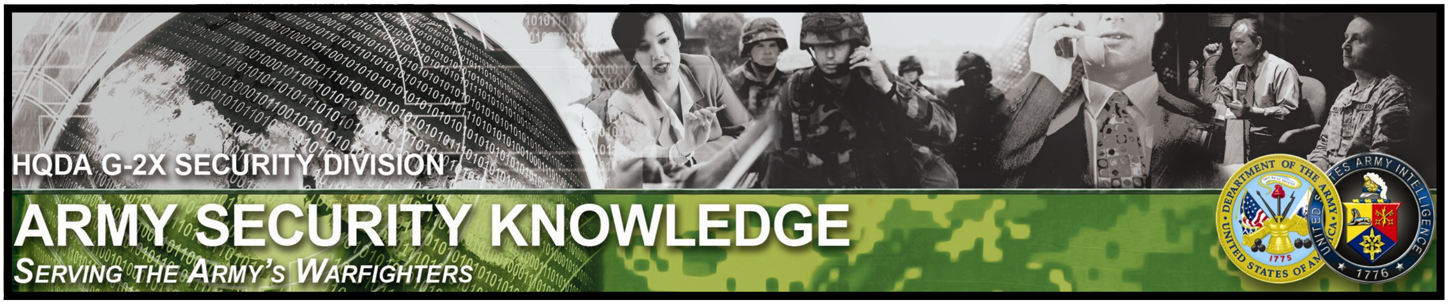


HQDA G-2X SECURITY DIVISION

ARMY SECURITY KNOWLEDGE

SERVING THE ARMY'S WARFIGHTERS

Senior Security Advisor Message

My fellow security professionals. We are receiving very positive feedback on these newsletter communications. Please keep the comments coming and let us know your thoughts.

On 26 Mar 2010, I was formally appointed to the Defense Intelligence Senior Level with Mr. James T. Faust, Assistant Deputy Chief of Staff, G-2, presiding. This event allowed me the time to reflect on its significance, not only to me personally, but to our security profession. This appointment will serve as a catalyst for raising the level of importance of the security profession across the Army. I hope that this is just one of many more senior level security positions to be created in the future. I am honored to serve all of you and the United States Army in this important role.

Our Army Investigative Enterprise Solution (AIES) is being deployed. The Personnel Security Investigation Center of Excellence (PSI-CoE) has been established and is rapidly growing at Aberdeen Proving Ground, MD. In case this is new to you, this is your one-stop-shop for the submission of all personnel security investigations for the U.S. Army. The concept is sound, tested and proven. It is the culmination of two years of concept development, prototype testing, and continuous improvement. Army senior leadership endorse AIES, which will improve Army readiness, save Army resources and embrace the enterprise approach to conducting business.

In order to support the Army's BRAC hiring surge challenge, the Civilian Personnel Advisory Centers (CPACs) will be in our first wave of deployment along with their Servicing Security Offices. All other Security Offices will follow. Deployment to Security Offices will be coordinated through all Command, ASCC, and DRU Headquarters. Most Headquarters elements have already been contacted. Army Accessions will join the process early next fiscal year followed by the National Guard and Reserve components.

If you need assistance, please contact the PSI-CoE help line at (410) 278-4194 or DSN 298-4104 or the AIES Deployment Director, Ms. Judy Tang, Judy.Tang@us.army.mil at (703) 695-3053 or DSN 225-3053.

This is transformational, and we look forward to serving you!

I also want to take this opportunity to remind all security managers of their continued responsibility with regard to the education of our soldiers reference Question 21 on the Questionnaire for National Security Positions. As you all know, the SECDEF officially mandated the new Q#21 language effective 18 April 2008. The language was subsequently modified on the Standard Forms. However, it is imperative that this new language with regard to Q#21 be re-emphasized to soldiers when completing these forms. Remember, we want to encourage the well being of our soldiers. It is a mark of strength and maturity to seek appropriate healthcare. Let's ensure we serve those who serve us.

Finally, I want to thank Mr. Carl Johnson for allowing me to come and speak to the assembled security professionals at his recent conference in Germany. USAREUR put on an excellent conference, exchanged and presented valuable information and provided a forum for security professionals to network and share real world experiences. Well done Carl.

Thank you all for your continued support and please remember those we serve - our Soldiers!

Sincerely,

Patricia P. Stokes

Arrivals

Ms. Teane Smith

Personnel Security Reform Integration and Policy Development

Ms. Smith personnel security experience include assignments at a joint intelligence activity, DISCO, DoD Security Services Center, HQAF Surgeon General and Langley AFB. Ms. Smith will be supporting key personnel security initiatives to include AIES. Welcome to G-2!

April 2010
Inside This Issue

ARTPC POC

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

Tailored Protection for Rapid Acquisition Efforts

A critical requirement for all rapid acquisition efforts is to provide the warfighter a system that has not been compromised. When fielded, rapid acquisition efforts – be it commercial off the shelf technology (COTS), modified COTS or government furnished equipment, or future force technology insertions – meet a current operational need. Unfortunately, information released during the rapid R&D and acquisition process may provide the enemy with sufficient information to develop suitable countermeasures – even before the system is fielded. The fact is our enemies actively harvest worldwide open-source information, and what we say about a certain piece of technology may limit the combat effective life of that system. To maintain our technological overmatch, it is imperative that rapid acquisition technologies, and often the true operational capabilities, remain protected throughout the acquisition and fielding process.

