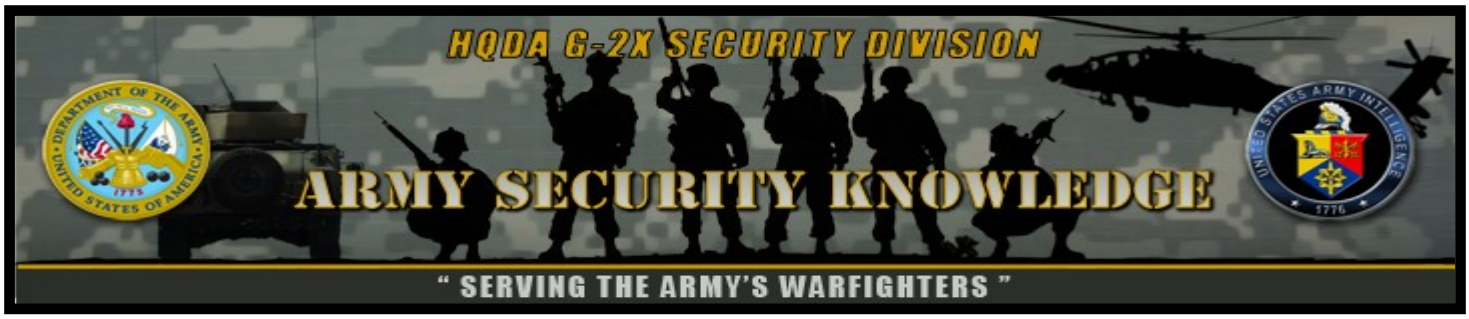


Director's Message

Hello again Army Brethren,

This is the second edition of our G-2 Security Newsletter. This newsletter presents many critical issues facing the Army security community today. The articles on psychological and financial conditions and their affect on the security clearance process are especially relevant to all Army personnel. They tackle the negative perceptions often associated with those seeking mental health and financial counseling.

In support of the Mental Health Campaign Plan, the G-2 will partner with the Suicide Prevention Program to educate those hesitant about seeking mental health counseling in fear of the negative impact on their career and obtaining or retaining their security clearance. Security personnel have a critical role to play in educating the Army on this issue. The Army is on the cutting edge of the transformation in our personnel security system. Stay tuned for the rollout of the Army Investigative Enterprise Solution, Direct e-QIP, and eAdjudication.

On a personal note...each time that I attend the monthly Wounded Soldiers Welcome, that takes place in the Pentagon, I am reminded that our jobs protect our Soldiers. I am touched and inspired by their spirit, courage, and commitment. Thank you for your support to the Army

Patricia Stokes
Director of Security

"If you don't like change, you're going to like irrelevance even less."
– General Eric Shinseki

Announcements

New Arrivals: We are pleased to announce the new arrivals to HQDA G2:

SETA Program Manager
Ms. Luisa Garza

Information Security
Ms. Liza Vivaldi

ARTPC
Mr. Paul Watkin

Foreign Disclosure
Mr. Dave Grob

Security Generalist
Ms. Judy Tang

Functional Management
Ms. Paola Apodaca

Bid Farewell: HQDA G2 would like to bid farewell to Mr. Ed Anthony, Chief of Army Foreign Disclosure. Ed retired on 30 Apr 2009 after more than 49 years of combined government service. He will be greatly missed.

HQDA G2 support for Command Conferences: We welcome the invitations to brief the security programs at your Command conferences. All requests should be forwarded to Ms. Judy Tang, email: Judy.Tang@us.army.mil. In the requests, please provide the following information: date of conference, location, the specific topics to be briefed (include an agenda), and whether or not your request will cover TDY expenses. This will expedite the process and allow us to provide the appropriate briefer(s) to support your conference.

The Army Security Managers Collaboration Forum (ASMCF)

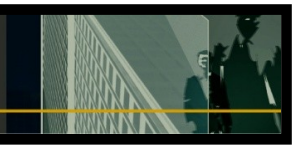
The Army Security Managers Collaboration Forum (ASMCF) was held from 23 – 26 February 2009 at the Millennium Hotel Complex, in St. Louis, Missouri. It was great meeting all the Army security professionals, and spending time listening to their challenges and accomplishments.

