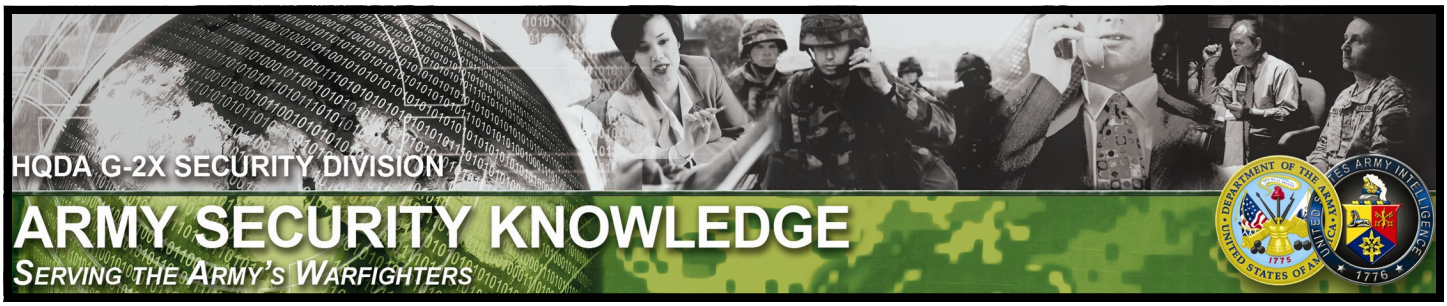


Senior Security Advisor Announcement

I hope everyone had a wonderful holiday season and my best wishes for a prosperous new year. This past year was filled with many trials and tribulations within the Army community. Unfortunately, tragic events have provided us with the opporunity to relook many of our security and Force Protection processes and procedures. Events such as the Fort Hood shooting and unauthorized Wikileaks releases have heightened our awareness and sensitivity regarding the Insider Threat.

I encourage all of you to be aware of the ALARACTs that have been issued related to Wikileaks to date. I also draw your attention to the recent G-2 Sends reference Wikileaks dated 3 December 2010. Please be diligent in reviewing your security programs and processes accordingly. Our security programs, training and education are the first line of defense in ensuring a strong security posture across the Army.

Patricia P. Stokes
Senior Security Advisor, DISL

Message from the Security Division Chief

The HQDA, ODCS, G-2 has established a Staff Assistance Visits (SAVs) program that will commence around Jan 11. The Army, G-2 SAV is an instructional and educational session that will afford the visited Commands an opportunity to discuss Army G-2 security policy, funding, resource, training and program management related efforts.

The G-2 SAV will also provide Army staffs an opportunity to identify and resolve Army security issues; provide a basis to gauge the security posture of Army; facilitate trend analysis; identify exceptional security practices; and assist ACOMs/ASCCs/DRUs in the effective management of security programs under their cognizance.

Army, G-2 staff will review and analyze SAV results, suggestions, comments and feedback for lessons learned and information that may prove beneficial not only to the visited Command, but to other Army Commands. Such information will be consolidated and shared with other Army agencies via the Army, G-2, SETA website (http://www.dami.army.pentagon.mil/site/SETA/).

The ODCS, G-2 point of contact is Mr. Karl Borden, (703) 695-3060, DSN 225-3060, karl.borden@us.army.mil.

Karl Borden
Chief, Security Division

Arrivals

Mr. Dave Stiffler
Deputy Chief, ARTPC Branch

Mr. Chuck Jordan
Program Protection Architect, ARTPC

Ms. Sherry Dixon
Management Analyst

Mr. Alan Tomson
Program Manager, AIES

Ms. Shannon Wright
Security Specialist, SSO

Jan 2011
Inside This Issue

ARTPC POC

Mr. Dave Stiffler
Acting Chief, ARTPC
Ph: (703) 601-1595
Dave.Stiffler@us.army.mil

The Role of System Decomposition in the CPI Identification Process

By: Dave Stiffler

The goal of the Program Protection process is to first identify Critical Program Information (CPI) and then to identify threats to the CPI, the vulnerabilities of the CPI, and ultimately to select and implement countermeasures that will minimize the risk of compromise of the CPI.