Various DoD and Army regulatory requirements, to include DoDI 5000.2, DoDD 5200.39, DoD 5200.1-M, AR 70-1, and DA PAM 70-3, address technology protection in formal acquisition programs. Due to operational realities and short timelines, rapid acquisition efforts by-pass the traditional acquisition process model. To assist rapid acquisition managers, the Army Research and Technology Protection Center (ARTPC), Army G-2, developed the Accelerated Fielding Initiative (AFI) team to address the protection of quick reaction capabilities and technologies.

There is no “one size fits all” for the protection of quick reaction capabilities. In some cases, the technology in use is well known, but the intended purpose or target is unique and often sensitive. In other cases, there may be state-of-the-art technology involved, the designated operational unit’s mission could be sensitive, or the system might be owned by a foreign government. The ARTPC AFI team works with project leaders and technology developers to assess any requirements to protect critical and/or sensitive information and then helps address the means to implement this protection. Some essentials about the ARTPC AFI team:

∗ Protection is designed based upon the needs of the project. This could take the form of a security classification guide, an OPSEC plan, tailored public affairs guidance, or customized countermeasures focused on sensitive item(s) – or any combination of these. The goal with all protection measures is easy to implement countermeasures that protect the technology and capability.

∗ Understanding that rapid acquisition projects are often short staffed, the AFI team will assist with building all protection related products for the project.

∗ The ARTPC AFI team is fully funded by Army G-2. The team is flexible and works within project timelines to deliver common sense protection solutions.

Let the ARTPC AFI team assist with extending the combat effective lifespan of a system. We owe it to the warfighter to field not only a system that works, but also a system that is uncompromised. If you have a rapid acquisition project and have protection concerns, contact the ARTPC AFI Team at 703-601-1576/1568.

A critical requirement for all acquisition efforts is to provide the user a system that has not been compromised

Communications Security

COMSEC / TEMPEST / ISSM POCS

Mr. Richard Niederkohr
Lead, COMSEC/TEMPEST/ISSM
Ph: (703) 602-4628
Rick.Niederkohr@us.army.mil

Mr. Harry Byrd, Jr.
Ph: (703) 607-1874
Harry.Byrd@us.army.mil

Technical Security Monitoring Team

Since the last edition of the DCS G-2 newsletter, there have been some recent developments within the Technical Security team's area of responsibility. The Technical Security Team continues to focus on ensuring the Soldier's interests are heard and addressed in a timely fashion so personnel can have the necessary changes in policy to function effectively and achieve mission success. Accordingly, the following issues are continuing to be worked diligently to ensure objectives are met in a timely manner.

Currently, AR 380-27, Control of Compromising Emanations (TEMPEST), has been approved by the Army Publishing Directorate and is now pending Secretary of the Army signature. A noteworthy change to the new publication will be the change in classification of the regulation. Previously, its predecessor (AR 381-14) was classified, but the new regulation will be unclassified and more easily available through Army Publishing Directorate (APD) Army Knowledge On Line (AKOL). The new regulation will also include Protected Distribution Systems (PDS).

AR 380-53, Communications Security (COMSEC) Monitoring (ISSM), was entered into formal staffing and all comments have been adjudicated, and as of 12 March submitted to the Office of The Judge Adjutant General (OJAG) and the Army Office of General Counsel for review. It is our intent to have AR 380-53 submitted to APD within 60 days once it is approved by TJAG.

A significant accomplishment concerning AR 380-53 is the biennial request for Certification of ISSM. We would like to take this opportunity to thank all the Army commands for their contributory efforts in the Army's ability to achieve total compliance of approved certification requests until 30 September 2011.

Another responsibility of the Technical Security Team is the publication of AR 380-40. AR 380-40 is pending leadership decision and we will continue to keep the COMSEC community abreast on any developments concerning its status or policy changes, which directly affect personnel associated with the safeguarding, control and accountability of COMSEC material.

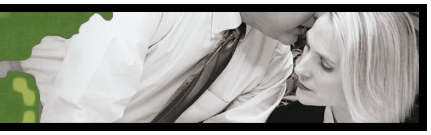
An important event within the COMSEC community is the GIPC Conference, which is scheduled to occur 5-9 May at Fort Huachuca, AZ. HQDA DCS G-2 will be part of the Policy and Procedures workshop this year. Topics to be covered during the workshops by the Technical Security Team include black key, IIA-002-2010, and Controlled High Value Products. This event, which occurs on an annual basis, is an opportunity for the field to present questions and ideas to the entire COMSEC community on a large scale and bring back recent policy changes to the unit.

The Technical Security Team also hosts video-teleconferences (VTCs)/telephone-conferences (TCONs) on a quarterly basis, to ensure information is being relayed in the field and to solicit input from the various commands. We encourage the commands to continue their strong attendance and participation as they have in the recent conferences. These conferences serve as a conduit to ensure the needs of the Soldier are heard and in turn incorporated into Army policy. The next Technical Security VTC/TCON is scheduled to occur on 15 June 2010.

The DIASPOM webpage, which can be accessed via SIPRNET at http://www.dami.army.smil.mil/offices/dami-ch/daispom/comsec.asp. serves as an excellent source for guidance and access to NSA newsletters reflecting recent news within the COMSEC world. Please take time to view this site if searching for recent changes concerning COMSEC related issues.

In closing, the Technical Security Team remains vigilant in addressing the needs of the Army and to ensure the Soldier's mission is successful and we welcome comments concerning this article. If you have any questions, comments or suggestions, please feel free to contact Mr. Rick Niederkohr at (703)602-4628 or rick.niederkohr@us.army.mil and Harry F. Byrd Jr. at (703)607-1874 or harry.byrd@us.army.mil. We look forward to hearing from you.

