Garrison Security Newsletter

Special points of interest:

- **A Focus on OPSEC**
- **Maintaining your security clearance.**
- **Security Training**

Inside this issue:

OPSEC and Internet Safety

Do you have a web log (blog), personal or family web page, or use instant messaging? If so, realize there can be risks associated with using these forms of media.

Is there Really a Risk?

Estimates show that approximately 900 MILLION people have Internet access. Realize not everyone on the Internet is a patriotic American. If you are going to post information out on the worldwide web consider the audience – 900 Million people! Some people use the Internet for disreputable purposes to engage in illegal practices such as identity theft, or even worse, use social engineering tactics to exploit you or your family.

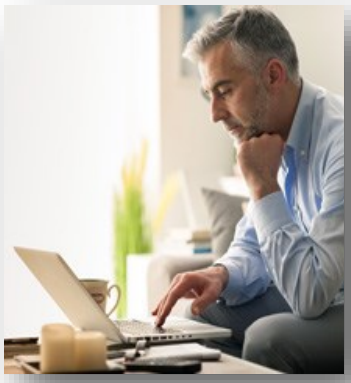
If you are going to use blogs, personal web pages or instant messaging, be sure to keep safety in mind while doing so. Additionally be careful not to divulge sensitive DoD information – information that by nature of your association with DoD the general public would not have access.

OPSEC for DOD Personnel

If you are a DoD employee, remember information you have access to – even though unclassified, can be valuable to adversaries. Be careful not to post sensitive information about DoD activities on your blog or web page. Also take caution about the pictures you post on the Internet from your work environment. These can be valuable to our adversaries so don't help them conduct surveillance by posting photos of DoD facilities.

If you are not sure if the information you wish to post is DoD sensitive information – ask your supervisor, or your security or OPSEC manager.

In many DoD facilities photography is prohibited. Make sure the pictures you post do not violate DoD policy.



Practice good OPSEC at work and at home.

Be courteous when posting information about colleagues and co-workers. Be sure to respect their right to privacy especially when giving names and posting photographs.

Remember, just because DoD information may be unclassified, doesn't mean it's appropriate for the web.

Foreign Travel Reminder

All Civilian Employees, Service Members and Contractors are reminded that when traveling outside the United States they are required to get a travel briefing for the country(s) they will be visiting. This applies for leave and vacation. When traveling outside the United States on TDY they require the travel briefing and theater/country clearance which can take up to 30 days. Depending on security clearance level there may be additional briefings required.

These briefings take very little of your time but ensure that you are aware of any State Department warnings, Combatant Commander concerns, travel restrictions, off limits areas, and any identified crime or disease issues. This can be important for you to protect yourself and your family.

Professional Counseling and Your Security Clearance

Seeking support to address mental health issues demonstrates inner strength and embodies the Warrior Ethos

"All Army personnel should understand that they can obtain counseling services for financial and mental health issues without undue concern of placing their security clearance status in jeopardy"

Using credit cards responsibly won't impact your security clearance

The stress of deployments and the rise of financial difficulties have some Soldiers wondering if their security clearance will be impacted if they seek professional counseling.

The DoD Consolidated Adjudications Facility (DoD CAF) leaders want to ensure Soldiers that the security clearance process is fair, equitable and comprehensive and the Army is taking steps to ensure it remains that way. Leading this effort is the deputy chief of staff, G-2, who is responsible for policy formulation, evaluation, and oversight of intelligence activities for the Department of the Army. This includes policy development and oversight of the security clearance process, to include oversight of the DoD CAF.

The DoD CAF reviews personnel security investigations to grant security clearances for Soldiers, civilian employees and contractor personnel. The DoD CAF uses the national adjudicative guidelines to process security clearance requests. These guidelines outline the standard application of the process, which includes consideration of both favorable and unfavorable information, identify specific concerns, and highlight associated mitigating factors. A bankruptcy or foreclosure will not automatically prevent one from obtaining or maintaining a security clearance, according to G-2 officials. There are many conditions surrounding financial hardships that often mitigate security concerns.

The guideline for financial considerations focuses primarily on individuals who are financially overextended because they may be at risk of engaging in illegal acts to generate funds. For instance, financial guidelines consider "the conditions that resulted in the financial problem were largely beyond the person's control and the individual acted responsibly under the circumstances." Adjudicators identify such conditions as mitigating circumstances.

For example, if an individual did not have financial problems in the past, yet was forced into foreclosure because of a permanent change of station, or PCS move, adjudicators would consider this a mitigating circumstance. However, if the individual has a history of not meeting financial obligations and now forecloses on a home, this would display a pattern of financial irresponsibility that cannot be easily mitigated, officials said.

In addition, Soldiers and civilians should not be forced to weigh the detrimental impacts of a possible loss of a security clearance against the choice of whether or not to seek mental health counseling or treatment, officials said. Many Soldiers expressed an unwillingness to participate in behavioral or psychological health programs based on the perception that a "Yes" answer to the mental health question (Q21) on the U.S. Office of Personnel Management Standard Form 86 Questionnaire for National Security Positions would lead to denial, suspension or possible loss of a security clearance.

The Office of Personnel Management (OPM) conducts the background investigations on Army personnel seeking a security clearance. The OPM ensures that investigations are conducted in a manner compliant with the revised Q21, which excludes the reporting of treatment related to adjustments from service in a military combat environment, such as post traumatic stress disorder, known as PTSD, or mild traumatic brain injury.