The intent of the ASMCF was to provide a forum to educate and disseminate updated information affecting Army Security Programs and impart an understanding of the transformation efforts occurring within the security arena at the National, DoD and Army levels. Since the ASMCF, we have had numerous requests for implementing Army Investigative Enterprise Solution (AIES) throughout the Army.

A special thanks to the ASMCF guest speakers: Mr. Tom Faust, Ms. Elizabeth McGrath, Ms. Teresa Nankivell, Ms. Sebrina Nelson and Mr. Stephen Schooley, and Mr. Jim Lynch. We were honored to have them participate and appreciate their time and commitment.

Proud to be Army and to serve!

Inside This Issue



Psychological Conditions and the Security Clearance Process

Through policy changes and education, the DoD and Army are addressing the negative perception regarding mental health counseling, in order to ensure that Soldiers and Civilians are not deterred from obtaining needed mental health treatment. Both Soldiers and Civilians should take advantage of mental health treatment without the fear of unfavorable action being taken against their security clearance eligibility. For this reason, the Army is working aggressively to change the perception associated with mental health treatment and the perception of its negative effect on the security clearance process.

The Questionnaire for National Security Positions (SF86) required applicants to identify all mental health treatment received within the last 7 years. Many Soldiers expressed an unwillingness to participate in Army mental health programs based upon the perception that a 'Yes' answer to the question would lead to denial, suspension or possible loss of a security clearance.

The Army has served as a catalyst in revising the SF86 so that it excludes treatment strictly related to adjustments from service in a military combat environment. Executive Order 12968, Access to Classified Information, governs access to classified information and specifically addresses the perceived inferences in obtaining counseling services. Section 3.1(e) states: "No negative inference concerning the standards of this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determination." All Army Leaders must take an active role to educate Soldiers and Civilians that receiving assistance for mental health is acceptable.

Furthermore, the new adjudicative guidelines approved by President Bush on 29 December 2005, provides two new mitigating factors regarding psychological conditions:

a. "A condition that is readily controllable with treatment and the individual has demonstrated ongoing and consistent compliance with the treatment plan."

b. "The individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment and the individual is currently receiving counseling or treatment with a favorable prognosis."

These new guidelines are intended to promote and encourage individuals who need counseling or treatment to seek it, rather than avoid it for fear it will negatively effect their security clearance.

Clearance eligibility statistics additionally support this fact. Recent statistics reveal that 99.99% of security clearances with mental health concerns were granted. For these reasons, the Army is trying to reduce the stigma and fear associated with the security clearance process to ensure that all Army personnel understand that security clearances are fair, equitable and consistent with preserving our national security.

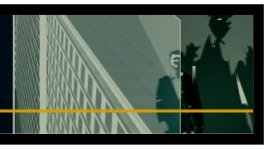
Processing the Questionnaire for National Security Position (SF 86) at the Military Entrance Processing Stations (MEPS)

The Office of Personnel Management (OPM) conducts background investigations and reinvestigations of persons under consideration for, or retention in, national security positions, as defined in 5 Code of Federal Regulations (CFR) 732, and for positions requiring access to classified information under Executive Order 12968. Providing information on the SF86 is voluntary, however, withholding, misrepresenting, or falsifying information will have an impact on the applicant's security clearance.

OPM investigators have observed on several occasions where incorrect information was listed on the SF 86. A current example is, under the "residence, person who knows you at this address section." An applicant had listed himself and his address, but listed a false "person who knew him." When the applicant was interviewed by the OPM investigator, they were unable to recall or explain why this falsified information was listed in their SF 86. The OPM investigator had to confer with the applicant about the incorrect residence and "person who knew him" at that residence. As a result, the subject interview took three to four hours instead of the standard one hour interview. Not only is this not an efficient use of resources, but it also affects timeliness under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The IRTPA provides a time range in which OPM must complete their part of the investigation. It is imperative that Recruiting and MEPS Commanders are aware of this issue and use this as an educational tool to reiterate the importance of accurately completing the required security forms.