Foreign Disclosure



Foreign Disclosure POCs

Mr. Scott Shultz
Chief, Foreign Disclosure
Ph: (703) 695-1096
Scott.Schultz@us.army.mil

Technology is a Wonderful Thing

by Dave Grob

Technology is wonderful thing, or so the saying goes. However, the current tendency in the foreign disclosure community is to lump all modeling and simulation (M&S) issues into the Category 3 bin of Classified Military Information (CMI). When this is done as a default, the results are usually less than wonderful. A portion of this problem can be attributed to not understanding all that is involved with M&S. Let's begin with the basics.

Model: A representation, generally in miniature, to show the construction or appearance of something. Models may also be virtual.

Simulation: The representation of the behavior or characteristics of one system through the use of another system.

An easy way to envision this relationship is with a chess set. The pieces on the board are models used to represent the various combatants, each with their own capabilities. These pieces are used to simulate tactics and strategies that may have military application. This use or application is the simulation.

In trying to identify and articulate disclosure guidance for M&S issues, the FDO has to know what part of the M&S pipeline they are dealing with. For our purposes, this pipeline has three distinct segments of the information considered for disclosure:

Segment I: What is being modeled or simulated.

Segment II: The actual model and/or simulation.

Segment III: The output from the model or simulation.

In all cases, regardless of the segment, the FDO must know what category of CMI they are dealing with as it relates to the level of classification of the information, who the proponent of the information is, and the nature of the current disclosure authorities in place for the country in question. Consider these examples currently found in Delegation of Disclosure Authority Letters (DDLs) for M&S related programs:

1. *Live, Virtual and Constructive (LVC) Models and Simulations Information concerning the development, application and verification/ validation of M&S used to estimate item, system, force and theater level operational performance for conventional (including non-lethal) weapons.*

"*Information concerning the development, application and verification/ validation of M&S.*" This would fall into Segment II. It deals with the actual M&S itself, and as such, could be considered Category 2 or 3 CMI. The difference being the nature or maturity of the M&S process itself with respect to fielding and utilization.

2. *Data describing capabilities of military systems, tactics used by forces and terrain data that are used in combat M&S.*

In this case, we have both Category 1 CMI (*tactics*) and Category 2 CMI (*capabilities of military systems*). We could also be dealing with Category 3 CMI if the *"capabilities of military systems"* involves those that have not completed operational suitability testing or have not been adopted for military use or production.

As you can see by now there is no single category for M&S information and that M&S disclosure issues also relate to what part of the M&S pipeline you are dealing with. While we don't expect the FDO to be any more of an M&S expert than we are (and we aren't), we do expect that they can explain all of this to their organizations in order to properly capture all of the requirements by Category of CMI and all the other associated disclosure implications. Technology is a wonderful thing.

As always, if you have any questions, please feel free to contact your regional desk officer.

Mike Shropshire
Regional Desk Officer Team Chief
Portfolio includes Israel and Japan
HQDA, ODCS G-2, DAMI-CDS
(703) 695-1081

Sam Ault
Asian/South and Central American Desk Officer
Portfolio also includes France
HQDA, ODCS G-2, DAMI-CDS
(703) 695-1091

Dave Grob
European Regional Desk Officer
HQDA, ODCS G-2, DAMI-CDS
(703) 695-1959

Ashleigh Rogiers
African/Middle Eastern Desk Officer
Portfolio includes the UK, Canada, and NATO
HQDA, ODCS G-2, DAMI-CDS
(703) 695-1085

Functional Management

The Army Security Manpower Model Data Call: It's Important

By the time you read this article, chances are you received the Army Security Manpower Model Data Call, completed it, or at least heard of it. It is important that Army security professionals complete the Data Call and respond to G-2 Security Division by the suspense date (16 April 2010).

The Army Security Manpower Model will establish a standard security structure for Army Commands (ACOMs), Army Service Component Commands (ASCCs), and Direct Reporting Units (DRUs). The Office of the Deputy Chief of Staff, G-2 Security Division in coordination with the U.S. Army Manpower Analysis Agency (USAMAA) are developing the Security Manpower Model in support of the Army Campaign Plan (ACP), Decision Point 91 (DP91) and Decision Point 59 (DP59). The bottom line concept for DP91 and DP59 as it relates to Army security, is that all Commands (ACOMs, ASCCs, and DRUs) are responsible for the functional management and oversight of their security programs.

Many commands are working these programs with minimal resources; others may be over; and some commands are just right. The fact is – we don't know. Therefore, we're developing the Security Manpower Model through the following five phase process to provide a tool to help determine appropriate manpower strength to support current mission requirements.

Phase 1 – Select the function. Frame the problem by identifying the type of security function(s) to analyze, and then select the level the security function(s) execute. This process establishes a security baseline.

Phase 2 – Business Process Analysis. The next step evolved through coordination with USAMAA and the security subject matter experts who have in-depth knowledge of the security processes that comprise the security functions under study. This step began with an initial development of business process models. The business process models took on the form of a process map similar to those created using Lean Six Sigma methodology. When building the process model, the Working Group comprised of G-2 and Command subject matter experts, and facilitated by USAMAA representatives, considered a set of basic questions. Here are examples of the questions:

What takes place inside this function? Why does this function exist in this organization and is it performed elsewhere within the command, or across the Army? Is this function mandated by a law, regulation, or policy? What creates the demand for the output generated by these processes? Is the demand driven by internal or external forces?