A challenge in identifying CPI is determining which parts, pieces, or subsystems of the program, system, or technology should be assessed. The problem of "what" to assess in a program can seem daunting when assessing a highly complex program like the Army Field Artillery Tactical Data System (AFATDS), whose "basic" block diagram of system components and functionalities can fill the walls of a conference room. However, even in a much simpler program like the Commander's Digital Assistant (CDA) the Protection Integrated Product Team (IPT) still must determine which parts of the program warrant being assessed for CPI.

To enable the IPT to determine which items should or should not be assessed, a process known as "decomposition" is used. Decomposition is defined as: separating into constituent parts or elements or into simpler compounds; the process by which a complex problem or system is broken down into parts that are easier to conceive, understand, program, and maintain. Prior to meeting with the Protection IPT, the ARTPC members facilitating the CPI assessment develop a "decomposition strategy" by breaking the program down into its various sub-systems and sub-components in a logical method. This is not the final decomposition but will be used by the IPT as a starting point. During the IPT's discussion, items may be added or deleted from the decomposition plan as appropriate. How deep the system is examined will vary for each program, however as a general rule, each program should be reviewed, at a minimum, to the sub-system level at a minimum.

One factor driving how far the IPT decomposes the system is the concern of "masking" CPI. For instance, stopping the review of a Counter IED system at the sub-system level could lead to that sub-system being designated as CPI. In this case, if the IPT had drilled down to the next level it would have discovered the classified CPI was actually tied to a specific Circuit Card Assembly within that sub-system. As a result, it causes the over protection of the entire sub-system instead of focusing protection on the Circuit Card Assembly alone. This could drive increased costs for the Program Manager (PM) when designing countermeasures (Anti-Tamper or Systems Security Engineering), and could greatly increase the number of components that have to be evaluated for supply chain risk. The end result is additional time, money and resources being spent by the PM, as well as potential schedule impacts – not a good news story for the PM or the Army.

As the IPT looks at the program, there are a number of documents and sources that help to focus their attention and aid in culling out those items that should be assessed for CPI from those that obviously should not.

Some of those sources are:

- ***The Work Breakdown Structure (WBS).*** The WBS is a great way to see the entire structure of the program in one source document. Their size can range from a hundred lines to several thousand lines depending on the program. This document will allow the IPT to see each sub-system and a great amount of detail below that.

- ***Program Briefings.*** These are usually good for high-level block diagrams of a systems parts, pieces, and functionalities that give an overview of the system. Depending on the brief, it may have varying levels of technical details which could be useful in developing the decomposition plan.

- ***ICDs, SCGs, DDLs, and Other Program Documentation.*** These documents contain lists of Key Performance Parameters, items that are classified or sensitive, and items within the program we do not want released to foreign countries. These are all examples of items that the IPT might want to evaluate to determine if they are also CPI. Knowing this information will allow the IPT to focus on specific areas of the program that provide or enable specific functions. Areas or items in the system also include those that contribute to Lethality, Survivability, C3 or SA functions. Knowing which parts within the system contribute to these functions enables the decomposition to focus on these important aspects of the program.

As you can see, a good decomposition plan can help the IPT focus on those items that should be evaluated for CPI and should CPI be found, make it more likely that countermeasures and protection is focused on the right system components.

Farewell and Best Wishes

Mr. Dick Henson, Chief of the Army Research and Technology Protection Center (ARTPC), will retire from civil service after 44 years of distinguished service on 31 Jan 2011. For the last ten years, Mr. Henson has been a trusted advisor to senior Army leaders and an invaluable member of the Army G-2. Among his many accomplishments, Mr. Henson was instrumental in the establishment of the ARTPC concept and has effectively managed the ARTPC since its inception from May 2001 to Jan 2011. Under Mr. Henson's leadership the ARTPC has become the premier RTP organization within DoD, developing processes and tools to identify and protect Army Critical Program Information which have become the model for the rest of DoD.

We would like to take this opportunity to thank Mr. Henson for his leadership and selfless dedication to the Army G-2 and wish him and his family the best of luck.

