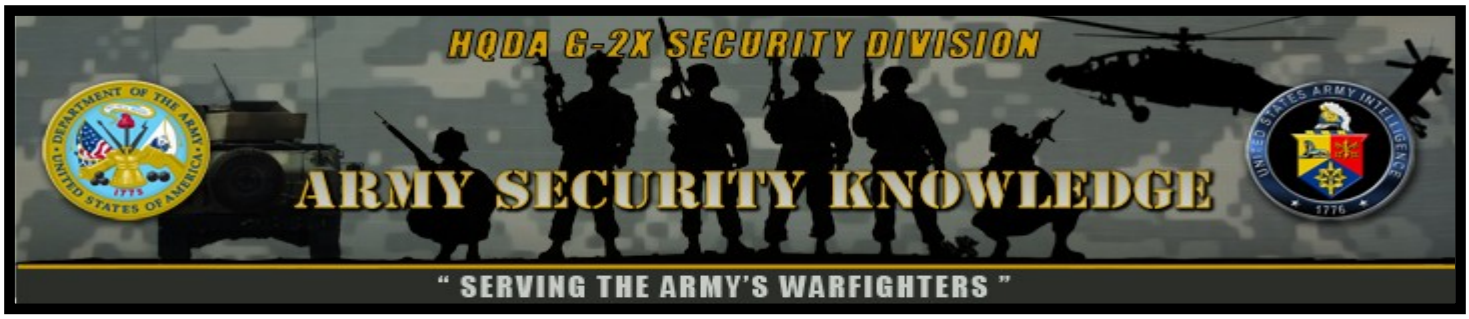


Director's Message

Welcome to our third edition of the G-2 Security Newsletter. Once again, I think you will find some very useful articles that will bring you up-to-date on the on-goings in the Army Security arena. Take note of the "almost" official stand-up of the Army's Personnel Security Investigation Center of Excellence (PSI-CoE). At end state, we will have one central location for the submission of ALL Army personnel security investigations. This translates into one location, one system, one process; simply put, this leads to consistency and efficiency and enhanced Army Readiness! The PSI-CoE is part of the Army Investigative Enterprise Solution (AIES). AIES is an enterprise solution comprised of a *re-engineered* and *automated* process for the submission, processing, and adjudication of personnel security investigations. Our progress in AIES has reduced the total time to obtain a security clearance by 80% (that is more than 250 days on average). For details on the PSI-CoE and AIES, check out the article on page 2 of this newsletter. Army is leading the way in clearance reform!!! Hooah!!!!

Another key initiative I draw your attention to is the development of our Security Education, Training and Awareness program (SETA). We are working with DoD on the development and deployment of the Security Professional Education and Development (SPeD) program; a professional certification and training program for security professionals. This will transform our Army ACTEDs program and realign it to conform with the SPeD model providing a means for professional training and certification for our security workforce. Your participation in the program development is essential. This is our future!

Finally, through the Army Campaign Plan Decision Point (DP) 59 initiative, the Army G-2 Security Division in coordination with the ACOM, ASCC, and DRU Command Security Managers will complete a manpower modeling analysis for all Army security disciplines. The manpower modeling associated with DP 59 is affording us the opportunity to collect data on all our security disciplines to include Personnel Security; Information Security; Industrial Security; Communication Security (COMSEC); Security Education Training and Awareness (SETA); Foreign Disclosure; Sensitive Compartmented Information (SCI); and Special Access Program (SAP) Security. Data collection will commence in early October and run for a period of approximately 3-4 months. This data will then be used in the validation of a manpower model that has never existed before for security functions. This model will not only allow us to achieve the desired outcome of the DP 59 initiative (establishing the right TDA structure and alignment of security resources across the Army) but also provide a validated tool for Army components to use to further justify additional security manpower for their activities.

Please remember our soldiers in all your daily support activities. Their honor, commitment to duty and country and personal sacrifice is daunting. Thank you for all you do in supporting the Army mission.