In order to have a better understanding of your security functions, the Working Group developed a candidate list of workload and process drivers.

Phase 3 – Select Potential Modeling and Simulation Approaches. Once the Working Group mapped out the business process and identified the modeling drivers, we began to select candidate approaches, also known as the Data Call.

Once the Data Call is complete, the Working Group will resume the continuous verification by ensuring the data logically fits the security functions and processes being modeled.

Phase 4 – Develop models, create simulations. In this phase, the Working Group will take the process model created in phase 2, and combine it with the Data Call results in phase 3 to create a model that can be populated with data to become useful and useable.

By the end of this phase, the Working Group should have confidence that the conceptual security model is a reasonable representation of the actual process, and the set of equations or simulations are reasonably accurate.

Phase 5 – Validation. Validation is defined as ensuring that the model represents the real world to a degree sufficient enough for the model to be useful. A model may not be able to address all contingencies or answer every possible question, but a model can be useful and valid if it addresses the questions for which it was designed.

If a model employs workload or process drivers that were developed using subject matter expert opinion, but was not statistically validated, then the model may be approved for up to one year. If the model employs statistically validated drivers, which is our intent, the model may be approved for up to three years.

Once the data is received and validated from the Commands and the previous five phases have been completed, the result should be a security model that is verified, and approved for use as an independent tool for Commands to validate and justify current and additional security resources. The Army Security Manpower Model should be complete by June – July 2010, at which time G-2 Security will present the Model to Army Leadership and request resource re-alignment or adjustments to execute and manage their security programs consistent with DP 91 and 59.

Mr. Drew McCall
Security Functional Manager
703-695-2569
Andrew.mccall@us.army.mil

Information Security

INFOSEC POCs

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

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

Development of national policy for the implementation of controlled unclassified information (CUI) is continuing. DoD and other national level agencies continue to work out the details for a system that will standardize the protection and handling on sensitive unclassified information.

The President has issued a new Executive Order dealing with classified information. Executive Order 13526 replaces Executive Order 12958. As expected, there are several notable changes in the order. The establishment of a National Declassification Center is one.

The center will centralize declassification efforts under one roof and will be managed by the National Archives. How the center will be staffed and what role will be played by the agencies is yet undecided. It seems certain that the Army will have a continuing need to manage it's own program, in addition to involvement in the National Declassification Center.

The new order also requires that all Original Classification Authorities (OCAs) are required to receive training annually. All derivative classifiers will require training every two years. Those derivative classifiers who do not receive training will no longer be authorized to apply derivative classification. The order also states that the Army is required to review all existing classification guides to ensure they conform to the tenants of the new order. It is not known at this time how DoD will implement the new requirements. The changes in the order itself will be reflected in the revision of AR 380-5.

*****

DoD has issued a draft manual concerning Mandatory Declassification Review (MDR). The draft manual is separate from DoD 5200.1R and addresses only MDR. The draft manual more closely aligns the MDR process with the current Freedom of Information Act process (requiring a review under the terms of the FOIA prior to any release). Army G-2 is working with OSD, Army General Counsel and the Army FOIA Office in order to ensure the process will work well within the Army. When DoD issues the manual, our current plan is to issue an Army version as a separate Army Manual. We will keep you informed of our progress.

Writer's Block: Resources for SCG Authors

Trying to write a Security Classification Guide (SCG) but don't know where to start? Check out some of the resources below:

In 2006, the Army G-2 developed a standardized methodology for making original classification decisions, along with an online tutorial, as an Army "best business practice." To assist those working to update, review or develop SCGs, this tool outlines a standardized method of making objective decisions about subjective issues- a key challenge in SCG writing. Extremely well-written and very user-friendly, this document takes you through every aspect of SCG creation and even includes quiz questions so you can test your knowledge as you go. It is available at: http://www.dami.army.pentagon.mil/offices/dami-cd/classification%20mgmt%20tutorial.pdf

SENTRY, a web-based tool supporting the Foreign Disclosure, Security, and Counterintelligence Communities on SIPRNet, provides a centralized repository for a great deal of information, including security classification guides. Listing over 500 guides in the main database and the archive, this a great resource to review already existing guides and get the latest information on Army technology, weapons and systems. Accounts can be requested at http://www.dami.army.smil.mil/offices/dami-cd/guardian.asp#

The U.S. Army Communications-Electronics Life Cycle Management Command Regulation 380-3. Published in January 06, this document provides a step-by-step methodology for writing a SCG. Starting at the beginning of the process with background and preparation guidelines and continuing through four chapters and a detailed appendix which explains how to go about the actual writing of the guide. You can find the complete document at: http://www.sed.monmouth.army.mil/114/C-E%20LCMC%20380-3%2020060104.pdf

The Defense Security Service Academy (DSSA) provides a plethora of online web-based training modules, including one focused solely on SCGs! The Security Classification Guidance Course identifies U.S. Government and DoD policies governing SCG creation and outlines the process for developing classification and declassification guidance. Original Classification Authorities (OCAs) and derivative classifiers alike will benefit from the lessons offered in this training, and at a length of 2 hours the course is short enough to fit into most busy schedules. The student guides included in the training module are great job-aides in explaining the different SCG sections and providing guidance on SCG writing. Enroll online at:
http://dssa.dss.mil/seta/courses.html

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

What is the Industrial Security Program?

The Department of Defense states that Industrial Security is the portion of information security concerned with the protection of classified information in the custody of U.S. industry. The purpose of the Industrial Security Program is to safeguard classified information that may be or has been released to current, prospective or former contractors.