Mr. Dave Stiffler will serve as the Acting Chief of ARTPC as of Monday, 29 Nov 2010, and can be contacted at (703) 601-1595.

COMSEC / TEMPEST / ISSM POC

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

Mr. Harry Byrd
COMSEC/TEMPEST/ISSM
Ph: (703) 607-1874
Harry.Byrd@us.army.mil

Technical Security Team

By: Harry Byrd

A significant event within the Technical Security Team was making contact with the U.S. Army Africa Command, located in Vicenza, Italy. U.S. Army Africa is a relatively new command that falls under AFRICOM and they are working hard to get their programs up and running. U.S. Army Africa recently received their certification to conduct COMSEC monitoring operations for organizations within the Command, and are also helping them work through numerous TEMPEST related issues. Through working with NSA, 1st Information Operations Command (1st IO CMD), and the U.S. Army Africa staff, we were able to broker an agreement that will allow the 1st IO CMD to conduct COMSEC monitoring operations for US Army Africa regardless of their geographic location, including units conducting tactical operations. The 1st IO CMDs ability to conduct COMSEC monitoring operations in tactical environments provides Army Commanders with an invaluable assessment tool to help ensure the integrity and security of on-going operations.

Policy Update

AR 380-53, COMSEC Monitoring: The draft of this regulation was submitted to the Office of The Judge Adjutant General (TJAG) and the Army Office of General Counsel (OGC) for review on 12 March 2010. We are currently working with these offices to resolve comments and move this forward for signature and issuance.

AR 380-40, Policy for Safeguarding and Controlling COMSEC Material: This regulation was resubmitted for formal staffing as of 18 May 2010. We have collected and adjudicated comments from the various Army Commands and are currently working to resolve comments from Army CIO/G6 prior to submitting the draft regulation to TJAG and OGC for review.

Quarterly VTCs

The Technical Security Team hosts video-teleconferences (VTCs)/telephone conferences (TCONs) on a quarterly basis to ensure that information is relayed to the Soldier in the field and to solicit input from Commands. We have also used this media as a mechanism to listen, teach and train, and serves as a tool for Commands to hear the HQDA, ODCS, G-2 as a unified voice. We have been fortunate to have strong attendance and participation and encourage your continued support. These VTCs and TCONs conferences serve as a conduit to ensure the needs of the Soldier are heard and in turn incorporated into Army policy. Please contact us to take part in our next VTC.

Conferences

The Technical Security Team will be participating in the Global Information Partnership Conference (GIPC) to be held May 2011 at Fort Huachuca, AZ. While at the conference, we will be conducting extensive workshops on COMSEC, TEMPEST and COMSEC Monitoring. These workshops will provide Commands the definitive knowledge of what these subject areas consist of and how they can develop/improve their Command's programs. Information provided will include procedures for Commands to request training and to formally request services to be provided.

In closing, the Technical Security Team remains committed to addressing the needs of the Army and to ensure the Soldier's mission is successful. Therefore, we welcome comments concerning this article. If you have any questions, comments or suggestions or would like to have any particular topics addressed during our VTCs or in future newsletters, please feel free to contact us. 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

Covering the Ground Rules And Winning the World Series

By: Dave Grob

Umpires and managers have been gathering around home plate to discuss ground rules for the World Series since 1903. Ground rules are just that...they address how the game is to be played at a particular location. At Chicago's Wrigley Field, a ball hit into the outfield that ends up lodged in ivy is a ground rule double. A ball hit through the large green, majestic, manually operated scoreboard in Boston's Fenway Park left field wall is a ground rule two base hit. Cincinnati's Crosley Field once included this language painted on the outfield wall in the place where concrete met a field fence*: "Batted ball hitting concrete wall on fly to right of white line - home run."*

In any given year our Army:
-Entertains approximately 8,000 requests for visit authorization (RVAs)
-Hosts hundreds of extended visitors
-Trains over 10,000 international students

In other words, our Army hosts the World Series each year. The message to the Army team from management is simple…play to win every day, play by the ground rules, and good sportsmanship towards the visiting team is a must.