Financial Considerations and the Security Clearance Process

The National Adjudicative Guidelines are used as the standard to determine security clearances. The guidelines are designed to provide adjudicators flexibility in applying factors to mitigate concerns regarding financial considerations. More specifically, the adjudicative process is not



driven or limited by a fixed figure, instead adjudicators apply the "whole person concept" when reviewing case files.

Adjudicators consider all relevant factors (i.e. loss of employment, economic downturn, life changes, etc.) when making a determination. Although the current economic environment may result in negative financial situations, an individual's good faith efforts to resolve or address financial difficulties will have a positive impact on an their security clearance. Thus, a bankruptcy or foreclosure is not a "bad" indicator by itself.

Conditions that could mitigate security concerns are "...conditions that resulted in the financial problem were largely beyond the person's control...and the individual acted responsibly under the circumstances." For example, if an individual has never had financial problems in the past, yet was forced into foreclosure due to housing downturn and inability to sell property (a home), this would be mitigated by condition above. However, if the individual has a history of not meeting financial obligations documented from previous investigations and now forecloses on a home, there is a pattern of financial irresponsibility that cannot be easily mitigated.

The Department of Defense leadership is addressing this security clearance issue with each of the Services. It should also be noted that in 2008, CCF rendered 227,000 final adjudicative actions. Of that number, 3,757 (1.6%) of clearances were denied or revoked due to financial issues. This statistic has been consistent since 2005.

eAdjudication

Executive Order 13467 of June 30, 2008, calls for "end-to-end automation" which is defined as an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant documentation of the application (but not an employment application), investigation, adjudication and continuous evaluation processes. For this reason, the Army Central Clearance Facility (CCF) developed an information system, the Clearance Adjudication Tracking System (CATS) to facilitate automated or electronic adjudication (eAdjudication). eAdjudication is a viable technical means to make eligibility determinations for security clearances by applying computer coded business rules to the adjudicative process.

In November 2008, the CCF began a pilot eAdjudication program covering Soldiers, Civilians and Contractors requiring a Secret security clearance eligibility determination using the established business rules. The business rules serve to check that no issues requiring human adjudication exist and that the investigation is complete by verifying the following using the Case Closing Transmittal (CCT): CRED - credit report; SII - Security/ Suitability Investigations Index; DCII – Defense Central Index of Investigations; FBIF/FBFN - FBI finger print checks; FBIN/FBNF - FBI name check; SESE - Selective Service Registration; and LAWE/LAC - local agency checks were performed. Cases which fail to meet the business rules are auto-assigned for human adjudication.

For those investigations not requiring a security clearance received by the CCF that do not meet the eAdjudication business rules, have no interim clearance in JPAS and do not have a request to research/recertify/upgrade eligibility (RRU) reflected in the JPAS, an eligibility of No Determination Made will be entered in the JPAS.

Verification of Security Clearance Eligibility Prior to Attendance to Service Schools

In accordance with Army Regulation 614-200, Army Training Requirements and Resource System (ATRRS) Course Catalog and the Department of the Army Pamphlet 611-21 SMARTBOOK, Soldiers (RA, NG, USAR) must be certified in their new MOS.

Security managers are reminded to verify a Soldiers' clearance eligibility prior to attendance to a service school. At a minimum, the appropriate investigation should either be submitted and/or opened at OPM, prior to departing the Command. It is the responsibility of the losing Command and/or security manager to ensure that the selected Soldiers (including Officers) are eligible. If a Soldier arrives to a service school without the required investigation or clearance eligibility, the Soldier will be placed on security hold. This is not only significantly costly and inefficient, but also delays the process.

PERSEC POC

Ms. Andrea Upperman
Chief of Personnel Security
Ph: (703) 695-2616
Andrea.Upperman@us.army.mil

Mr. Eric Novotny
Chair, Personnel Appeals Board
Ph: (703) 695-2599
Eric.Novotny@us.army.mil

Ms. Julia Swan
System Integration & Policy Development
Ph: (703) 695-2629
Julia.Swan@us.army.mil

Ms. Brenda Kendrick
Contract Linguist Program
Ph: (703) 695-9605
Brenda.Kendrick@us.army.mil

Ms. Tamara Haire
CCF Oversight & Policy Development
Ph: (703) 695-2647
Tamara.Haire@us.army.mil

Controlled Unclassified Information (CUI) Update

On 7 April 2009, the Under Secretary of Defense for Intelligence issued a memorandum to the Department of the Army. The memorandum states that while CUI policy was still being developed on a national level, Department of Defense (DoD) components are not to use any of the new CUI markings until policy development is complete. The memorandum reminded DoD components that existing policy guidance pertaining to information, such as For Official Use Only (FOUO), must be followed, and that the designation, marking, safeguarding and dissemination of such information remains unchanged.

