Classified Matters @ Buckley

460th Space Wing Information Protection Office, Buckley AFB CO

Operations Security (OPSEC) 101

The History of the Purple OPSEC Dragon

OPSEC as a methodology was developed during the Vietnam War, when Admiral Ulysses Sharp, Commander-in-chief, Pacific, established the "Purple Dragon" team in order to determine how the enemy was able to obtain advanced information on military operations.

The team realized that current counterintelligence and security measures lone were not sufficient. They conceived of and utilized the methodology of "Thinking like the Wolf", or looking at your own organization from an adversarial viewpoint.

They discovered that US forces were unvarying in their tactics and procedures, and were able to make certain predictions based on that knowledge. When developing and recommending corrective actions to their command, they coined the term "Operations Security".

The Post-Vietnam the OPSEC process was refined, culminating in the National Security Decision Directive 298 (NSDD 298) was officially drafted and signed by President Reagan which formed the Interagency OPSEC Support Staff (IOSS).

OPSEC at the "World's Best Space Wing", Buckley AFB

OPSEC is everyone's responsibility. Ideally, the AF uses OPSEC countermeasures to protect its critical information. Failure to properly implement these countermeasures can result in serious injury or death to our personnel; damage to weapons systems, equipment and facilities; loss of sensitive technologies; and mission degradation or failure.

OPSEC is a continuous process and an inherent part of military culture. (AFI 10-701) As great stewards of the OPSEC process we should be very cognizance to integrate OPSEC into the execution of all of our AF activities.

Both the SECAF and the CSAF, as recently at December 2017, stated, "We must relentlessly protect both classified information and any sensitive information that may tip our hand to our enemies as a fighting force. It is not a choice, but a distinct duty we fulfill as guardians of our nation's security."

Additionally, Colonel Endicott's OPSEC Policy memo dated 21 Feb 18 states, "Buckley AFB is involved in an escalating information war with our adversaries who constantly monitor us using a wide range of tactics to gain information to use

INSIDE THIS EDITION:

QUARTERLY DEFINITIONS:

Classified Messaging Incident (CMI):

A higher classification level of data is transferred to a lower classification level system/device via messaging systems, e.g., e-mail, instant messaging, etc.

Classified Spillage:

Occurs whenever classified information or CUI is transferred onto an information system not authorized for the appropriate security level or not having the required CUI protection or access controls. For example, when a user takes a file such as a word document and copies it to removable media (e.g., DVD or CD) from SIPRNET and then the user takes that media and loads the data onto a NIPRNET computer. A classified data spillage is a security violation. A data spillage is not necessarily a CMI.

Negligent Discharge of Classified Info:

Term based on the familiar firearms term "Negligent Discharge" to connote the seriousness of a spillage or unauthorized disclosure of classified information while using an information system.

Fall 2018 Edition

OPSEC 101 (con't)

against us. All individuals on Buckley AFB must be fully engaged in this fight by maintaining I00% shred of waste printer paper, including outdated regulatory guidance".

460 SW Information you MUST protect:

NOTE: Each unit has a Critical Information List (CIL)

Mission Capabilities

- ✓ Info revealing security deficiencies or vulnerabilities
- ✓ Scheduled or unscheduled maintenance trends/downtime
- ✓ Key personnel information / personal info
- ✓ Locations of sensitive / classified areas
- ✓ Emergency action procedures
- ✓ Antiterrorism plans
- ✓ Budget
- ✓ Current or future operations

Manning Status / Readiness

- ✓ Combat readiness / training
- ✓ Medical readiness / immunizations
- ✓ Tactical qualifications
- ✓ Security clearances
- ✓ FPCON / INFOCON posture

Deployment Specifics

- ✓ Location, dates, times, numbers
- ✓ Other equipment going

If you have OPSEC questions, please contact the wing OPSEC Manager 847-5638.

Reference: 460 SW/XP | 21 Aug 2018 | Mr. Ben Roberson

Insider Threat Case Study

WHO: Edward Lin – LCDR U.S. NAVY. 40 year old naturalized citizen from Taiwan. Held a TS/SCI clearance with extensive background in signals intelligence.