In keeping with our baseball analogy, this means the foreign disclosure/security ground rules in the Army's ball parks must be clearly explained and understood by both the visiting and home teams. When this doesn't happen or when it's done poorly; managers become irate, ejections are called, and folks turn to the foreign disclosure/security umpire for guidance and rulings. The foreign disclosure/security umpire can mitigate much of this if the ground rules they establish and communicate address some common fundamentals. Think of these fundamentals as the four bases (or basics) that must be touched in order to claim a home run:

First Base: Requesting and obtaining military information. This is where it all begins and includes the basic ground rules: how requests for information (RFIs) are processed to the formal rule set; who to ask for information, who can ask for information, and what information can be asked for. This basic should also address any provisions for searching or obtaining military information via electronic means such as through the internet or local networks.

Second Base: Sharing of military information. Ensure both teams understand their security responsibilities for the information they obtain. This must include the provision that the information may not be shared with anyone else without obtaining the proponents permission, nor may it be shared for any purpose other than what has been previously agreed upon.

Third Base: Protection and safeguarding of military information. All players must realize that ***third base*** tells them there are three basic components related to protecting and safeguarding military information. Those components are access control, markings, and medium. Access control refers to things like badges or other forms of identification/personal verification that are intended to protect and safeguard information from those who otherwise, should not have access to it. Markings on documents serve several purposes. They alert holders to the presence of classified or sensitive information, identify exact information or portions that require special protection, and provide guidance and or restrictions on distribution. Medium refers to the active and conscious decision to convey or withhold information through either oral, visual, or documentary means.

Home Plate: Storage and transmission of military information. As in baseball, if you miss home plate, your efforts up to that point will have all been for not. Both teams must clearly understand what are and are not acceptable practices for the storage and transmission of military information. Players must be made sensitive to the fact that home plate represents both a starting and ending point. Your ground rules should be explained along a similar continuum, covering both relevant polices/rules and the physical actions to take or avoid along this journey from home to home. Don't just mandate that documents in transit must have

double barrier protection, and then call it a day. Does folding a piece of paper constitute one barrier and placing it your pocket constitute the second? Make sure everyone knows what the ground rules are and how they are to be applied and executed.

As you develop or review your existing ground rules (briefings, policies/procedures or educational products), make sure they cover the four bases, or basics, mentioned above. Ground rules that are well established up front, clearly communicated, and understood by all can make for an enjoyable Fall Classic. When they aren't, they can lead to a less than classic fall by our disclosure and security personnel.

INFOSEC POCs

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

Controlled Unclassified Information

By: Bert Haggett

On November 4, the President signed Executive Order (E.O.) 13556, Controlled Unclassified Information (CUI). This order "… establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under E.O. 13526 of December 29, 2009, or the Atomic Energy Act, as amended." This E.O. (Section 3.(a)) requires that each agency head shall, within 180 days, review all categories, subcategories and markings used by the agency to designate unclassified information for safeguarding or dissemination controls, and submit to the Executive Agent (NARA) a catalogue of proposed categories and subcategories of CUI. We will continue to work with the Office of the Under Secretary of Defense for Intelligence to develop a process as to how the information will be protected and marked.

Classified Information - Executive Order 13526

By: Bert Haggett

On December 29th 2009, the President issued a new Executive Order (E.O.) dealing with classified information. E.O. 13526 replaces E.O. 12958.

As a reminder, there are a number of notable changes in the order. The establishment of a National Declassification Center is perhaps the most notable change. 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 each agency will play is yet undecided. The Army will have a continuing need to manage it's own program, in addition to involvement in the National Declassification Center.

The new E.O. also requires that all Original Classification Authorities (OCA) 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 that they conform to the tenants of the new order (DoD is currently staffing new implementing guidance). The basic changes in the order itself will be reflected in the revision of AR 380-5.

Mandatory Declassification Review

By: Bert Haggett

DoD has issued a draft manual concerning Mandatory Declassification Review (MDR), which is now in the public comment phase of publication. Formal publication is expected in the early Fall. The draft manual is separate from DoD 5200.1R and addresses only MDR. The draft manual closely aligns the MDR process with current Freedom of Information Act process (requiring a review under the terms of the FOIA prior to any release). When DoD issues the manual, our current plan is to issue an Army version as a separate Army Manual.