USPS and Foreign Carriers

The United States Postal Service has announced a change in the way Registered mail will be processed. The Office of the Under Secretary of Defense for Intelligence is consulting with the Military Postal Service Agency concerning the change in procedures. They have informed the MPSA that, at this time, there are no modifications to the policy concerning registered mail. OUSD(I) is working with other national level agencies in regard to the issue and will issue updated policy if needed.

Foreign Ownership, Control or Influence

Foreign investment is playing a significant role in our global economy today. As such, U.S. companies are being purchased, merged or acquired by foreign companies at an increasing rate. A U.S. company is considered to be under Foreign Ownership Control or Influence (FOCI) when a foreign interest has the power, direct or indirect (exercised or not through the ownership of the U.S. company's securities, by contractual arrangements or other means), to direct or decide matters affecting the management or operations of the company in a manner that may result in unauthorized access to classified information or adversely affect the performance of classified contracts. In making a determination as to whether a company is under FOCI, Defense Security Service (DSS) considers the information provided by the cleared company, or its parent entity, on the Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," and any other relevant information. DSS will determine the appropriate mitigation instrument (s) that must be put in place to mitigate any FOCI. Whenever a company has been determined to be under FOCI, the primary consideration shall be the safeguarding of classified information. DSS is responsible for taking whatever interim action is necessary to safeguard classified information, in coordination with other affected agencies as appropriate.

When a merger, sale, or acquisition is finalized prior to having an acceptable mitigation agreement in place, DSS invalidates the existing Facility Clearance (FCL) until such time as DSS determines that the company has submitted an acceptable FOCI action plan in accordance with paragraph 2-303 of the NISPOM. Invalidation of the existing FCL renders the company ineligible to receive new classified material or to bid on new classified contracts. However, DSS may continue the FCL so long as there is no indication that classified information is at risk of compromise. If there is any concern that classified information is at risk of compromise due to the FOCI, and security measures cannot be taken to remove the possibility of unauthorized access to classified information, DSS will terminate the FCL.

There are several ways for DSS to mitigate FOCI, but the most common are: Special Security Agreement (SSA) and a Proxy Agreement (PA). A SSA is one way to mitigate FOCI. The SSA is used when a company is effectively owned or controlled by a foreign entity. The SSA has access limitations. Access to proscribed information by a company cleared under a SSA may require that the Government Contracting Activity complete a National Interest Determination (NID). The NID will allow the U.S. cleared company access to such information (i.e., Top Secret; Communications Security (COMSEC), except classified keys used for data transfer; Restricted Data (RD); Special Access Program (SAP); or Sensitive Compartmented Information (SCI)), and the access of such information will not harm the national security interest of the United States. A PA may be used as a FOCI mitigation instrument vice an SSA. The PA is more robust and stringent because it requires the foreign owner (s) to forfeit their voting rights to proxies who are U.S. citizens, and approved by the Federal Government. The PA is used when a cleared company is owned or controlled by a foreign entity. The PA is an arrangement whereby the voting rights of the foreign owned stock are vested in cleared U.S. citizens approved by DSS. The PA does not impose any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts. More to follow on NIDs.