To promote our national interests, the U.S. Government issues contracts, licenses, and grants to nongovernment organizations to include Universities, consultants and contractors. National security also requires that the industrial security program promote economic and technological interests of the U.S. The U.S. industry develops and produces the majority of our nation's defense technology – much of which is classified – and as a result, plays a significant role in creating and protecting the information that is vital to our nation's security.

The National Industrial Security Program (NISP) was established by Executive Order 12829, as amended, to ensure that cleared U.S. defense contractors safeguard the classified information in their possession. The National Security Council sets policy for the NISP, while the Director of the Information Security Oversight Office (ISOO) is the authority for implementation. Under the ISOO, the Secretary of Defense is the Executive Agent, but the NISP recognizes four different Cognizant Security Agencies, all of which have equal authority; the Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission.

Pursuant to the NISP is the establishment of the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC is chaired by the Information Security Oversight Office (ISOO) and has representation from DoD, non-DoD Agencies and 7 appointed members of Industry that collectively represent all of industry. The NISPPAC is responsible for recommending changes in industrial security policy through modifications to the NISP, its implementing directives, and DoD 5220.22-R, “Industrial Security Regulation”. The NISPPAC also advises ISOO on all matters concerning the policies of the NISP, including recommended changes to those policies, and serves as a forum to discuss policy issues in dispute.

Currently, there are approximately 13,000 contractor facilities that are cleared for access to classified information. The Defense Security Service (DSS) estimates that around 11 million classified documents are in the hands of U.S. industry. At this time, there is no DoD database which provides the exact number of classified contracts the Army currently holds; however, a recent HQDA, G-2 data call was forwarded to the Army Commands, Direct Reporting Units and Army Service Component Commands in support of the Army Security Manpower Model to gather the total number of classified contracts.

To have access to U.S. classified information and participate in the NISP, a contractor must have a legitimate requirement, must demonstrate the ability to protect the classified information to the appropriate level, and must execute a Defense Security Agreement, DD Form 441, which is a legally binding document between the government and contractor. This Agreement sets forth the responsibilities of both parties and obligates the contractor to abide by the security requirements of DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

The Security Agreement (DD Form 441), executed between the government and all cleared facilities under the NISP, obligates the Government to provide the contractor appropriate classification guidance for the protection of the classified information, furnished to or generated by the contractor, in the performance of a classified contract. The Government fulfills this obligation by incorporating a “Security Requirements Clause” and a DD Form 254 for each classified contract. The “clause” identifies the contract as a “classified contract” and the DD Form 254 provides classification guidance.

The DD Form 254 is a contractual specification. It is as important as any other specification in a contract. It is the vehicle that provides the contractor with the security classification guidance necessary for the classified information to be received and generated under the contract. It was developed as a contractual document to capture all of the security requirements for a classified contract and legally bind the contractor to adhering to them in the execution of the contract.

The Federal Acquisition Regulation (FAR) requires that a DD Form 254 be integrated in each classified contract. The DD Form 254 provides the contractor (or a subcontractor) security requirements and the classification guidance that is necessary to execute a classified contract.

Ultimately, the purpose of the Industrial Security Program is to safeguard classified information in the custody of contractors.

The security of the U.S. depends in part on the proper handling and storage of classified information released to industry.

Personnel Security

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

Clearance Denial or Revocation: What are the Due Process options?

The Army CCF has denied or revoked a soldier or civilian's security clearance - what's next? When the Army Central Clearance Facility (CCF) makes a final determination to deny or revoke a soldier or civilian's security clearance, they do so based upon their inability to mitigate disqualifying information reported as part of the background investigation. Disqualifying information are those matters referenced in the national security adjudicative guidelines.

If a Letter Of Denial (LOD) or Letter Of Revocation (LOR) has been issued, what are the appeal or due process options?

The DoD 5200.2-R mandates that an individual who has been issued an LOD or LOR must be afforded the opportunity to appeal – either without a personal appearance directly to the Army Personnel Security Appeals Board (PSAB) or with a personal appearance to the Defense Office of Hearings and Appeals (DOHA).

The Army CCF includes a notice of Intent to Appeal (Army CCF Form 54) in all LOD and LOR correspondence. The LOD and LOR are forwarded to the Command Security Manager via Command channels. The Army CCF Form 54 outlines two appeal options that the subject can choose from:

One option is appealing directly to the Army PSAB; or
The other option is to request a personal appearance before a DOHA Administrative Judge.

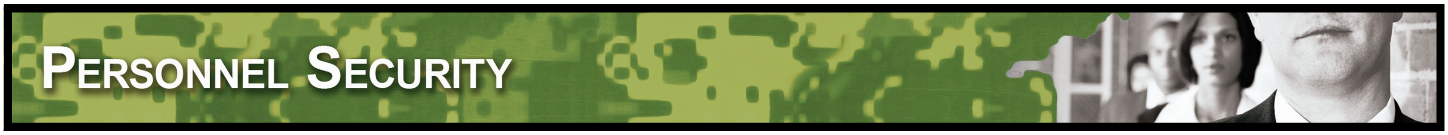
The subject should select his appeal option and submit the Form 54 directly to CCF within ***10 calendar*** days after receiving a LOD or LOR. In addition to selecting the desired appeal option, it is important that the individual complete the remaining portion of the form – which includes their current command and home addresses, and their active e-mail address. If the individual is deployed, the Command Security Manager is responsible to notify the Army CCF the dates of his or her employment and the expected return date. A deployment does ***not dismiss*** the individual's responsibility to address the concerns outlined in a LOD or LOR, ***nor does it guarantee*** that the individual will retain their security clearance.