Ms. Patricia P. Stokes
Director of Security

Arrivals:

Mr. Harry Byrd Jr.
COMSEC/TEMPEST

Mr. Robert Cunningham
Chief, PSI-COE (Aberdeen Proving Grounds)

Ms. Monique Hampton
Security Specialist, SSO

Ms. Ulinda Harper
Security Specialist, ARPTC

Mr. Robert Horvath
Chief, Linguist Security Office

Mr. Sylvester Mitchell
Security Specialist, ARTPC

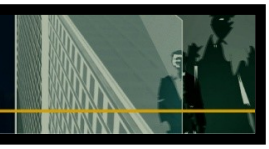
Mr. Thomas McNear
Security Specialist, ARTPC /TRADOC

Mr. Linwood Smith
Security Specialist, SSO

Ms. Pamela Spilman
Industrial Security

Inside This Issue

Personnel Security…..……...…...2-4
Information/ Industrial Security ...5-6
SCI Policy ……...…...…...…7
Foreign Disclosure …..……..… 8-9
Army Research and Technology Protection Center…...…….10
Security Education, Training and Awareness…..……....11-12



The Personnel Security Investigation Center of Excellence (PSI CoE)

The Army's personnel security investigation pilot is evolving into the Personnel Security Investigation Center of Excellence (PSI CoE). The PSI CoE located at Aberdeen Proving Ground in Maryland will be the central location for all security clearance and suitability investigations submitted by the Army for its civilian military personnel, and Army contract linguists. Senior Army leadership set the goal for the PSI CoE to service all Army installations and organizations by the end of FY 2010. Partnerships with the Office of Personnel Management (OPM) and the Army's Central Clearance Facility (CCF) facilitate information and technology sharing that enhances the total security investigation process.

The PSI CoE currently supports organizations at multiple locations around the world. The process has become more streamlined and efficient and continues to evolve as improvement opportunities arise. You are likely wondering what the "new and improved" process looks like, and how it will affect the way you process personnel security investigations? Here's how it works: security officers and Civilian Personnel Advisory Centers (CPACs) identify an individual who requires a security investigation. The requester, submits the individual's basic identifying and contact information through the Personnel Security Investigation Portal (PSIP) and arranges for the subject to be fingerprinted (where required).

The PSI CoE initiates the investigation and works directly with the individual to ensure that their eQIP forms are properly completed to investigative standards, that they have submitted the proper releases, and assembles the entire package to send to OPM for action. The PSI CoE tracks the case throughout its entire lifecycle, closing the action when an adjudicative decision has been made and recorded. Through the use of careful quality controls in the review process, the PSI CoE has reduced the number of cases rejected or delayed for missing or incomplete paperwork. If an interim collateral clearance is required, the requester will receive a copy of the individual's SF-8X packet for review so that they may facilitate the granting of that interim clearance by the organization's commander. The Army CCF will continue to grant SCI access interim clearances.

Here is what this means to you: As a requester, the PSI CoE greatly reduces your workload in personnel security matters. AIES reduces the time it takes from an investigation opening to the final granting of the security clearance, thus improving individual and organizational readiness. At program initiation, the Army average was more than 300 days to process a clearance. Currently, individuals who have submitted through this program, have had their security clearances granted in an average of 78 days – an 80% decrease in time compared to the current process.

Contacting CCF

The Army Central Clearance Facility (CCF) has the largest workload and volume of cases in the Department of Defense (DoD). We are pleased to report that CCF has successfully eliminated its backlog of cases pending initial review, Incident Reports and Requests for Research, Recertify or Upgrade Eligibility (RRUs). DoD adjudication timelines are being monitored at the highest levels of the federal government. In order to minimize the call volume to the CCF Call Center, request your assistance with regard to the submission of Incident Reports, RRUs and contacting the CCF call center.

Incident Reports: When a commander learns of credible derogatory information on a member of his or her command that falls within the scope of the adjudicative guidelines, the commander will immediately document in writing the incident and his/her recommendation. The commander will ensure the timely submission of an Incident Report via the

Joint Personnel Adjudication System (JPAS) to the Commander, CCF. At a minimum, initial reports will indicate the details of the credible derogatory information and actions being taken by the commander or appropriate authorities (for example, conducting an inquiry or investigation) to resolve the incident. Follow up reports will be submitted via the JPAS at 90 day intervals if the commander has not taken final action or, for example, the subject is still pending action by a civil court. At the conclusion of the command action, a final report will be forwarded to CCF indicating the action taken by the commander. The final report must contain copies of relevant documents such as 15-6 investigations, UCMJ actions, court documents, etc., if not previously provided, as well as results of any local inquiry, investigation, or board action and recommendation concerning restoration, denial or revocation of the person's security clearance, if appropriate.