Information Security POCs

Mr. Bert Haggett
Ph: (703) 695-2654
Bert.Haggett@us.army.mil

Industrial Security POC

Ms. Lisa Gearhart
Ph: (703) 695-2636
Lisa.Gearhart@us.army.mil

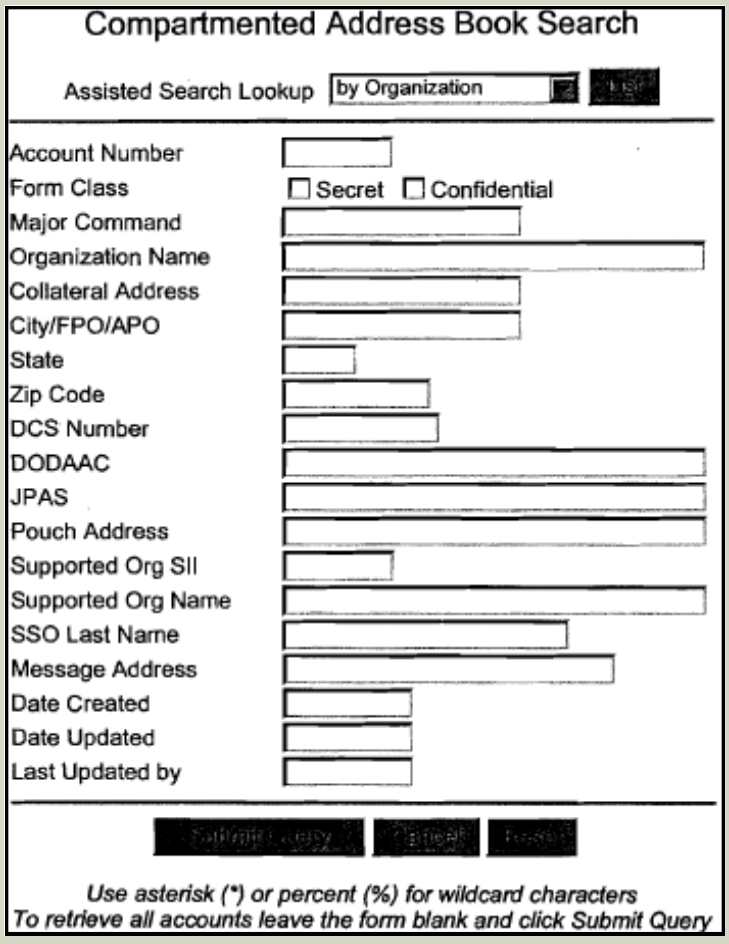
Defense Intelligence Agency's (DIA) Compartmented Address Book (CAB)

The search for particular information on Special Security Offices has just been simplified! The CAB is still available is easier, quicker and definitely user friendly. Guest access to the CAB can be given via SIPRNET or JWICS.

The CAB is an electronic database registry that contains various information such as Defense Courier Service addresses, SCIF collateral mailing addresses and special handling instructions on DoD and U.S. Military Special Security Offices around the world. It is a component of DIA's Joint Dissemination System (JDS), which is accessible via JDS link on the the INTELINK DIA Homepages or INTELINK SCI at https://ismapp3.dia.ic.gov:4444/pls/jds/jds.login1 and also on INTELINK SIPRNET at http://ismapp4s.dia.smil.mil:7779/pls/jds/jds.login .

Getting access to the CAB is a easy as 1, 2, 3. Please proceed to the SIPRNET address above and login by clicking on the guest icon in the center of the page. This will take you to the JDS page to continue accessing the CAB site. On this page, click on the CAB link under components and then click CAB application to get to the search page.

Users will be able to search for SSO information through a variety of ways such as by CAB account number, by organization, command, state and/or SSO message address. Once SSO information has been retrieved, take time to review and submit updates and changes using the CAB template located back on the components page via the New CAB Request Form link.


Compartmented Address Book Search

Assisted Search Lookup by Organization

Account Number	
Form Class	☐ Secret ☐ Confidential
Major Command	
Organization Name	
Collateral Address	
City/FPO/APO	
State	
Zip Code	
DCS Number	
DODAAC	
JPAS	
Pouch Address	
Supported Org SII	
Supported Org Name	
SSO Last Name	
Message Address	
Date Created	
Date Updated	
Last Updated by	

Use asterisk (*) or percent (%) for wildcard characters
To retrieve all accounts leave the form blank and click Submit Query

The Department of the Army's Intelligence Information Services Office is the designated office to approve new CAB accounts and record updates for Army SSOs. Submit request to establish new CAB accounts or updates/changes to one of the following e-mail addresses:

JWICS: dissem@inscom.ic.gov
SIPRNET: disem@mi.army.smil.mil

NEW to CAB is the JPAS SMO code entry. Please ensure you provide all the pertinent information for greater accuracy.