What are the differences between the two appeal options and how is the final appeal determination made?

When appealing directly to the PSAB, the Army CCF provides all of the pertinent documents (to include the background investigation, the statement of reasons and/or letter of intent, the rebuttal and command response, is included, as well as any other correspondence that identifies the disqualifying information and final determination) to the PSAB. It is important to note that when the individual declares their intent to appeal, any supporting documentation which may not have been included in a response to a LOD/SOR, as necessary, should be submitted through the command to the Chairman.ArmyPSAB@mi.army.mil or by mail to:

U.S. Army Personnel Security Appeals Board Department of the Army, DCS G-2
ATTN: DAMI-CD (Rm 2D350)
1000 Army Pentagon
Washington, DC 20310-1000

The PSAB is comprised of a chairperson, who is a permanent member, and two rotating members from the Headquarters Department of Army staff elements, who do not hold a position in the security field. The rotating members can include Army officers with the rank of Lieutenant Colonel or Colonel. To ensure a fair and equitable decision process, the PSAB membership provides a mix of background and experience. Each PSAB member independently reviews the case file of each individual appeal and renders an official vote. The PSAB board convenes monthly and votes are officiated. The individual will receive an official written notification, through command channels, of the final determination that has been made by the board.



If the other appeal option is chosen, the individual can request a personal appearance before a DOHA Administrative Judge. It is important to note that there are important differences in the appeal process when compared to a direct appeal to the PSAB.

Once the Army CCF receives the Form 54, they prepare the appeal packet and send it directly to the DOHA. Appeal packets do not change based on an appeal option; the DOHA and PSAB receive the same information from the CCF.

The DOHA will contact the individual to schedule a personal appearance at a mutually convenient time for the appellant and the Administrative Judge. Depending on the individual's location (inside or outside the continental United States), the personal appearance may take place via video teleconference. At the time of notification, the individual will also be informed how to submit additional information/documentation for consideration prior to or at the personal appearance.

The DOHA creates official transcripts of all personal appearances; in addition, the DOHA Administrative Judge prepares a summary that identifies findings of fact, analysis, and concludes with a ***non-binding*** recommendation to be presented to the Army PSAB. The Army PSAB will review the case and make a final determination, in accordance with DoD 5200.2-R. Appeals to the DOHA are reviewed by the Army PSAB in the same manner as if they were appealed directly to the PSAB, except they will also ***consider*** the DOHA recommendation.

So, if the PSAB makes the final determination, what is the benefit of going to the DOHA at all? Although for each appeal option, an explanation along with documentation must be submitted, the personal appearance before an Administrative Judge provides a unique opportunity for the appellant to ***verbally*** explain their circumstances which led to a decision to deny or revoke the security clearance. The personal appearance provides an opportunity to communicate with the DOHA Administrative Judge by posing and/or responding to specific questions regarding the circumstances that lead to the final denial or revocation of the individual's security clearance.

A recommendation from the DOHA to the PSAB will generally occur within 60 days of receipt of the request. Once the PSAB receives the Administrative Judge's recommendation, a final decision can be expected in approximately 30 additional days. If the individual appeals directly to the PSAB, a final decision will generally be made in 60 days.

There are generally three specific outcomes that can occur by the board with respect to the final determination:

∗ The PSAB may deny the appeal and uphold the Army CCF clearance denial or revocation decision. An individual may request reconsideration of the denial or revocation through their command directly to Army CCF, no earlier than one year from the date of the PSAB determination.

∗ The PSAB may grant the appeal, which will approve security clearance eligibility; and, if previously revoked, restore the security clearance.

∗ The PSAB may grant the appeal, on a conditional basis. A conditional security clearance requires the involvement of the Commander to ensure the individual is meeting the requirements of the conditional security clearance (e.g., monitoring financial obligations to ensure avoidance of any new derogatory debts).

The Army CCF is notified of each PSAB determination, and will reflect the decision in the Joint Personnel and Adjudication System (JPAS). Any change to the individual's security clearance eligibility will be updated accordingly.

Centralizing Personnel Security Investigations (PSI)

The administrative processing of all Army personnel security and suitability investigations (PSIs) is being centralized into the Personnel Security Investigations Center of Excellence (PSI-CoE) for submission to the Office of Personnel Management (OPM). The PSI-CoE is located at Aberdeen Proving Ground, Maryland. This centralization includes investigations required for initial new hires, periodic reinvestigations, upgraded investigations to support a new clearance requirement, and investigations required in determining a contractor's suitability for the duty position being filled. This centralization will not include the processing of contractors requiring a security clearance - the exception being PSIs needed for our Contract Linguist population, which will be processed and submitted to OPM by the PSI-CoE.

The process of migrating Army investigation submissions through the PSI-CoE has been broken into four phases. The first phase of began with the Civilian Personnel Advisory Centers (CPAC). The second phase has begun involving the installation and organizational security offices that support a CPAC in conjunction with all other active Army security offices. The third phase will integrate Accessions Command and the fourth phase will include the organizations of the Army National Guard and Army Reserve. Integration of the active Army including Accessions is scheduled for completion before the end of this calendar year, National Guard and Reserves are scheduled for integration before April 2011. "Integrated" into AIES consists of being a registered user of the Personnel Security Investigation Portal (PSIP), and requesting ALL investigations through that portal. Other means of investigation requests or initiations will no longer be available for organizations enrolled in AIES.