RRUs:

(1) RRUs should only be submitted for the following reasons:

-an investigation closed more than 20 days ago and JPAS does not reflect an eligibility determination;

-an individual has a higher eligibility level or investigation that is not reflected in the Joint Clearance and Adjudication Verification System (JCAVS), a subsystem of JPAS;

-an employee had a non-DoD clearance and now requires a DoD eligibility;

-an eligibility of No Determination Made was entered in the JPAS, and subsequent to that entry, a determination was made that the individual requires security clearance eligibility, provided that the requisite investigation has been completed;

-an eligibility of Loss of Jurisdiction was entered in the JPAS, and subsequent to that entry, the individual became re-affiliated with the Army and requires security clearance eligibility; or

-an individual has a current level of eligibility and requires a higher level of security clearance eligibility, provided that the requisite investigation has been completed.

(2) RRUs should not be submitted for the following reasons:

-an individual's name or other personal identifying data (PID) information is incorrect in the JPAS;

-to obtain the status of an investigation;

-to advise of a subject's voluntary separation; or

-to request reinstatement of a denied or revoked clearance; instead, follow the reconsideration procedures outlined in AR 380-67.

Call Center:

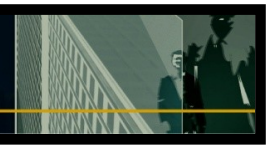
Any other questions should be phoned to the call center at (301) 677-7075 or DSN 622-7075.

Catch 'Em Program

The Catch 'Em Program has been in existence for many years and is of particular importance for those SSBI, SSBI-PR and PPR investigation requests, as the subject interview is required. However, the Office of Personnel Management (OPM) continuously receives investigation requests for Army Soldiers, civilians and contractors who are deployed, with no details as to when the individual will return stateside.

To ensure that the investigative standards are met, security managers must exercise their due diligence with regard to the application of the appropriate Catch 'Em code, "CC" - OPM Catch 'Em CONUS or "CL" - Catch 'Em Linguist. Catch 'Em requests should be submitted at least 1 month prior to subject's deployment.

If a security manager is aware of an upcoming deployment before a new investigation has been requested, the security manager will apply the applicable Catch 'Em code for electronic-Questionnaires for Investigations Processing (e-QIP) direct submissions in the Federal Investigations Processing Center (FIPC) block of the Agency Use Only (AUB) Block. Security managers will identify the subject's CONUS location to include



their complete street address, contact number(s), e-mail address, deployment dates and the name of a primary and alternate agency Point of Contact (POC) and the POC's phone number in the agency special instructions block.

When e-QIP is accessed via the Joint Personnel Adjudication System (JPAS) or in the event an individual deploys and the "CC" or "CL" code was not applied, the security manager will submit an OPM Catch 'Em request by e-mail to catcheminconus@opm.gov. The request must be clearly identified as Catch 'Em in CONUS or Catch 'Em Linguist at the top of the page and include the following information for the subject: complete name and SSN or OPM Case number, CONUS location to include their complete street address, CONUS contact number(s), e-mail address, dates of deployment or dates returning stateside on leave and the name of the agency POC and the POC's phone number.

Catch 'Em procedures do not apply to subject's returning stateside permanently from a deployment. Instead the OPM Customer Interface Branch should be contacted to request the investigation be reopened for completion of the interview. By utilizing the Catch 'Em codes for SSBIs, SSBI-PRs and PPRs, the number of Army cases closed incomplete should significantly decline.

CCF Correspondence

The Army Central Clearance Facility (CCF) routinely sends time sensitive correspondence pertaining to security clearance related matters to individuals through their servicing security management office (SMO). The role of SMO personnel with regard to the processing of CCF correspondence is of the utmost importance to both CCF and the individual. As such, the head of the SMO of the individual receiving correspondence from the CCF is responsible for designating a point of contact (POC) to serve as a liaison between CCF and the individual.

The duties of the POC will include, but not necessarily be limited to, delivering said correspondence to the individual and providing CCF with the individual's completed form letter within 10 days. The form letter provides CCF with pertinent information regarding whether or not the individual intends to respond to the correspondence. At a minimum, completion of the form letter requires the individual's signature and date. POC's must verify that the date placed on the form letter reflects the date the correspondence was actually received by the individual.

Ensuring the individual understands the consequences of not responding within the allotted time, how to obtain an extension and the procedures for responding to the request are also the responsibility of the POC. Individuals must be informed that legal counsel or other assistance can be obtained at his or her own expense. If necessary, POC's may need to explain how to procure copies of investigative records.

