in violation of the Arms Export Control Act and the International Traffic in Arms Regulations

Reference: Defense Security Service's Center for Development of Security Excellence

Foreign Travel Briefing Update

AFOSI offers foreign travel briefings every Wednesday morning at 0900 @ Building 1550. **Now no appointment needed, just show up**. This briefing can help make your trip safer by ensuring you are aware of potential foreign threats and pitfalls. If you have questions about these briefings, contact AFOSI Det 801, at 720 -847-6602.

Remember, all cleared persons in sensitive positions (those with a security clearance) are required to attend this briefing as well as providing their foreign travel itinerary to their unit security manager prior to their departure.

Reference: AFOSI Det 801 & 460 SW/IP

Did You Know?

American Revolutionary leaders used various methods to conceal their diplomatic, military, & personal messages. They even developed something they called a "sympathetic stain" that was used for writing secret communications. The stain required one chemical for writing the message and a second to develop it. The "stain" afforded greater security than the previously-used heat-developing invisible ink.

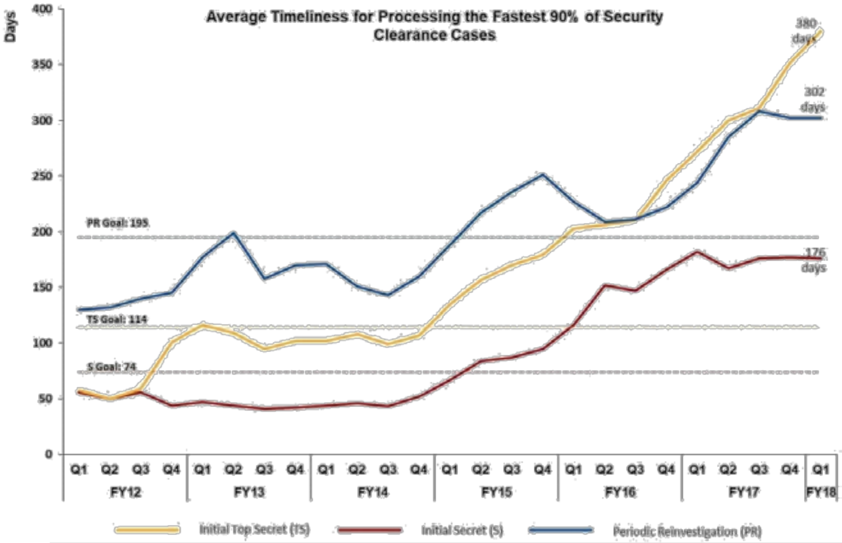
Even though the Patriots took great care to write sensitive messages in invisible ink, or in code or cipher, it is estimated that the British intercepted and decrypted over half of America's secret correspondence during the war.

Reference: cia.gov | Intelligence in the War of Independence | 15 Mar 2007

A Conversation about the Security Clearance Program Changes

As the Trump administration considers another round of major changes to the government wide security clearance program, key officials late last year approved 17 new initiatives they believe will reduce the size of the current backlog. The initiatives are much needed, as recent data from Performance.gov shows how the backlog of pending investigatory work has ebbed and flowed over time and reached a peak of more than **700,000** in 2017 and 2018.

The Performance Accountability Council met from Aug through Dec 2017 to agree on the 17 initiatives.



THE TIME IT TAKES TO RECEIVE AN INITIAL SECRET, INITIAL TOP SECRET & PERIODIC REINVESTIGATION HAS RISEN SHARPLY OVER THE PAST FY. THIS GRAPH SHOWS THE AVERAGE TIME IT TAKES TO PROCESS THE FASTEST MOVING 90 % OF BACKGROUND INVESTIGATIONS.

"Examples include guidance for temporary (interim) authorizations and pre-appointment waiver determinations, expanding the use of video teleconference technology and telephonic reference interviews, clarifying some requirements in the Federal Investigative Standards to improve efficiencies and expediting the deployment of the newly approved SF-85P," the Office of Management and Budget wrote on Performance.gov.Finding improvements to the security and suitability credentialing program is one of the 14 cross-agency priority goals the administration identified in the new President's Management Agenda.