SSOs, please take a moment to make sure your information in the CAB is updated!

SCI POLICY POCs

Mr. Cliff McCoy
Ph: (703) 693-1459
Clifford.McCoy@us.army.mil

Ms. Chalydria "Lynn" Taylor
Ph: (703) 6931454
Chalydria.Taylor@us.army.mil

Reporting Foreign Government Representative Misconduct

HQDA, ODCS G-2, DAMI-GXS, Foreign Disclosure Branch is the U.S. Army's Executive Agent for all official foreign government requests for visits by representatives of foreign governments and international organizations to Department of the Army (DA) commands or activities in the continental United States (CONUS), as well as requests by such representatives for U.S. Army information.

In the current international environment, interaction with foreign governments and international organizations is beneficial to both governments and critical to our bilateral relationships. While most interaction occurs without incident, there are instances where foreign representatives fail to comply with applicable statutory and regulatory guidance, or with established DA policies and procedures, or conduct personal or professional affairs in an unsatisfactory manner. In such instances, Army Regulation (AR) 380-10, *Foreign Disclosure and Contacts with Foreign Representatives,* requires the hosting command or agency to provide a written report regarding the inappropriate action, through foreign disclosure channels, to HQDA, ODCS G-2, DAMI-GXS Foreign Disclosure Branch, with a recommendation for final disposition. If the incident in question involves an extended visitor, an additional report should also be made concurrently to the manager of the program under which the visitor is certified.

Examples of misconduct that must be reported under this requirement are:

- Extended visitors who violate their Terms of Certification in any way, such as requesting information from Army personnel other than the assigned contact officer.
- Foreign government representatives who initiate contact with or solicit information from Army personnel without first obtaining authorization from HQDA.
- Violations of U.S. Army security policies and procedures, such as unauthorized photography.
- Possession of U.S. Army information that has not been authorized for release.
- Information security violations, such as unauthorized external media introduced to U.S. Army information systems.
- Foreign government military officers' failure to wear their service uniform during official interaction with the U.S. Army, unless specifically authorized to do so.

The requirement to report such conduct to HQDA is not intended to be punitive for the hosting command or agency, but is instead an important means by which they can assist HQDA in protecting U.S. Army information and managing the Army's International Visits Program. Even a seemingly inconsequential incident of misconduct or failure to comply with established statutory and regulatory guidance, Army policies and procedures, and standards of conduct, may be significant to the larger picture of a particular country's interaction with the Army. Therefore, it is critical that **all** incidents be reported so that HQDA may accurately track trends and pursue an appropriate response to the incident(s). HQDA responses to misconduct may be as mild as a reminder or briefing to a particular country or individual regarding proper US Army policies and procedures or, in the event of repeated or more serious incidents, the revocation of a particular individual's visitor privileges to the U.S. Army.

It is important to note that reporting foreign government representative misconduct to the supporting counterintelligence office under AR 381-12 does **not** preclude a command or agency from also reporting pertinent conduct to HQDA under AR 380-10. Furthermore, these reporting requirements do not relieve those personnel designated as contact officers for foreign visitors from the responsibility to counsel and documenting foreign visitors regarding unacceptable behavior.

Increased awareness of this requirement and its objective is essential to protecting U.S. Army information, technology, and systems. Please help us by reporting foreign government representative misconduct to HQDA, ODCS G-2, DAMI-GXS, Foreign Disclosure Branch. If you have any questions or need assistance, please contact the appropriate Regional Desk Officer. Disclosure POCs can be found at the following website: http://www.dami.army.pentagon.mil/offices/dami-fd/pocs.asp

Foreign Disclosure POCs

Mr. Greg Hatter
Ph: (703) 695-1089
Gregory.Hatter@us.army.mil

Mr. Mike Shropshire
Ph: (703) 695-1081
Michael.Shropshire@us.army.mil

Integrating OPSEC into Research and Technology Protection

"Earlier this year, a newspaper published details of a new anti-IED technology that was being developed. Within five days of the publication – using details from that article – the enemy had posted instructions for defeating this new technology on the Internet. We cannot let the enemy know how we're working to defeat him"