It is imperative that the POC obtain the individual's completed form letter and return it within 10 days of receipt of the correspondence to CCF. If a completed form letter is not received by CCF and/or the individual does not provide a response in a timely fashion, CCF may consider such actions to be a personal conduct concern in accordance with the adjudicative guidelines.

PERSEC POCs

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

Mr. Eric Novotny
Chair, Security PSAB
Ph: (703) 695-2599
Eric.Novotny@us.army.mil

Mr. Robert Horvath
Chief, Linguist Security Office
Ph: (703) 706-1929
Robert.Horvath@us.army.mil

Mr. Robert Cunningham
Chief, PSI-COE (Aberdeen Proving Grounds)
Ph: (410) 278-9745
Robert.Cunningham1@us.army.mil

Information Security Update

Since the last newsletter, development of national policy for the implementation of Controlled Unclassified Information (CUI) has continued with input from DoD and other national level agencies. A Presidential Task Force was formed to review the draft policy that had been developed to date and the Task Force has sent their findings to the President. It will take some time for the Administration to review those findings and suggestions and issue further guidance. At present, the draft policy still contains provisions for three levels of CUI. There are a number of working groups developing specific definitions and wording that will form the basis for distribution of certain types of information. An example would be legal or law enforcement information. The definitions developed for these terms will eventually drive the exact distribution of the information.

The draft revision to Executive Order (E.O.) 12958 has been submitted for comment a number of times and is now likely nearing it's final form. In it's current draft version, the greatest change in the Order is the proposed creation of a National Declassification Center. In theory the center would be run by the National Archives and would house all or portions of an agency's automatic declassification efforts. The current draft also calls for Original Classification Authorities to be trained annually and for derivative classifiers to be trained every two years. The Information Security Oversight Office (ISOO) estimates that it could be signed by the President as early as the end of the year.

The most recent information security policy issue is a draft new Executive Order dealing with sharing classified information with State, Local and Tribal organizations. This new E.O. has just been submitted to the armed services for comment.

INFOSEC POCs

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

Ms. Liza Vivaldi
Ph: (703) 695-2640
Liza.Vivaldi@us.army.mil

National Interest Determinations (NIDs):

A NID determines if release of proscribed information is consistent with the national security interests of the United States. Proscribed information is defined as Top Secret; Communications Security (COMSEC) (with the exception of classified keys used for data transfer); Restricted Data (RD); Special Access Program (SAP); or Sensitive Compartmented Information (SCI). NIDs may approve or deny contractor access to proscribed information. The requirement for a NID applies to new contracts, which include pre-contract activities if access to proscribed information is required, and to existing contracts when contractors are acquired by foreign interest. NOTE: A NID can only be prepared if a Special Security Agreement (SSA) is the anticipated foreign ownership, control and influence (FOCI) mitigation method.

The NID can be a program, project or contract. A separate NID is not required for each contract under a program or project, however, the NID must state the specific program. All contracts associated with a program or project must be identified on the NID request. The NID request must be signed at the Program Executive Level.

Additional guidance on NIDs can be found in the Directive-Type Memorandum (DTM) 09-019 "Policy Guidance for Foreign Ownership, Control and Influence (FOCI)" dated 2 September 2009 and posted in the Army G-2, Industrial Security folder on the DNI Portal.

NID Process:

Upon receipt of a request for a NID from HQDA, G-2, there are two requirements:

1. Determine if there is a SSA already established between the company and the DSS to negate the FOCI. If not, the FOCI must be mitigated with either a SSA or a Proxy Agreement. DSS will prepare this agreement.

2. The NID must be initiated by the Industrial

Security Specialist (ISS) in coordination with the Contractor Officer Representative and the Program Office. A written justification from the Program Office or activity must be attached to the NID. The company may assist in the preparation of a NID, but the government is not obligated to pursue the matter unless it believes further consideration to be warranted. The NID will be staffed through the appropriate office channels to the appropriate Program Official for signature. All Army units subordinate to a Command will process their NID packages through their respective Command. The Commands will forward the signed NID package to HQDA, G-2 Industrial Security email address: ArmyNIDRequest@us.army.mil. HQDA, G-2 will forward the NID package to the appropriate Agency of the proscribed information with Command recommendation to approve. The NID must include the following information:

a. Identification of the company or proposed awardee, along with a synopsis of its foreign ownership (include Government contract/solicitation number or other previous government contract solicitation numbers to identify the action);

b. General description of the procurement and performance requirements;

c. The fact that the contractor has an SSA with DSS (include copy of the DD254);

d. A justification/reason why access to the proscribed information is required;

e. Identification of national security interests involved and the ways in which award of the contract helps advance those interests;

f. The availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract; and

g. For COMSEC information: Number and type of COMSEC equipment/keys/documents required and specific locations.