Executive Order 12968, Access to Classified Information states mental health counseling in and of itself is not a reason to revoke or deny a security clearance. Seeking support to address mental health issues demonstrates inner strength and embodies the Warrior Ethos, Army leaders have said.

Professional counseling is not a threat to an individual's security clearance; rather it can be a positive factor in the security clearance determination process.

Personally Identifiable Information (PII)

PII is information that identifies, links, relates, is unique to, or describes the individual, such as name, SSN, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information, or any other PII which is linked or linkable to a specified individual. This definition of PII is not anchored to any single category of information or technology. Non-PII can become PII when information is publically available and when combined could identify an individual.

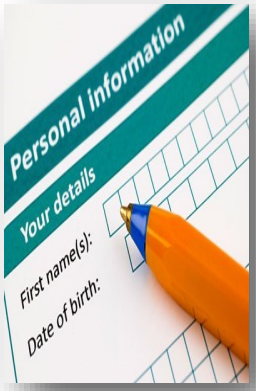
It is your responsibility to:

Ensure that the information entrusted to you in the course of your work is secure and protected. PII must only be accessible to those with an "official need to know."

Minimize the use, display or storage of SSNs and all other PII. The DoD ID number or other unique identifier should be used in place of the SSN whenever possible.

Keep personal information timely, accurate and relevant to the purpose for which it was collected. Delete the information when no longer required.

Immediately notify your supervisor if you suspect or discover that PII has been lost or compromised.



Do you really need to give out your personal information?

Information Security Refresher Training

Security training is required for all Civilian, Military and Contractor personnel. This training mentioned will satisfy requirements listed in AR 380 -5, AR 380-67 and 350-1.

Users should provide the certificate of completion generated at the end of the course to their security manager.

The initial security orientation is required for all military personnel and civilian new hires at their first permanent duty station.

The annual security refresher training is required annually for all military, civilian and contractor personnel.

The annual awareness training, Managing Soldiers and Civilians with Security Clearances is required annually for civilian supervisors, officers and enlisted personnel who manage personnel with clearances/access.

All the training can me accessed by going to AKO/Self Service/My Education/ ALMS/ and "Search" for your specific required training.

The annual security refresher training is required annually for all military, civilian and contractor personnel.

Homeland Security Presidential Directive-12 (HSPD-12)

Homeland Security Presidential Directive 12 (HSPD-12) establishes a government-wide standard of secure and reliable forms of identification for employees (Soldiers and civilians) and eligible contractors for long-term access to controlled facilities and/or information systems.

HSPD-12 compliance requires eligible individuals, who are issued a Personal Identity Verification (PIV) card, have been vetted to a common standard. DOD uses the Common Access Card (CAC) as its PIV card.

HSPD-12 compliance provides baseline level security against potential threats to Army personnel, facilities and IT systems. The CAC is no longer just an ID card. Possessing a CAC signifies the individual has been vetted to a common standard and does not create unacceptable risk.

If your organization requires a contractor to have access to the installation on a reoccurring basis and access to the network please contact the Garrison Security Office for assistance.

Common Access Card (CAC)

GARRISON SECURITY OFFICE

290 Grant Ave
Building 77
Fort Leavenworth, KS 66027

Garrison Security Manager
Phone: 913-684-1752

Garrison Security Specialist
913-684-1712

The Garrison Security Office in located in the Garrison HQ building, #77. We provide support to all Garrison and non-mission government, military, and contractor personnel on Fort Leavenworth. The Combined Arms Center (CAC) G2 provides security support for all other units/ agencies. Garrison security services include processing security clearance investigation requests, including processing and submitting security clearance reinvestigations for personnel with existing security clearances. The Commander Designated Entity (CDE) office located in The Resiliency Center, Building 198, which is overseen by the Garrison Security Office delivers similar serves to all personnel who provide child care services on Fort Leavenworth. The primary responsibility of the CDE is to ensure background checks are conducted on the covered child services population.

In addition to the above services we provide information and industrial security oversight to all units under our purview. These include processing Homeland Security Presidential Directive 12 (HSPD-12) investigations for contractor personal requiring access to both the installation and the network. A priority for us is providing security training to agency security managers and unit S2 personnel. This includes offering staff assistance visits, and support for Organization Inspection Programs. If your organization would like for the Garrison Security Office to provide a staff assistance visit in order to ensure you are meeting all security requirements, feel free to contact our office.

The Garrison Security Office can provide fingerprint services for all individuals who fall within our areas of responsibility. We are only able to provide fingerprint services for security clearance or suitability investigation purposes.

If you or your organization require security support or assistant please do not hesitate to contact us. Our office hours are 0800-1630.

Spy Stories

Julius and Ethel Rosenberg were arrested in 1950 for espionage thought to date back to 1940. They were most famous for giving the Soviet Union atomic secrets, specifically the design for the plutonium bomb dropped on Nagasaki.

The spy ring Julius operated was also responsible for giving the Soviets proximity fuses and radar tubes, two technologies key to effective air defenses which would have played a large part if the Cold War had ever turned hot.

The Trial of Julius and Ethel Rosenberg

Documents from the Venona Project have shown that Ethel may not have been involved. Her brother, who was caught before the Rosenbergs and testified against both of them, later said that Ethel was not part of the ring. Julius and Ethel were both executed in 1953 after a controversial trial. The trial was called a sham, especially the case against Ethel Rosenberg.

It was so hotly contested, it soured America's relationship with France.