WHAT:

- In 2013, Lin claimed to take leave in Virginia when in actuality he traveled to Taiwan to meet with the head of the Taiwanese Navy, Vice Admiral Richard Chen Yeong-kang.
- A tip to FBI in early 2014 indicated that Lin was sharing sensitive information with foreign agents, which led to a joint FBI/NCIS investigation.
- Investigation revealed close and continuous contact with senior official assigned to Taiwan's embassy equivalent in the U.S., Taipei Economic and Cultural Representative Office (TECRO).
- Developed relationship with a female registered foreign agent who worked for the Taiwanese Democratic Progressive Party (DPP)
- September 2015: After providing classified information to an undercover FBI agent in attempt to impress a woman, he was arrested for suspected espionage.

INSIDER INDICATORS:

- Unreported foreign contact with high ranking officials on multiple occasions
- Developed relationships with 2 female Chinese nationals and gave both women several thousand dollars.
- Falsified leave documents concerning a trip to Taiwan and scheduled trip to China.
- Unreported security violation after leaving classified information in an airport terminal
- Life crisis: Divorce

IMPACT: Lin may have shared technical or political classified information pertaining to the Navy's Special Projects Squadron Two mission with a foreign government.

PUNISHMENT: June 2, 2017: Found guilty of wrongly transporting classified material, failing to store classified material as SECRET, wrongly failing to report foreign connections to the security manager, 2 specifications of false official statements, and 2 specifications of communicating defense information. Sentenced to 9 years in prison with 3 years suspended: for making false statements, failing to report foreign contact, mishandling classified information, and disclosing secret information to a foreign citizen. Lin will be dismissed from the Navy, and will forfeit all pay and allowances.

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

AFOSI is Eyeing Threats to Buckley and Beyond

The Denver Metro Area has all the same criminal threats present, and at the same rate, as any major metropolitan area to include crimes against people and property. There is no indication that criminal organizations are specifically targeting military members.

Instead, **local crime** is either personal or targets of opportunity.

- Homegrown violent extremists (HVE) self-radicalize and tend to act alone.
- These factors make them difficult to identify and mitigate.
- AFOSI has one Agent assigned to the Joint Terrorism Task Force (JTTF) in Denver who are currently tracking HVE threats and receiving tips related to HVE indicators on a regular basis.

Aside from suspected HVEs, there are **other U.S.-based threats** in and around Denver.

- Sovereign Citizen groups in Northern Colorado have violated multiple federal statutes and do not recognize federal law as legitimate.

- Indications of White Supremacist Extremist (WSE) groups are present in Denver and seek to recruit for their cause by posting flyers and planning protests near local universities.
- In addition to WSE groups, Black Identity, Anarchist, and Militia Extremism are of concern and continue to be assessed for national security and criminal threats.

Foreign intelligence entities continue to pose a significant threat to Buckley personnel and Defense Contractors who possess a security clearance.

- Targeted collection has been toward specific individuals, companies, facilities, projects, or technologies based on their value to foreign governments and militaries.
- Due to the presence of multiple military installations, critical infrastructure facilities, and private industry involved in emerging technology development, the Denver metro area, and larger I-25 corridor, provide a target-rich environment for Foreign Intelligence Officers.
- Attempts to collect from cleared personnel includes unsolicited requests for information through e-mail or social media, visits to facilities, conference/symposium attendance, and foreign travel.

AFOSI liaises with local, state, and federal law enforcement, as well as private sector security officials to foster communication and reporting. Any personnel experiencing any attempt to make contact or elicit information, whether by known or suspected foreign nationals, should report that information immediately to their unit security representatives and AFOSI.

Reference: Det 801 AFOSI | August 2018

National Cyber Security Awareness Month (NCSAM)

NCSAM is held every October and is a collaborative effort between government and industry with the aim of helping everyone stay safer and more secure online. Follow these tips all -year-round! – to help protect yourself and your information.