Upon the final Agency approval/disapproval of the NID Request, HQDA, G-2 will forward the NID to the submitting Command and DSS for their records. The submitting Command must ensure that the NID is provided to the Program and company. For templates, please go to the DNI Portal: https://www.intelink.gov/passport/Login?returnURL=http%3a%2f%2fwww.intelink.gov%2fsites%2fssc%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252fsites%252fssc. Click on "Army G2," then "Industrial Security," and finally "Templates."

Industrial Security Update

The 2009 Industrial Security VTC was held on 24 Sept 2009 with 22 attendees and 4 Commands represented. The following items were discussed:

- AR 380-49 Update
- Army Security Knowledge (ASK)/DNI Portal
- DoD Security Managers Forum
- HSPD-12
- DTM 09-019/FOCI

The AR 380-49 was formally staffed on 15 Sept 2009 to the Commands. A consolidated Command review and comments are due 16 Oct 2009 and must be submitted on a Comment Matrix.

Industrial POCs

Ms. Lisa Gearhart
Chief, Industrial Security
Ph: (703) 601-1565
Lisa.A.Gearhart@us.army.mil

Ms. Pamela Spilman
Ph: (703) 601-1567
Pamela.Spilman@us.army.mil

Updates from the SCI Corner

Certified SCIF Inspector (CSI) Training in development at DIA SCIF Support Branch

The DIA SCIF Support Branch is in the process of enhancing their Inspector Training Program by developing a training module specifically to Certify SCIF Inspectors.

This innovative initiative will ensure DIA Inspectors are better equipped to evaluate SCIFs and conduct security and compliance inspections in accordance with the Office of the Director of National Intelligence and DoD security standards for protecting SCI. The CSI certification program will eventually be offered to Security Specialists at the Command Level responsible for the oversight and management of subordinate SCIFs for the Services, Combatant Commands and DoD elements.

Although the training program is still in the early stages of development and testing, the certification will include practical applications related to some of following areas: SCIF construction requirements, Sound Transmission Class, basic TEMPEST, Security in-Depth, T-SCIFs, Intrusion Detection Systems, Contractor SCIFs, doors, locks, Co-Utilization Agreements, Fixed Facility Checklists, security containers, waivers, and suspensions as well as hands on demonstrations to include an actual SCIF Inspection. The SCI Policy office will keep you informed as the certification training program further develops.

SCI POLICY POCs

WE HAVE MOVED!
Please note our new phone numbers.

Mr. Cliff McCoy
Chief, SCI Policy
Ph: (703) 602-3639
Clifford.McCoy@us.army.mil

Ms. Chalyndria "Lynn" Taylor
Ph: (703) 602-4665
TaylorCR@mi.army.mil

Future SCIF Construction Policy

Where is that new Director of National Intelligence (DNI) construction security policy that you said was coming out so soon? ICPG …ICD…ICS ….IC something that we have been hearing so much concern about, it is without a doubt (STILL UNDER CONSTRUCTION). There are still a variety of ongoing discussions pertaining to waiver/accreditation authorities, the need for SCIF re-accreditation, SCIF reciprocity, and other SCIF operational concerns that the ODNI Physical and Technical Security Expert Working Group along with the Intelligence Community are working to resolve prior to the final policy release. The SCI Policy Staff forwarded a DRAFT version of ICS 2009 705-1 for your review and comments back in July. That DRAFT is undergoing further intense reviews at the ODNI as of mid September. It may be several months before a final document is signed into policy. Please continue to familiarize yourself with the contents of that DRAFT because you will get another chance to provide feedback as necessary.

Upon DNI approval of the Intel Community Standard (ICS), the Office of the Deputy Chief of Staff, G-2, will provide implementation guidance accordingly. The ICS will contain a variety of changes that are expected to be phased in over a period of time. Planning and building SCIFs beyond 2012 will require a more in-depth relationship between the SIOs/SSOs/CSSOs and the U.S. Army Corp of Engineers. We will ensure that a winning way-ahead is developed and also ensure the SCIF Support Branch at DIA is fine tuned to the Army's SCIF requirements.