What does this mean to the requester?

Instead of the security office initiating and preparing subject packages for submission to the OPM, the requester will now submit a request for an investigation for an individual (subject) using our online portal. The PSI-CoE will ask for the requester's assistance up front in directing the subject to an office or location where fingerprints (if needed) can be done either electronically or on a hard card. Also, if the subject does not have fax or scan capability, the security office can assist in getting the required forms to the PSI-CoE on behalf of the subject.

How does the subject get notified and who works with the subject?

The PSI-CoE will initiate through e-QIP and invite the subject via e-mail to fill out the forms. The PSI-COE will work directly with the subject to ensure that their forms are properly completed and required attachments are received. The PSI-CoE will submit the entire package to OPM once all required documents are completed (i.e., e-QIP packet, OF306 and resume for initial civilian hires, signature pages, and fingerprints (hard copy on-hand or electronically submitted)). The requester and alternate requester identified on the original request will be copied on e-mails to the subject so they will know the status of the request.

How will the supported security office receive the necessary paperwork to render an interim clearance, exception appointment determination?

The requester and alternate requester will receive a copy of the subject's SF8x packet via encrypted e-mail from the PSI-CoE. The PSI-CoE will also update JPAS ("PSQ Sent Date" field) to show the date the investigation packet was submitted to OPM. This will give the security office the ability to confirm the investigation packet has been submitted. The PSI-CoE tracks the case until the investigation opens at OPM. The PSI-CoE has a "hotline" established with OPM that is used to request corrections for cases. This helps ensure the case does not get rejected for missing/discrepant data, unreadable attachments, or another issue that can be corrected to allow the case to schedule and open. It is recommended that security offices work with their supporting CPACs so a representative from the security office can be selected as the alternate requester on CPAC-submitted PSIP requests. This allows the security office to receive e-mails related to the request and receive a copy of the final SF8x for review.

What other documents will the supported security office receive to enable interim or other suitability decisions?

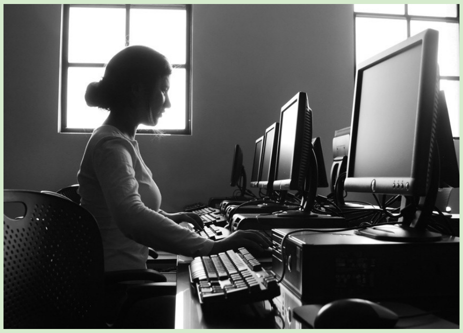
Since the PSI-COE uses "e-QIP, as designed", each investigative request will be processed so that advanced NAC results will be returned to the supported activity. Each organization/installation should have procedures in place for interim security clearance determinations and interim suitability determinations. The intent of the DA G2 and the PSI-CoE is not to change local policies or affect the relationships between the personnel and security offices ensuring that local procedures for interim determinations should continue as they have in the past.

When OPM concludes the investigation, the results will be returned to the Army CCF SOI (for cases that require a clearance adjudication) or to the requesting organization's SOI (for cases that require a suitability determination).

How do I register for a PSIP account?

The steps to register for PSIP: 1. Follow this link: https://www.psip.army.mil/; 2. Select "Register" in the top right hand corner of your web browser; 3. Fill out the requested information (please use your us.army.mil email account when possible); 4. Select "Register" at the bottom left hand side of your web browser. After you have registered you will see a red icon with an "X" inside of it. This indicates that you have successfully registered. You will receive an email within a few days, once you have been granted access to the full PSIP site. After receipt of the confirmation email, you may begin to use the new portal for the submission of PSI requests.

Your support is needed to ensure a smooth transition. All security offices that currently support a local CPAC for security investigation processing must immediately transition to AIES for all of their investigation submission requirements. That is, ALL PSIs that require the use of a SF-85, SF85P, or SF-86 form will be initiated using the PSI portal. If you have questions regarding the use of AIES, please do not hesitate to contact the PSI-CoE help line at (410) 278-4194 or DSN 298-4194 or the AIES Deployment Director, Ms. Judy Tang, Judy.Tang@us.army.mil, at (703)-695-3053 or DSN 225-3053.



SCI POLICY POCs

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

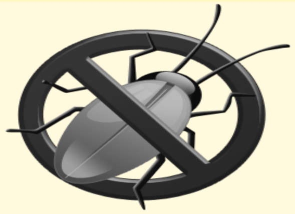
Contractor Support Element SCI Initiatives

As you know, the Army has been using Lean Six Sigma (LSS) as a continuous process improvement methodology to transform the way the Army does business. Several months ago, INSCOM's, Contractor Support Element (CSE), the Army's centralized operation for SCI contracting support began LSS projects focused on improving the overall SCI Contracting processes. CSE, under the authority of the INSCOM G-2, manages and provides security oversight for approximately 1900 active SCI contracts which enables SCI access for over 12,000 contractors.

The first project review targeted improvement in the flow of data for the Army Contractor Automated Verification System (ACAVS) Company Access and the second project review focused on improving the efficiency of the Contract Personnel Access Process. ACAVS tracks the contractor company clearance status and the contract personnel clearance status related to current contracts. The database is also used to track Sensitive Compartmented Information Facilities at contractor facility sites. Because of the CSE team's vital role, it requires an efficient operation to keep pace with growing requirements.

Both projects are currently in the Improve Phase of the LSS process and have identified some unique goals and quick wins toward improving the overall efficiency of the SCI contracting operation. The goals established thus far are to reduce the errors on the Statement of Work (DD Form 254) by 50%, improve quality and accuracy of the data submitted into ACAVS by 60%, reduce ACAVS work flow queuing by 40% and improve communications between CSE and the customer.

