Maintaining Your Security Clearance

Maintaining your security clearance is not a passive activity. You must actively execute specific security responsibilities and comply with defined standards of conduct. Ignoring these responsibilities and standards can lead to security clearance revocation and the loss of a job.

Being granted a security clearance means that the government has determined that you are able and willing to safeguard classified national security information, based on your loyalty, character, trustworthiness, and reliability. Once this initial determination has been made, and as long as you have access to classified information, you will fall under the Continuous Evaluation Program (CEP).

By definition, CEP involves the uninterrupted assessment of a person for retention of a granted security clearance. CEP has two complimentary parts – reinvestigation and monitoring.

- **Reinvestigation** means you will be reinvestigated at a given interval depending on the types of duties you perform and clearance level.

- **Monitoring** means that between security investigations, your behavior will continuously be monitored by supervisors, co-workers, security professionals, and yourself for behaviors of a security concern. These safeguards are necessary because situations and behaviors change over time. Past experience shows that some individuals fall into a pattern of unreliable or untrustworthy behavior after being granted their initial clearance.

Because you hold a security clearance, you are expected to comply with high standards of conduct. You are expected to report certain changes in your personal life or activities which may have potential security clearance ramifications. Self-reporting, although not always mandatory, demonstrates personal integrity and is always preferable to someone else discovering and reporting something on you.

What changes or activities might you need to report? Deciding what needs reporting can be confusing, but a new directive has been issued that provides clarity. Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, lists the reportable activities. Your reporting requirements are related to your level of security eligibility and/or position sensitivity. The following are incidents and life events where reporting is expected.

Inside this edition:

- **Maintaining Your Clearance** 1
- **Legalized Pot?** 2
- **Unclassified Info Do’s/Don’ts** 3
- **Foreign Travel Briefings** 3
- **Positive CAC Control** 4
- **New SF-86 Now Out** 4
- **Security in the News** 5
- **Quotable Security Quote** 6
- **Security Puzzler** 6
- **Security Poster** 6

**QUARTERLY SECURITY DEFINITIONS:**

- **Foreign Intelligence Entity:** Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

- **National Security:** Those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, terrorism.

**Fall 2017 Edition**
Maintaining Your Security Clearance

All Persons with a Security Clearance or in a Sensitive Position

- **Foreign Travel** - Unofficial travel must be reported prior to travel and you may be required to receive a defensive security and counterintelligence briefing.

- **Foreign Contacts** - Unofficial contact with a known or suspected foreign intelligence entity. Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact with a foreign national that involves the exchange of personal information.

- **Media Contacts** - Other than for official purposes, where the media seeks access to classified information or other information specifically prohibited by law from disclosure.

- **Other Contacts** - Attempted elicitation, exploitation, black-mail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

- **Arrests** - Any arrest, regardless of whether or not charges were filed.

- **Alcohol and Drug-Related Treatment** - Any treatment.

Additional Reporting for: Secret & Confidential/Non-Critical Sensitive Positions

- **Foreign Activities** - Application for and receipt of foreign citizenship. Application for, possession, or use of a foreign passport or identity card for travel.

- **Financial Anomalies** - Bankruptcy or over 120 days delinquent on any debt.

Additional Reporting for: Top Secret/Critical or Special Sensitive Positions


- **Financial Anomalies** - Including, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.

- **Foreign National Roommate(s)** - Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.

- **Change in Personal Status** - Marital status (marriage, divorce), cohabitation (living in spouse-like relationship, intimate relationship, or becoming engaged).

Contact your unit security manager or the Wing Information Protection Office if you have any questions on CEP. NOTE: Contact the Wing Special Security Officer for SCI reportable activities requirements.

Reference: SEAD 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position | 12 Jun 2017 | 460 SW/IP

---

**Legalized pot? Not for federal employees or military personnel!**

Pot is still illegal for you.

New guidance from the Office of Personnel Management is unambiguous and stern. Federal workforce rules remain unchanged for the roughly 4.1 million federal employees and military personnel across the U.S. The feds still consider marijuana an illegal drug, and possessing or using it is a crime.

“Executive Order 12564, Drug-Free Federal Workplace, mandates that (a) Federal employees are required to refrain from the use of illegal drugs; (b) the use of illegal drugs by Federal employees, whether on or off duty, is contrary to the efficiency of the service; and (c) persons who use illegal drugs are not suitable for Federal employment.