In the meantime, DCID 6/9 remains the policy to follow for physical security standards of SCIFs. There are only a few select organizations that have been specifically authorized by the DNI to use the construction security standards outlined in the DRAFT ICS to build ongoing SCIF projects. If your command has any questions about the SCIF construction standards, please contact the SCI Policy Staff for guidance. DIA SCIF Support Branch will continue their current role in supporting Army SCIF accreditation requirements.

You Can't Unring the Bell

Disclosures are permanent. Once the information has been disclosed, regardless of medium, it cannot be recalled or undone. This brings us to the topic of understanding and applying the definitions of mediums, or means of disclosure.

There are three ways that information is disclosed, those being through oral, visual and documentary means. While the first two seem intuitively obvious, documentary disclosures remain problematic in terms of understanding and application. This can be easily overcome when documentary disclosures are seen within the context of permanence. As a common frame of reference, consider disclosures relating to a photograph.

Oral Disclosures: Oral refers to your ability to convey information through conversation. Typically this is accomplished through briefings or presentations. The limiting factor is what can be conveyed through speech. In the case of our example of a photograph and oral disclosure, you could only describe what can be seen in the image and nothing more. Once you have told someone about the photograph, you are not in a position to take back what they have heard.

Visual Disclosures: Visual refers to your ability to actually show and allow for some temporal study and analysis of the information. With respect to our example, this means you could show or present the photograph. This does not mean that the audience for disclosure is free to take permanent custody of the photograph. As with the oral disclosure, you will never been in a position to take back what the individual recalls from seeing the photograph.

Documentary Disclosures: Documentary refers to your ability and authority to convey permanent physical custody of the information to be disclosed. In some instances, especially with respect to intelligence and intelligence related products (Category 8 CMI), this is also referred to as release. Release refers to the physical conveyance of the information. Documentary disclosure refers to the authority for both the medium of information and the custodial issue. Within the concept of permanence and thinking back to oral and visual mediums, when you request the authority for documentary disclosure, you are requesting the authority for permanent transfer of the information as presented in documentary form. A documentary disclosure of the photograph means permanent custody of it is now conveyed to the foreign government.

The authority for documentary disclosure is often requested in DDLs for extended visitors such as exchange or liaison officers. If you reflect on what the nature and purpose of that individual's mission is, documentary disclosures just don't make sense in all cases. Consider these examples:

Military Exchange Officer Program (MPEP): A foreign government individual assigned to a U.S. Army organization or activity for the purpose of filling a position normally reserved for Department of the Army (DA) personnel. The MPEP does not work for his parent country or government. While he may require access to classified documents to do his job, he has no requirement for the permanent custody of those documents.

Engineer and Scientist Exchange Program (ESEP): A foreign government civilian or military scientist or engineer assigned to a DA organization or activity for the purpose of conducting research, development, testing or evaluations. The ESEP does not work for his parent country or government. While he may require access to classified documents to do his job, he has no requirement for the permanent custody of those documents.

Cooperative Program Personnel (CPP): A foreign government individual that is assigned to a multinational program office hosted by the Department of the Army. The CPP reports to and takes their direction from a DA or DA appointed Program Manager (PM) or PM equivalent. While the CPP may require access to classified documents to do his job, he has no requirement for the permanent custody of those documents.

Foreign Liaison Officer (FLO): A foreign government civilian or military individual who is authorized by their government to act as an official repre-

sentative in its dealings with the U.S. Army. This interaction is in conjunction with programs, projects, operations, or agreements of mutual interest to the U.S. Army and the foreign government. Depending on the language contained within the terms of certification or similar supporting documentation, the FLO may be designated as conduit for documentary transfers back to their parent government.

As always, if you have any questions, give us a ring on the front end, as once the disclosure has been made, you can't unring that bell.

"Now Serving #37 at Window Five…"

The Foreign Disclosure/Security communities expend a great deal of time tracking and overseeing foreign visitors. Who would have thought a key individual in this effort was the person working window #5 at the Common Access Card (CAC)/ID Card section? I am referring to is the issuance of CACs to extended foreign visitors and identification cards to their dependants. There appears to be some confusion about what is or is not required for foreign visitors to obtain U.S. government identification, so lets' start with basics.

1. To be issued a CAC or ID card, an individual must prove two things: identity and sponsorship. This is the same for U.S. or foreign personnel. What varies are the source documents considered acceptable for these purposes.

2. DD Form 1172 is ***an application*** for a Uniformed Services Identification Card and DEERS enrollment. It is neither a form of identification nor proof of sponsorship.