Own Your Online Presence

Set the privacy and security settings on websites to your comfort level for information sharing. It's OK to limit how & with whom you share info.

Keep a Clean Machine

Keep all software on internet-connected devices – including PCs, smartphones &tablets – up to date to reduce risk of infection from malware.

Personal Info Is Like Money. Value It. Protect It.

Info about you, such as purchase/location history has value – just like money. Think about who gets that info &how it's collected by apps & websites.

Get 2-Steps Ahead

Use 2-step authentication on accounts where available. Authentication methods can be a text message, a token, or biometric like your fingerprint that provides enhanced account security.

Share with Care

Think before posting about yourself/others online. Consider what a post reveals, who might see it, &how it could be perceived now/in the future.

Reference: stopthinkconnect.com

Historical Information Security: Enigma Lessons

During World War II, Allied mathematicians (as well as linguists, egyptologists, chess players and even crossword compilers), created means of intercepting and deciphering German communications.

Enigma was a sophisticated ciphering machine, securing German communications and was believed to be unhackable. However, cryptanalysts managed to decipher Enigma's messages, giving the Allied forces a significant advantage (Churchill-Eisenhower said 'the definitive advantage') in WW2.

The creation of the "Bomba" cryptanalytic machine enabled the continuous decoding of Enigma's messages. It was the result of incredible scientific and analytical research, but at the same time, it stemmed from some mistakes made by the German operators and analyses of captured Enigmas.

What are some learned information security lessons from the Enigma story?

1. Don't dwell too much on your technical supremacy. The Germans had good reasons to consider Enigma unbreakable, but the Allies' "Bomba" machine which was powerful enough to analyze settings and crack the code. It was a real quantum leap for the technology available back then, so it was impossible for the Germans to predict such a development.

2. One should always look for an opportunity to make the key a bit more sophisticated. This applies to most protection efforts to include passwords. An additional rotor in the Naval Enigma version stalled cryptanalysts for 6 months, and were only able to crack it after recovering one from sunken submarine.

3. Human factor plays an important role, even when dealing with sophisticated systems. The Allies may have never broken Enigma, if not for tiny mistakes by German operators. The Germans also searched for reasons for Allied successes, but never considered that Enigma had been compromised.

4. Information supremacy is a double-edged sword. One of the most challenging tasks for the Allies was using the info obtained from deciphered messages without compromising the fact that it had been cracked. Sometimes special missions were used to masquerade successes, or relevant info was not acted upon, to disguise Enigma's compromise.

We enhance our technologies and increase computing power day by day, but the basic principles of using and protecting information change at a much slower pace, so the Enigma is a useful case study.

Reference: kaspersky.com | World War II information security: Hacking the Enigma | 7 May 2015

Geolocation Capabilities Prohibited in "Operational Areas"

The rapidly evolving market of devices, applications, and services with geolocation capabilities (e.g., fitness trackers, smartphones, tablets, smartwatches, and software apps) presents significant risk to DoD personnel both on and off duty, and to our military operations globally. These capabilities can expose personal info, locations, routines, and numbers of DoD personnel, and potentially create unintended security consequences and increased risk to the joint force and mission.

Effective immediately, DoD personnel are prohibited from using geolocation features on both non-government and government-issued devices, while in locations designated as operational areas (OAs).

In OAs, Combatant Commanders:

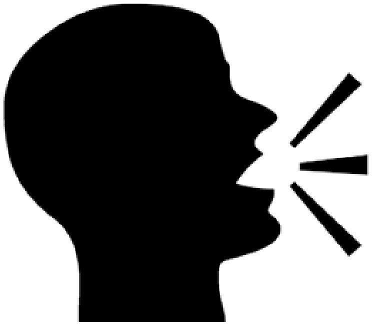
- May authorize the use of geolocation capabilities on non-government device in OAs after conducting a threat-based comprehensive OPSEC survey.
- May authorize the use of geolocation capabilities on government-issued devices in OAs based upon mission necessity, taking into account the potential OPSEC risks.
- Will ensure all personnel under their purview receive appropriate training.