Lastly, some quick wins will be to post frequently asked questions to ACAVS and incorporate updates in training, have Prime contractor enter Sub-contractor DD Form 254s electronically and transfer responsibility for welcome packets to the CSE Training Team for easier transition to contract companies.



Security Incidents can be contagious; don't get bitten by the bug!

Many people come in contact with classified information daily, either through physical handling or via information systems. It is essential to maintain a thorough knowledge of how to identify and properly handle classified information to avoid a security incident. Lack of knowledge or bad practices promotes a contagious bug called a "Security Violation or Infraction," which, if left unattended, can cause significant damage to the command's security posture and irreparable damage to National Security. Don't get bitten by the bug!

Report all SCI related security incidents to include those involving information systems to an SCI security official (Security Manager, SSO, SIO, SSR, IAM etc.) immediately upon discovery. This immediate action will ensure the incident is reviewed and acted upon by the appropriate personnel to prevent further damage to security. Most security incidents occur due to reasons such as: lack of attention to detail, rushing to meet deadlines, improper marking and handling, improper transmission, and just plain human error.

Security incidents can have a major impact on operations, especially when information systems are affected. Remember to log off or lock classified information systems when left unattended and never share passwords.

Simply put, it is imperative that all personnel handling classified information in any way be familiar with the regulatory requirements and local procedures in case of a security incident. The following are a few examples of incidents that could lead to security violations or infractions:

- Keeping classified material in a desk or unauthorized container, cabinet or area
- Reproducing or transmitting classified material without proper authorization
- Failure to mark classified documents properly
- Carrying safe combinations or computer passwords on one's person
- Discussing classified information outside accredited SCI Facilities such as lobbies, cafeterias, corridors or any other public areas where discussion might be overheard
- Discussing classified information over the telephone, other than a telephone approved for classified discussion
- Removing classified material from the work area in order to work on it at home
- A courier stopping at a public establishment to conduct personal business

Boost your knowledge today! For information on classification and control markings, see DoD 5105.21-M-1 or visit INTELINK on JWICS at (HTTP://capco.dssc.ic.gov) or SIPRNET at (HTTP://capco.dssc.sgov.gov).

SETA: Security Education Training and Awareness

New Website Announcement

SETA is pleased to announce the release of our new website http://www.dami.army.pentagon.mil/site/seta/default.aspx. Our new site contains key SETA program elements; the latest on the SPēD certification, training opportunities; security events; and a security toolbox. The toolbox contains briefing resources, customizable security guide, policy and guidance library, and videos. It is our goal to enhance the security posture of the U.S. Army by promoting and communicating security awareness across broad security disciplines to all designated security personnel. Additionally, our new site will provide support and information to answer security professionals most common questions regarding security education, training, and awareness.

This newsletter and previous editions are available on the new site. To help you stay connected to the latest information from SETA, we have added an RSS (Really Simple Syndication) news feed. The SETA news feed contains frequently updated content that can be automatically delivered to user's computer. Users can elect to subscribe and have content automatically delivered via Microsoft Internet Explorer or Outlook. Make sure you use Internet Explorer 7 or higher. When you use Windows Internet Explorer 7 and Office Outlook 2007, you can add RSS Feeds from either program as well as view the feeds in either program. To subscribe:

1. Access the SETA website by entering the URL http://www.dami.army.pentagon.mil/site/seta/default.aspx
2. Click on the " SUBCRIBE TO RSS FEED" icon on the bottom right of the homepage
3. Click on "Subscribe to this RSS feed" on the SETA News Page
4. On the RSS Feed pop up box, select "Subscribe"
5. Click the Favorites star icon ☆ and select " Feeds" to view the SETA News Feed

New SETA mailbox

We have established a new SETA mailbox in conjunction with the new site. Use this mailbox SETA@mi.army.mil to contact us with comments, questions and feedback.

Want your security event posted to the site?

Now that we have a website, your event can be listed under our "Army events" page. Send your request to SETA@mi.army.mil and include the following: title of event, date, place, and target audience. Ensure we have at least three weeks notice.

2010 Worldwide Security Conference

The 2010 Worldwide Security Conference will be held 3-6 August 2010 in Rosedale, Illinois (suburb of Chicago). The theme is "Staying Connected For Security Excellence". Personnel from the Defense Security Service, Center for Development of Security Excellence (CDSE), formerly Security Education, Training and Awareness, will serve as the conference staff. The venue location places limits on attendees; therefore, HQDA, G-2 is requesting projections from Army command points of contact to fulfill allocations. Allocations will be managed by the HQDA G-2.

Additional conference information:

✦ The conference is intended for middle to senior level professionals (military, civilian, and contractors who provide onsite security support for DoD components and activities).

✦ Registrants must have a .mil email address.

✦ DSS registration will be done in phases: pre-conference, pre-registration, and final agenda. Registration will close 30 days before.

✦ Attendees will pre-register and receive an email notifying them registration is pending approval by their organization representative within 48 business hours. Once approved, they will receive an email with the conference code to register with the hotel. Only approved conference attendees will be able to register at the hotel.

✦ Speakers will also register on the website; however, they are not included in the allocation distribution.

Registrants can register through July 2, 2010. A waiting list will be utilized as deemed necessary.

This conference will not offer training, workshops or external exhibit booths. Army breakout sessions will be provided several times during the conference.

Ms. Luisa Garza
SETA Program Manager

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

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