Industrial POCs

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

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

GOCO's Not Your "Typical" Government Facility!

By: Pamela Spilman

Let us unlock a little bit of the mystery about something called GOCO. GOCO means Government Owned/Contractor Operated facility and is a partnership between the government and contractor. This partnership gives the government and contractor the ability to perform duties for which it is uniquely suited: the government establishes mission areas and the private sector implements the missions using best business practices.

During the Manhattan Project (codename for a project conducted during World War II to develop the first atomic bomb), the federal government asked the University of California to operate what is now Los Alamos National Laboratory. A GOCO model for managing research and development labs was born; the government owned the laboratory site, the buildings and the equipment; the University provided the employees and managers.

In the United States, GOCO arrangements help to manage 19 laboratories, nearly a dozen manufacturing and production plants and numerous repositories.

Some of the other government partnerships include:

GOGO - Government-Owned/ Government-Operated. A facility owned and operated by the government for all regulated activity. (Federal)

GOCO - Government-Owned/ Contractor-Operated. A facility owned by a Federal agency, but operated in whole or part by private contractor(s). (Federal)

GOPO - Government-Owned/ Privately-Operated. The government leases all or part of its facility to a private operator for its operation and profit. (Federal)

COCO - Contractor-Owned/ Contractor-Operated facility that provides goods and/or services to a Federal agency under contract. (Private)

COCO(E) - Same as COCO. However, the contractor may be furnished government equipment to manufacture a product or provide a service. (Private)

POGO - Privately-owned/ government-operated. The government leases buildings or space for its operations. (Federal)

FUDS - Formerly Used Defense Sites. A Federal agency may or may not presently own this site. However, it is responsible for hazardous waste cleanup because of previous operations. (Federal)

Briefly (and greatly simplified), here is how it works: The GOCO allows proven private sector processes to operate without bureaucratic restrictions. Scientists are, by in large, insulated from political pressures while performing for a GOCO contractor. As a result, they have the independence to speak out as honest brokers, acting truly in the national interest.

Some important things to remember about GOCO: The Federal Government already "owns" more than 20 corporations, including the Tennessee Valley Authority, Saint Lawrence Seaway Development Corporation, Federal Prison Industries Corporation and Federal National Mortgage Corporation. These corporations are federally chartered entities created to serve a public function of a predominantly business nature. The mission and situation governs whether or not a GOCO is the appropriate partnership.

If the contractor is awarded a classified contract, even if they are working in a government owned facility, the contractor is still responsible for adhering to security requirements. If the awarding government agency does not carve the Defense Security Service (DSS) out of the security inspection and oversight responsibilities, DSS is the cognizant security authority.

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

Financial Disclosure Form (SF 714) Fact Sheet

By: Ashley Kirby

What is it? A federal form approved by the Office of Management and Budget, the SF 714 supports the implementation of the Financial Disclosure requirements outlined in Executive Order (E.O.) 12968, Access to Classified Information, as well as DoD implementation mandates and is made available via OPM's e-QIP portal. The SF 714 is a financial disclosure form that requests financial information concerning the designated employee, their spouse and any dependent children.

Why is it important? The espionage cases of Aldrich Ames and Robert Hansen provide good examples of the importance of examining the financial status of cleared personnel. The SF 714 was designed to detect unexplained affluence, and is a tool that assists in espionage prevention, deterrence and detection.

Who is required to file? As mandated in E.O. 12968, all employees with regular access to especially sensitive classified information are required to file the SF 714. Especially sensitive information includes information about: the identity of covert agents, intelligence collection and processing systems, certain cryptographic systems and equipment, certain special access programs, and some nuclear weapons design information. Within the Department of Defense, full implementation is required by December 31, 2012.

What records are required in order to answer the Financial Disclosure Form questions? Records required to complete the form include: IRS 1040 form; bank and credit union year-end statements; investment or IRA year-end statements; real estate records; capital improvement cost records; records relating to leased or rented real estate, vehicles, boats or airplanes; other assets; mortgages, loans and other liabilities; credit cards; bankruptcy; safe deposit box information.