For all other locations, the risks associated with using geolocation capabilities will be assessed. When info derived from these capabilities poses a threat to personnel and operations, commanders:

- Will provide OPSEC training/guidance on the risk and local operating conditions.
- Classify location/operations sensitivity to ensure restrictions are consistently/rationally applied.

Reference: DoD Memo "Use of Geo location-Capable Devices, Applications, and Services | 3 August 2018

Reporting… The Truth or Face Consequences!



The Truth. If you hold national security eligibility (regardless of whether you have access to classified information), you are expected to comply with high standards of conduct. You are expected to self-report certain changes in your personal life or activities which may have potential security clearance ramifications. In other words, don't hide anything, tell the truth when involved with any activity of a security concerns.

AFMAN 16-1405, *Air Force Personnel Security Program,* recently published on1 Aug 18, further expands/clarifies the reporting requirements already contained in other security publications.

Reporting derogatory information is everyone's responsibility. Commanders, supervisors, and coworkers must also report information on a fellow cleared employee.

The Consequences. What happens if reporting does not occur as required?

If a cleared person fails to self-report and the derogatory info ends up being reported by another source, the original security concern becomes more complex. Not only will the DoDCAF have to review the reported information but now has to consider the integrity/honesty issues of not reporting. You can understand how that will not work in the favor of receiving a favorable adjudication

If it is proven that another cleared employee, that includes commanders, supervisors, and coworkers, failed to report the derogatory information, an adverse national security eligibility action may be initiated against the employee who failed to report it.

What's Required to be Reported? Deciding what needs reporting can be confusing, but the below 2 directives provide some clarity.

The first publication is **Security Executive Agent Directive 3,** ***Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position***. This directive establishes the reporting requirements for individuals who have access to classified info or hold a sensitive position.

- Reporting requirements are dependent on the level of security eligibility and/or position sensitivity.
- Individuals must report any planned or actual involvement in any activities prior to participation in such activities or otherwise as soon as possible following the start of their involvement.
- The types of incidents and life events which are reportable to include alcohol/drug treatment, arrests, foreign travel/activities/contacts, media contacts, and financial anomalies.

The second publication is **Security Executive Agent Directive 4**, ***National Security Adjudicative Guidelines***. This directive establishes the single, common adjudicative criteria for individuals who require initial/continued eligibility for access to classified info or eligibility to hold a sensitive position.

- Outlines the 13 adjudicative guidelines used by security clearance adjudicators.
- Each guideline lists behaviors of a security concern & conditions that could mitigate the concerns.
- The guidelines are a useful reference when deciding if derogatory info should be reportable.

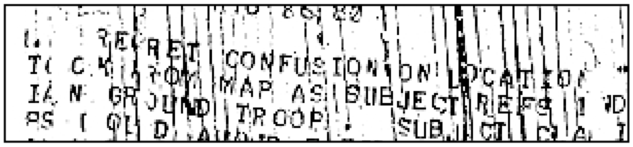
Who Can Receive a Report? Self-reports or reports on other cleared persons can be given to your Commander, Unit Security Manager, or Wing Information Protection.

Contact your unit security manager or the Wing IP Office if you have any questions on reporting.

Reference: 460 SW/IP | 22 Aug 18 | Mr. Chris Johnson

Did You Know?

After the takeover of the U.S. embassy in Tehran in 1979, the Iranians enlisted local carpet weavers who reconstructed numerous strip-cut documents by hand. The Iranians later released the documents in a series of books called "Documents from the US espionage Den". The USG subsequently improved its shredding techniques by adding pulverizing, pulping, & chemical decomposition protocols.