- President Bush during a speech at The George Washington University, March 2006

The goal of research and technology protection is to prevent the exploitation of, or the countermeasure development against U.S. technology. This goal is accomplished through integrated, holistic protection. Program protection is a lifecycle process – it must start early and continue until the system is taken out of service. Therefore, protection must account and be adapted from the pre-acquisition phase through design, development, testing, production, operations, sustainment and demilitarization. The problem is that all too often information released early in the lifecycle can compromise a future capability. At this point, it may be too late to retrieve and protect this information. One way to mitigate the potential loss of sensitive information is the utilization of innovative and tailored OPSEC countermeasures that integrate and enable protection.

The reality of the research and development community is one of openness and collaboration; of commercial entities managing defense tech development; of coalition operations; and one where more commercial and fewer military technologies with development are occurring in the private sector. These are not bad things but they do present challenges in protecting research, technology and maintaining our edge.

The OPSEC process of determining critical information, analyzing the threat, vulnerabilities, and risks, and – most importantly – developing and implementing countermeasures – is a key aspect to program protection – and in many ways OPSEC serves to bridge existing stovepipes.

So in essence, OPSEC integrates protection while helping inform decisions and balancing program requirements with protection requirements.

For more information on integrating OPSEC countermeasures into research and technology protection, please contact the ARTPC.

"Through the Army Research and Technology Protection Center, support integration of OPSEC as a countermeasure in Program Protection Plans (PPP)." AR 530-1 para 2-16.f

ARTPC POC

Mr. Dick Henson
Ph: (703) 601-1930
Richard.Henson@us.army.mil

Did you know...

Security Professionals,

Professional certification is coming! The National Strategy identified in the Executive Order 13434, National Security Professional Development, May 17, 2007 provides a plan to give security professionals access to education and training. This will increase their professional experience, skill level and ability to protect our nation's secrets. Certification will professionalize our security workforce of the future.

As directed in DoD Instruction 3305.13, DoD Security Training, Dec 18, 2007, the DoD Security Training Council (DSTC) was established as an advisory body on DoD security training and is chaired by the Defense Security Service. The DSTC will identify development of a DoD certification program. OCDS G-2 is a member of the DSTC and has an active voice. The DSTC has engaged all the Military Departments and participating DoD agencies to identify their security training requirements and account for their security work force.

Why earn a security certification?

1) Career enhancer
2) Allows security practitioners to take advantage of opportunities
3) Receive credit for security experience through grandfathering
4) Certifications may become requirements in the civilian sector and perhaps even in government security positions

What can you do in the meantime to increase your experience and skills? Take advantage of the many free classes available through DSS, DNI, and JCITA. Many of them are available on-line. Contact your CP 35 Program Manager and/or training advisor for information on training opportunities.

Whether or not you will make security a career, enhancing your security education, training and awareness is a great move and makes your job easier. More details to come….

DNI Portal:

Army has moved their HQDA G-2 website to the DNI Portal. All of the ASMCF briefings have been uploaded to the Army site. If you have registered, go to "Agencies" and our site is called "Army G2". Once in the "Army G2" site, on the left side of the screen, there is a section titled "Divisions". Army Security Forum is the last Division. If you have not registered, you must first register for an INTELINK-U passport account. If you already have an INTELINK PASSPORT ID, go to step 2. To get a PASSPORT ID you must first register at: http://ra.intelink.gov. Then you register at: https://www.intelink.gov/passport/servlet/Passport.

Step 2: Once you have your PASSPORT ID, open your browser and type the following address into the address bar: https://www.intelink.gov/sites/ssc. Then click on the link to request an account. Follow the instructions on the account request. Once you have requested a portal account, an email response will come to the email address that you gave for your PASSPORT ID. Please feel free to call the DNI Portal Helpdesk if you have any questions at 1-866-304-4238.

What's New!

New training video from DSSA: "Need-to-Know Training Video"

This video provides a short refresher on the fundamental Need-To-Know security principle. It reviews a case history and provides guidelines on your responsibilities for applying the principle.

It is available at http://dssa.dss.mil/seta/training_videos.html.