3. Foreign military family members/ dependants are not covered under, nor are they tracked by, the International Visit Program (IVP). As such, they will not have a Request for Visit Authorization (RVA).

When CAC/ID cards are issued incorrectly, it places the Army and those involved in the issuance at risk. In June of 2009, AF136-3026-IP became the consolidated DoD regulation for *"Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel."* Rule 13 of this regulation reads:

If the person's status is:

Military Affiliate (formerly identified as Foreign military member) and his or her dependents)

Then eligibility is verified by:

The Invitational Travel Order (ITO) or other document establishing his or her sponsorship or invitation to the United States in lieu of a marriage certificate. A foreign passport and Visa may be used to verify foreign military personnel dependents since the dependents need legal documents to accompany the member to the United States. A secondary form of identification may include foreign driver's license (if not in English, will require English translation).

In the absence of an approved RVA, the issue becomes under what authority is the US Army sponsor providing this certification? The sad fact of the matter is there isn't any.

What you can do:

1. Ensure the CAC/ID issuing authority at your installation/command knows to ask for either an ITO or RVA when dealing with official foreign visitors and their requests for CACs. Also make them aware that the RVA process does not apply to family members and dependants.

2. Ensure the persons taking the "Military Affiliate" through the process, do not take any action without an approved RVA for both initial issue and renewals of CACs/ID cards.

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

INTERIM PROTECTION PLANNING

The Army Program Protection Process exists to protect Army Acquisition research and technology programs as they traverse the acquisition cycle and achieve milestones. This Process consists of five basic steps. Those five steps are the identification of Critical Program Information (CPI), Analysis of the Threat, Analysis of the Vulnerability, Evaluation of the Risk and Development of the Countermeasures. Following these five steps and bringing it all together is the implementation of countermeasures. This total process can take over ten months to complete! So this begs the question, what do organizations do during those ten or more months if sensitive information is discovered? Should organizational programs wait until the fifth step to develop their countermeasures, especially if it could take several months to get there? Doing so could leave possible sensitive information open to disclosure for adversaries. It just doesn't make sense, does it?

Take the case of the Joint IED Neutralizer (JIN). This was a Counter-IED device that was developed and produced with plans of sending it into Iraq. The JIN program ended up being scrapped. Why? Because before JIN was sent, a high level government official's briefing to an audience that included a reporter resulted in the 12 February 2006 LA Times article revealing how JIN worked. In less than one week, a JIHADI website posted instructions on countering the JIN. Even the President at the time, George Bush, stated during his speech March 2006 to the George Washington University, "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."

So, what can be done to protect sensitivities identified during the first step of the Army Program Protection Process? Develop an Interim Protection Plan (IPP). The IPP, modeled after and designed to evolve into the Program Protection Plan (PPP), is designed to provide a means for a program manager to identify and implement Interim Countermeasures (ICMs) which immediately focus protection on the CPI or sensitive information. These ICMs are normally identified immediately following the CPI Assessment in a Program Protection Working Group (PP WG). The IPP also works to develop and/or update the program's Security Classification Guide and Foreign Disclosure documents, such as the Delegation of Disclosure Letter and Technology Assessment/Control Plan. This ensures the CPI is protected in those documents. The main benefit of an IPP is it provides immediate protection to a program's CPI while the program is awaiting completion of the Multi-Disciplinary Counterintelligence Threat Assessment and the analysis required to develop and implement tailored countermeasures as part of a PPP. The PP WG will identify ICMs for use in developing the standard operating procedures and implementing countermeasures focused on the protection of CPI at the locations where CPI is present.

Some examples of ICM's are Limited Access Rosters, Document Accountability Systems, End Item Accountability, Pre-publication/Presentation Reviews, Manual Destruction Procedures and Tailored Counterintelligence Briefs. These are just a small example of the numerous ICM's that are available, and in many cases organizations are already following these type procedures.

The main thing to remember is that any protection afforded to a research or technology project/program is ineffective unless it is implemented. Merely recording data for the purpose of recording data does nothing to enhance the protection for the Soldier.

Any questions regarding the Army Program Protection Process can be directed to the author at William.e.daniel@mi.army.mil or the Army Research and Technology Protection Center Operations Officer at Gerald.wayne.boardman@us.army.mil

ARTPC POC

Mr. Dick Henson
Chief, ARTPC
Ph: (703) 601-1929
Richard.Henson@us.army.mil

Training Opportunities

The Defense Security Service (DSS) Academy, and the Security Education, Training and Awareness Directorate (SETA) offers more than training. I encourage you to subscribe to their SETA Newsletter "Focus on Security" to get the latest on recently released courses and products.