Reference: washingtonpost.com | 27 May 2015 | Lisa Rein
Do’s And Don’ts for Unclassified Information

DO NOT:

• Post sensitive information on social networking sites, such as Facebook, Twitter, YouTube.
• Post sensitive information on public websites.
• Place sensitive information in trash cans or recycle bins.
• Leave sensitive information in vacated offices.
• Leave sensitive information unattended.
• Allow access to those individuals without a “need to know”.
• Place sensitive information on shared drives, unless password protected.

DO:

• Encrypt e-mail when sending sensitive information.
• Review information for sensitivity prior to posting on social networking sites.
• Review information for sensitivity prior to posting on websites.
• Look at information before throwing it in the recycle or trash bins.
• Ensure only unclassified non-sensitive information is discarded in trash and recycle bins.
• Conduct an annual clean out each year.
• Ensure you have enough supplies (burn/shred bags) on hand to discard sensitive information.
• Look behind desk drawers and under desks for information that may have fallen.
• Password protect information placed on shared drives and apply the “need to know” principle.

Sensitive information requires protection! This information may contain the following markings:

• FOUO
• Privacy Act
• Not for Public Release
• Sensitive
• Proprietary
• Limited Distribution

Sensitive information may also be unmarked. Make sure to look at the information prior to throwing it in the garbage or trash bin. Information pertaining to scheduled network outages, VIPs, detailed budget information, refueling schedules or programs may be unclassified but are still sensitive. Before you throw away this information, ask yourself:

“Would a spy, terrorist, or even the media find the information valuable?” If you think they would…..then put it in the shredder!

REMINDER – Buckley AFB has a 100% shred all policy!

Reference: http://www.dodea.edu | 460 SW/XP

Foreign Travel Briefings

Traveling somewhere outside the U.S. soon? AFOSI can help make your trip safer by ensuring you are aware of potential foreign threats and pitfalls.

AFOSI conducts foreign travel pre-briefings every Wednesday morning at 0900 @ Building 1550. To get scheduled, go to the AF Portal and complete the “foreign travel pre-brief” and then contact AFOSI Det 801, at 720-847-6602, to sign up.

This briefing is designed for leisure travel. However, if an Airman needs a briefing for official travel/out-processing, they can contact AFOSI to set that up as well.

Remember to provide your foreign travel itinerary to your unit security manager prior to your departure.

Reference: AFOSI Det 801
Do "You" Have Positive Control of your CAC?

If a Common Access Card (CAC) is found unattended, it should be confiscated and reported through your chain. IAW AFI 36-3026 section 12.2.2., CACs “shall be in the personal custody of the member at all times.” The term “unattended” is defined as out of the user’s line of sight.

Come on, does it really matter if I have Positive Control of my CAC?

It sure does! Here’s a few examples why it matters:

- Say you’re responsible for approving an emergency purchase for your unit, but you left your CAC unattended and now it’s missing. How will that affect your unit?
  - Repairs for a fork lift? Not going to happen.
  - Need immediate medical supplies? Nope, not today.

- Maybe the Wing Commander is waiting for you to send an urgently needed briefing?
  - Well, I’m sure the boss will understand if you lost your CAC.

- Or maybe need to shop at the Commissary (for military members)?
  - That’s OK, who needs food? Right?

These examples illustrate how CAC carelessness can seriously impact you, your family, and the mission.

So please, for everyone’s sake, have some Positive Control!

Reference: Wing Cybersecurity Office

New SF-86 is Now Out

The 2017 SF 86, Questionnaire for National Security Positions, replaced the previous versions of the form on August 27th. Several changes have been made throughout the form to clarify specific questions, but overall the form remains much the same. Additional marital status types include legally recognized civil union and legally recognized domestic partnership, and the ability to identify and provide information on derivative citizenship has also been added. Significant changes include:

- **Section 9** - Addition of Derived US citizen.
- **Section 12** - Where You Went to School - added link to assist determining school address.
- **Section 17** - Marital Status follow-up on Civil Unions/Domestic Partnerships and updates to citizenship of spouses/cohabitants.
- **Section 18** - Relatives have updated citizenship questions.
- **Section 21** - Psychological and Emotional Health - includes vastly different questions than previous versions as a result of a comprehensive review to clarify mental health treatment and to encourage proactive management of mental health conditions to support wellness and recovery. It is important to note that mental health treatment and counseling, in and of itself, is not a reason to determine the suitability or fitness for federal or contract employment, or to determine the eligibility for access to classified information, for holding a sensitive position, or for physical or logical access to federally controlled facilities or information systems.
- **Section 23** - Illegal Use of Drugs and Drug Activity - includes a statement that “illegal use” is in accordance with Federal laws, even though permissible under state laws.
- **Section 26** - Financial Record - added Chapter 12 Bankruptcy.
- **Certification** - added words to affirm that classified information is not provided on the form.