Security Training Opportunities

Defense Security Service (DSS)

Please register (24 hour access) online at http://dssa.dss.mil/seta/seta.html for immediate status/confirmation. Online registration requests are granted first priority. Please be sure to enter a valid email address. All confirmations, notices and orientation information will be sent via email.

The Security Education, Training and Awareness (SETA) Directorate released its April issue of "Focus on Security."

SETA launched its new monthly PDF version of the newsletter in March 2009. You will receive a SETA Flash notification when each new edition is available. Click on the following link to access this product: http://dssa.dss.mil/seta/documents/focus/FocusApril2009.pdf. The April edition features:

* From the Desk of the Editor: Notes
* Spotlight On: DSS Academy Trains Security Specialists in Kuwait and New Physical Security Measures Course
* In the Community: Special Access Program (SAP) Orientation Course in California
* All Aboard: Important ENROL notice
* Under Construction: Coming soon, six new online courses
* Recap: Previously released SETA courses and products (2009)

The DISA PII training is available on the Defense Security Service (DSS) ENROL system: https://enrol.dss.mil/enrol/lang-default/SYS_login.asp.

The following link to DSSA will provide you with specific courses that are being offered by DSSA: http://dssa.dss.mil/seta/documents/combined_catalog_v0.2.d.pdf

Director of National Intelligence (DNI)

Available courses can be found on the DNI portal at: https://www.intelink.gov/sites/ssc

Joint Counterintelligence Training Academy (JCITA)

CI Fundamentals	27 Jul 2009 – 07 Aug 2009
	07 Dec 2009 – 18 Dec 2009
CI support to Research, Development & Acquisitions	13 Jul 2009 – 24 Jul 2009
	14 Sep 2009 – 25 Sep 2009
	26 Oct 2009 – 06 Nov 2009

JCITARegistrar@jcita.cifa.smil.mil – Please contact for registration and availability.

Other Related Security Courses:

Defense Institute of Security Assistance Management (DISAM)

Available courses can be found at: http://disam.afit.edu

Defense Personnel Security Research Center (PERSEREC)

This database of providers of security training offers course information to security practitioners who may wish to update or enhance their security training in one or more disciplines.
http://www.dhra.mil/perserec/stpdb/STPDB_Disciplines_Selection_List.html

Some of the disciplines available are listed below:

1. Communications Security	4. Information Security	7. International Programs
2. Counterintelligence Awareness	5. Information Systems Security	8. Investigations
3. Industrial Security	6. Intelligence	9. Operational Security (OPSEC)

AND MORE ARE DISCIPLINES ARE AVAILABLE ONLINE!

Final Thoughts

Security Professionals,

Security begins with you. Policies and procedures have been developed to ensure protection of our assets. However, to be effective, security must become a practice which all users adopt. It need not be so restrictive that it interferes with the normal course of work. But it must be robust enough to eliminate as many threats as possible and manage those which can be negated.

Over time, we may develop habits that compromise security of our systems and environment. Offset the negative habit with security awareness and reminders of the threat.

Recognize the threat. Understand why and know what information can be disseminated. Inadvertent disclosure can result in loss of time and resources for all involved. Always give security consideration before hitting that "send" button.

Protect passwords and avoid sharing them with others. Be pro-active in prevention of compromises. As we have become reliant on technology, the risks they bring are often overlooked. Sharing the technology and research could result in a number of undesirable situations. Projects may go unfinished, resources can be affected or reduced and some incidents could lead to litigation.

We move forward in establishing a robust SETA program that provides you guidance, best practices, templates and awareness products. In the meantime, you will receive information via mass emails, written and web publications to help you achieve better results in the programs.

Luisa Garza
SETA Program Manager

SETA Questions or Comments

In order to provide you the best information and products, your input is needed. What information on security education, training and awareness would you like to receive? What kind of security training do you need or would like developed? What awareness products will improve your SETA program? Feel free to send your input directly to me.

Luisa Garza
Ph: (703) 695-2644
Luisa.Garza1@us.army.mil

Address:
1000 Army Pentagon (2D350)
Washington, D.C. 20310-1000

WHO is RESPONSIBLE

for SECURITY?

EVERYONE
IS
RESPONSIBLE
FOR
SECURITY