SETA also offers a new subscriber email service. Subscribers to the service will receive periodic emails regarding current or upcoming SETA events, products, services, processes, and projects. This will allow the subscribers a "peek behind the curtain" to see the things that we are working on as well as items of interest for our students.

For more information go to http://dssa.dss.mil/seta/seta.html.

Director of National Intelligence (DNI) Special Security Center

DCID 6/9 Physical Security Seminar
- Nov 16-20, 2009 - Linthicum, MD
- Dec 7-11, 2009 - Chantilly, VA

GOV Special Security Officer Course
- Nov 30 – Dec 4, 2009 - Chantilly, VA

Manager's SSO Course (MSSOC) (Gov only)
- Oct 19-23, 2009 - Chantilly, VA

For instructions on registering for DNI courses email SSC directly at dni-ssc-training@dni.gov or visit https://www.intelink.gov/sites/ssc.

National Security Training Institute

Information Systems Security Training (ISST)
- Oct 21-23, 2009 - Chantilly, VA

Practical SCIF Construction (PSC)
- Dec 7-11, 2009 - Chantilly, VA

Security Presentation Skills Seminar (SPSS)
- Nov 18-20, 2009 - Chantilly, VA

For course descriptions, cost and registration information go to http://nstii.org/index.htm

Joint Counterintelligence Training Academy (JCITA)
For registration and availability, email JCITARegister@jcita.cifa.smil.mil.

Army Regulations:

1. **AR 380-5**, *Information Security* - Formal Staffing
2. **AR 380-10**, *Foreign Disclosure* - Internal Review
3. **AR 380-13**, *Acquisition & Storage of Information* - OTJAG
4. **AR 380-27**, *TEMPEST* - Army Publications Directorate
5. **AR 380-28**, *DA Special Security System* - Formal Staffing
6. **AR 380-40**, *Communications Security* - G2/G6 Working Groups
7. **AR 380-49**, *Industrial Security* - Formal Staffing
8. **AR 380-53**, *Information System Security Monitoring* - Formal Staffing
9. **AR 380-67**, *Personnel Security* - Informal Staffing
10. **AR 381-45**, *Investigative Records Repository* - OTJAG

DoD Security Professional Education Development (SPeD) Certification Program

We are in the throes of it all! As previously explained in the May edition, the DoD Security Training Council (DSTC) and sub-working group members have been busy molding and shaping the program. Skill Standards Review is almost complete. We've reached out Army-wide to Subject Matter Experts (SMEs) who participated in the building of this crucial component of the program design. I want to thank everyone, especially our SMEs, who have participated in the skill standards review. We've received a tremendous amount of feedback and valuable information. There is still much to accomplish as we quickly move on develop the program design, certification blueprint, assessment strategies and develop policy and procedures. We have an aggressive schedule and expect to "soft launch" this project in Summer 2010.

Information regarding this program was shared with principal security personnel via VTC and telephone conferencing on September 2. It was during this forum, that we requested volunteers to serve on a certification committee. The purpose of this committee is to share information; collaborate on actions requiring input; and to carry out tasks.

Below are the issuances that drive this effort and provide a platform on which to build this national certification:

Executive Order 13434, National Security Professional Development, May 17, 2007

- Mandates policy to promote the education, training and experience of current and future professionals in national security positions.

DoD Instruction 3305.13, DoD Security Training, December 18, 2007

- Assigns the Director, Defense Security Service (DSS), as the functional manager responsible for the execution and maintenance of DoD security training.
- Establishes and designates the Security Professional Education Development (SPeD) Program as the DoD security training program.
- Establishes the DoD Security Training Council (DSTC) as an advisory body on DoD security training that reports to the Defense Intelligence Training and Education Board (DITEB).

DoD Instruction 3115.11, DoD Intelligence Human Capital Management Operations, January 22, 2009

- Designates the USDI as the accreditation and certification official for Defense Intelligence Components and designates the Director, USDI Human Capital Management Office (HCMO) to serve as the Chief Human Capital Officer.

DoD Manual 3305.13, Accreditation and Certification Manual, Draft Aug 2009

- Serves as the implementation guide for DoDI 3305.13.

Stay tuned!

Ms. Luisa Garza
SETA Program Manager

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

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