Reference: en.wikipedia.org

Security in the News *(to view the whole article - cut & paste the URL into your browser)*

Air Force Drone, Army Tank Documents for Sale on Dark Web

An Air Force officer's computer was purportedly hacked, compromising a cache of sensitive documents relating to the MQ-9 Reaper, which were then put up for sale on the dark web in June. Also for sale: an Army M1 Abrams tank operation manual.
https://www.airforcetimes.com/news/2018/07/11/air-force-drone-army-tank-documents-for-sale-on-dark-web/

Reference: airforcetimes.com | 11 July 2018 | Kyle Rempfer

Troops Beware: New Security Clearance Rules Could Bite You

More service members could be at risk of losing their security clearances if they don't keep on top of their finances, because of changes in rules for the security clearance process, according to advocates.
https://www.militarytimes.com/pay-benefits/2018/08/30/troops-beware-new-security-clearance-rules-could-bite-you/

Reference: militarytimes.com | 30 Aug 2018 | Karen Jowersr

6 Ways to Tell an Insider Has Gone Rogue

Insiders with legitimate access to enterprise systems and data are responsible for far more data breaches than many might realize. Granted, very often the breaches are accidental or caused by an individual's negligence or failure to follow policy – but when a malicious insider is responsible, the results can be disastrous.
https://www.darkreading.com/vulnerabilities---threats/insider-threats/6-ways-to-tell-an-insider-has-gone-rogue/d/d-id/1332327

Reference: darkreading.com | 179 July 2018 | Jai Vijayan

The Future Airman is a Hacker

Forget the flight suit. The ideal airman of the future has serious tech chops in programming, signals intelligence, or some other core technological capability and isn't afraid to break things. The AF is looking to begin recruiting more intensively for these core competencies, in anticipation of the ways artificial intelligence will change the nature of air war.
https://www.defenseone.com/technology/2018/08/future-airman-hacker/150334/?oref=d-channelriver

Reference: defenseone.com | 7 August 2018 | Patrick Tucker

Government Background Investigator Pleads Guilty In False-Reporting Case

A onetime background investigator accused of falsifying reports to the federal government pleaded guilty Thursday and faces a prison sentence expected to range from 12 to 18 months, according to the U.S. Attorney's Office for the District of Columbia.
https://www.washingtonpost.com/local/public-safety/government-background-investigator-pleads-guilty-in-false-reporting-case/2018/07/19/26dd7aba-8b79-11e8-85ae-511bc1146b0b_story.html?utm_term=.ee6fa1ba9215

Reference: washingtonpost.com | 19 July 2018 | Dan Morse

FBI Director Warns China is America's Most Significant Intelligence Threat

China is engaged in aggressive intelligence operations in the United States, ranging from the recruitment of academics to stealing agricultural secrets from farmers, FBI Director Christopher Wray says.
https://freebeacon.com/national-security/fbi-director-warns-china-americas-significant-intelligence-threat/amp/

Reference: freebeacon.com | 16 July 2018 | Bill Gertz

Security Puzzler

Find **15** security-related words in the below grid. The included words are highlighted yellow throughout this newsletter.

N	Y	J	D	Q	Y	R	R	C	V	P	W	C
K	T	C	E	S	P	O	T	L	O	W	O	F
S	S	S	R	T	N	C	L	E	Q	M	O	O
I	E	B	H	A	E	A	L	A	P	W	U	M
R	N	N	S	E	V	D	D	R	A	G	O	N
Y	S	L	L	R	I	N	O	E	M	K	S	J
G	I	E	A	H	T	M	P	D	T	R	C	D
O	T	G	Y	T	I	R	U	C	E	S	L	S
L	I	J	U	S	S	N	L	C	I	H	E	L
O	V	V	E	T	N	O	P	N	A	Z	A	K
N	I	D	T	V	E	P	I	E	N	M	R	W
H	T	T	L	Z	S	F	N	J	D	B	A	M
C	Y	W	F	U	V	I	G	I	S	P	N	O
E	P	R	O	T	E	C	T	D	G	R	C	W
T	Z	Z	E	L	B	A	T	R	O	P	E	R

Security Poster of the Quarter

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

Happy Halloween!

Quotable Security Quote

"Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge."

Bruce Schneier - American cryptographer, computer security professional, and writer.

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

Air Force Office of Special Investigations (Det 801, AFOSI) AFOSI.AFOSIDet801.CI@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.