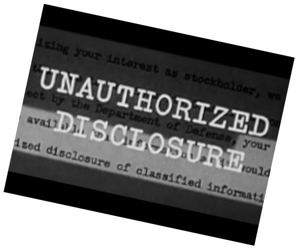
Specifically, the administration has also tasked the Office of Personnel Management and Office of the Director of National Intelligence with developing quality standards for making adjudicative determinations and with options to expand continuous evaluation and vetting programs across all government.

The administration is also interested in finding more opportunities to use shared services on the security clearance program, specifically for an unclassified information exchange, an automated system that determines a position's sensitivity and risk level, and a program that develops background investigation reports.

Expanding the number of federal and contracted investigators is not among the administration's key milestones to improve the security clearance program this year. The National Background Investigations Bureau has hired more investigators in recent years, but it hasn't been able to keep up with demand.

Reference: Federal News Radio | 13 Apr 2018 | Nicole Ogrysko

What Do You Think?

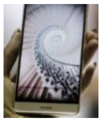


Do you think your annual security training is dull and too long? Well, then check out this 1965 ***DoD security training film*** that lasts 12:42 and covers only just one required security topic, *"Unauthorized Disclosure"*, and you may change your mind. It's not only a blast from the past, but demonstrates that basic commonsense security practices and policies stand the test of time. Enjoy!

Reference: YouTube post by PublicResourceOrg | 30 Jun 11

Security in the News

Pentagon Bans Sale of Chinese-Designed Phones on Military Bases



The Pentagon is cracking down on the sale of Chinese-designed phones and other devices over hacking concerns.

The DoD announced that it is banning the sale of phones made by Chinese-based companies Huawei & ZTE on military bases worldwide over worries that the companies could hack the phones and use them to gather intelligence for the Chinese gov't. More…

Reference: nextgov.com | 2 May 2018 | Caitlin Fairchild

You May Have to Wait 2 Years to Get That Security Clearance

Security clearance reform is back in the news. Congressional testimony and proposed legislation is drawing attention to the problems with the security clearance process, including a backlog of pending cases which reached 725,000.

But there is another number that is much smaller, but much more significant for those awaiting a security clearance determination. More…

Reference: nextgov.com | 3 May 2018 | Lindy Kyzer

Pentagon Innovation Group Aims to Protect Bases from Rogue Drones

The Pentagon's innovation office on Tuesday announced a partnership with the airspace security company Dedrone to improve how the military defends U.S. skies against rogue drones.

The Defense Innovation Unit Experimental awarded Dedrone a $426,000 contract to test the group's drone detection technology at military bases across the country. More…

Reference: nextgov.com | 24 Apr 2018 | Jack Corrigan

Former CIA Case Officer Charged With Conspiracy to Commit Espionage and Retention of National Defense Information

The Justice Department announced today that Jerry Chun Shing Lee, 53, of Hong Kong, was indicted by a federal grand jury sitting in the Eastern District of Virginia with one count of conspiracy to gather or deliver national defense information to aid a foreign government, and two counts of unlawfully retaining documents related to the national defense. More…

Reference: U.S. Department of Justice | 8 May 2018

CIA Contractor Secretly Hoards His Classified Work

The saying goes that memories are all that remain from one's work within the CIA or any other classified environment. That is, of course, unless you are one who likes to keep those memories alive with your own set of Cliff Notes.

That is exactly what occurred at the CIA with Reynaldo B. Regis of Fort Washington, Maryland, from Aug 2006 to Novr 2016. More…

Reference: csoonline.com | 30 May 2018 | Christopher Burgess

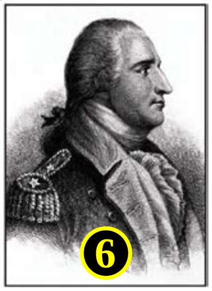
Hackers Find 65 Bugs in the Pentagon's Travel Management System

Ethical hackers exposed more than 60 cybersecurity holes in an enterprise system used by millions of Defense Department employees to organize travel plans. The vulnerabilities within the Defense Travel System were uncovered during the Pentagon's fifth bug bounty program, *Hack the DTS*, which ran from April 1 to April 29. More…

Reference: nextgov.com | 30 May 2018 | Jack Corrigan

Security Puzzler

Can you name the 6 infamous figures below who have leaked sensitive information, spied on, or otherwise betrayed their country? See the answer key for more information on each person!