Reference: https://www.dmdc.osd.mil | 460 SW/IP
Security in the News

Number of New Secrets in 2016 at New Low

Last year executive branch agencies created the fewest new national security secrets ever reported, according to an annual report published today by the Information Security Oversight Office (ISOO).

The number of new secrets — or “original classification decisions” — was 39,240 in 2016, an all-time low. The previous low of 46,800 was set in 2014. By comparison, more than 230,000 new secrets a year were being generated a decade ago. Since such record-keeping began in 1980, the total number never dropped below 100,000 until 2012. See 2016 Annual Report to the President, Information Security Oversight Office, July 2017. More...

Reference: fas.org | 20 Jul 2017 | Steven Aftergood

Cyber Command to Become Unified Combatant Command

President Donald Trump announced Aug 18 he plans to make U.S. Cyber Command a unified combatant command on par with U.S. Central Command and other similar independent units in the military that report directly to the secretary of defense.

The move would end the so-called “dual hat” arrangement in which Cyber Command is part of the National Security Agency under Navy Adm. Mike Rogers. “The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries,” Trump said in a statement. More...

Reference: military.com | 18 Aug 2017 | Richard Sisk

Pentagon Now Offering Top Officials Classified Tablets

Top Pentagon officials can now access classified documents and correspondence on tablet computers under a pilot program, the Defense Department said Tuesday. The pilot program, which includes 24 top officials so far, expands on an earlier DOD program that allowed top officials to receive and access classified documents and communications on smartphones.

Pentagon officials could also discuss classified information on the phones if their correspondent was on a similarly classified device. The phones are available at both the secret and top-secret classification levels while the tablets are only cleared for secret communications so far. More...

Reference: nextgov.com | 1 Aug 2017 | Joseph Marks

It's Not Top Secret: The Intelligence Community Encourages Data Sharing

For the 17 agencies that make up the intelligence community, keeping secrets is a priority. But intelligence leaders have learned that if they share information — not hoard it — they can fulfill their missions more effectively.

In the past five years, the IC has been using technology to break down barriers between agencies and to make intelligence data a community asset, says Jennifer Kron, the acting tech chief for the intelligence community. The IC is shifting away from a “castle-and-moat approach”. More...

Reference: fedtechmagazine.com | 3 Aug 2017 | Dan Tynan
Quotable Security Quote

“We should treat personal electronic data with the same care and respect as weapons-grade plutonium - it is dangerous, long-lasting and once it has leaked there's no getting it back.”

Cory Doctorow - blogger, journalist, and science fiction author

Security Poster of the Quarter

DON'T MAKE A GRAVE MISTAKE

PROTECT CLASSIFIED INFORMATION!

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

Security Puzzler

Can you find all the words?

Security Word Search

q q y c p o l i c i e s g k q q p y p t c e c y p q f e k s j s o l t o v o w f i r r a m v h n h s e l p k y e x g l c v c g v r p o l i w p a f o p n l z u r c a d k i o c o m a a t l u a i s n a c p a y u u g v w a j n w p c e e g b s n m e m r h z i k r u h d l t a f y t c a g s l i f w y o i z n i k o f e h p c i e r t t f w e e r q p n j m f t y a g n e f c c d i i e p o t m a h t e p d q y e x a g f b d r e e k g f r t a u w i o i o b a y r k i t a p s a s n z h d e i d j o c d k e y o e n n x q s b p c s t c t r l t v n l j m c j k c i e h p t e a l c b l m r x z i e x o f b g v g e e t j x o c c o o a a f d y r v p e g t j a w a r e n e s s s u k g u d l r z u o q u v i i f i r e w a l l i n d r u o n g s t s a u t h e n t i c a t i o n w v g e p u t e b z i v u b o p r i v a c y q u a o z m d a t m d z r y s u r f r e s p o n s i b l i t y j

encryption
firewall
backup
email
internet
surf
virus
privacy
copyright
login
security
authentication
firewall
authentication
password
account
security
security policies
tailgate
secured
access badge
key
authentication

Security Poster of the Quarter

460th Space Wing Security

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

Wing Cybersecurity (460 SCS/ SCXS)
460sccs.scsxscs.460thwingcybersecurityoffice@us.af.mil

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

Keeping Buckley's Information Safe!

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