ANSWER KEY:

1 - Bradley Manning - U.S. Army soldier who leaked 750K classified docs to WikiLeaks (2009) - Sentenced to 35 years (2013) Sentence commuted (2017)

2- Edward Snowden - U.S. gov't contractor who leaked Top Secret NSA info to several media outlets (2013) - Still at large after fleeing to Russia (2018)

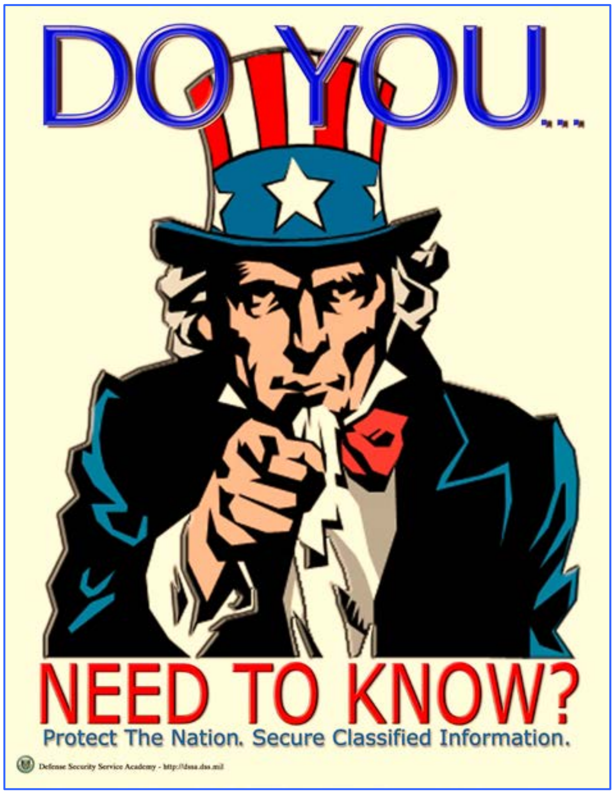
3 - Robert Hanssen - FBI agent who spied for the USSR passing double-agent & signals intelligence info (1985-2001) - Sentenced to life in prison (2002) - Still in prison

4 - Mata Hari - WWI Dutch exotic dancer who had relationship with senior allied officials & was thought to have passed sensitive info the Germans (1914-17) - Executed in Paris aged 41 for spying (1917)

5 - Belle Boyd - Confederate spy who passed Union army strengths/movements (1861-64) - Captured several times & finally deported (1864) - Died aged 56 while touring the U.S. lecturing on her spying conquests (1900)

6 - Benedict Arnold - Renowned U.S. revolutionary war general who masterminded the failed attempt to surrender West Point to the enemy, defected to the British (1790) - Moved to England & died aged 60 (1801)

Security Poster of the Quarter


DO YOU...
NEED TO KNOW?
Protect The Nation. Secure Classified Information.
Defense Security Service Academy - http://dssa.dss.mil

Want some new security posters for your unit? We have hundreds to choose from! Contact Frank Pablo via e-mail or at 847-5086.

Quotable Security Quote

"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees."

Kahlil Gibran (1883 – 1931) - Lebanese-American writer, poet and visual artist.

460th Space Wing Security

Wing Information Protection (460 SW/IP) 460sw.ipo@us.af.mil

Wing Cybersecurity (460 SCS/SCXS) 460scs.scxs.460thwingcybersecurityoffice@us.af.mil

Wing Operations Security (460 SW/XP) 460sw.opsec@us.af.mil

Keeping Buckley's Information Safe!

This newsletter is produced for members of the 460 Space Wing & other Buckley AFB security-supported organizations to increase the general security awareness of contemporary & emerging security issues. We solicit your feedback on how this product can be improved or what content you would like to see added.