How is the Army planning to implement the SF 714 requirement? A phased implementation is planned to begin in 2nd Quarter FY 11 with a small population of personnel in the National Capital Region. Future phases will expand implementation throughout the Army. The process will begin with the Command Security Manager designating personnel who must file the SF 714. Selected individuals will then be invited and initiated to the form in e-QIP. Once completed, the form will be processed to the Automated Continuous Evaluation System (ACES). The ACES will use algorithms to process the form to commercial and government databases; the Personnel Security Research Center (PERSEREC) will analyze the results and provide them and their analysis to the Army Central Clearance Facility (CCF). The CCF will evaluate the results using the National Adjudicative Guidelines. Support and training will be provided to personnel selected to file the SF 714. Instructor-led and online training on the SF 714 will be available to filers as part of the implementation process. The Special Programs and Activities (SPA) community will implement their respective financial disclosure requirements within SPA channels.

Who may I contact with questions/comments/concerns about the SF 714? Ms. Andrea Upperman, the Branch Chief of the G-2 Personnel Security. Please feel free to reach her at (703) 695-3053 or via email at Andrea.Upperman@us.army.mil

SCI POLICY

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

What to Expect Upon the DNI's Release of the IC Technical Specifications for the Construction and Management of SCIFs

By: Cliff McCoy

The Director of National Intelligence is close to releasing the Intelligence Community (IC) Technical Specifications for the Construction and Management of Sensitive Compartmented Information Facility (SCIFs). This is the fourth and final policy document pertains to construction security and will replace DCID 6/9. Earlier this year, the DNI released ICD 705 and ICS 705-1/705-2, all which established the physical and technical security standards that applies to all SCIFs within the IC.

Upon final release of the IC Tech Specs, Defense Intelligence Agency (DIA) along with the Army G-2 will provide implementation guidance to the Sensitive Compartmented Information (SCI) community which will identify the specific applications for following the new construction security policies. ICS 705-1, which was signed in September this year, identified a 180 day window for IC elements to implement the standards. Those timeline give DIA and Army until March 2011 to finalize the implementation plan, but don't be alarmed because we have been working closely together over the past months towards developing a solid plan. The implementation plan will direct and clarify construction security standards for the following: active construction or renovation projects, existing projects beyond 60% design review and construction or renovation projects at less than 60% design review.

The implementation plan will further address concept approvals, which are required for the establishment of new SCIFs, limitations on waivers, mitigations/standards and SCIF inspections and oversight responsibilities. Over the next few months, the SCI Policy Office will be reaching out via VTC and other electronic means to educate you on all new construction security policy changes. In the interim, if you have developed concerns or questions based on an ongoing SCIF project, please provide your questions via e-mail so that we may have the chance to address each appropriately. DIA SCIF Support Branch is the accrediting authority for Army SCIFs and will continuing working with commands to ensure the highest integrity for every SCIF construction project they approve. Stay Tuned!

T-SCIF Reminder

By: Cliff McCoy

Command SCI Program Managers must ensure that Tactical SCIFs (T-SCIF) granted an Approval To Operate (ATO) comply with DIA Implementation Guidance outlined in message, dated 171736Z Oct 07. The ATO remains at the Command Senior Intelligence Officer Level and copies of the approval shall continue to be forwarded to the policy office via secure means. Please consult the SCI Policy Office if you have any concerns or questions about the process.

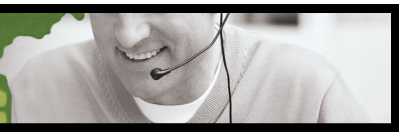
Be Vigilant At All Times!

Often we let our guard down during the celebration of the holidays but our adversaries are watching and waiting for seams (gaps) in security at all times. Use the following tips from our security professionals at the U.S. Army Contracting Command year-round:

* Be alert for unusual situations
* Be mindful of the insider threat
* Be aware that the adversary is always watching
* Be prepared to respond to crisis situations

If you notice something suspicious, report it to your security office or appropriate law enforcement agency.

SETA: Security Education Training and Awareness



SETA

It is the SETA 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. The Army G-2 is emphasizing the SETA website (http://www.dami.army.pentagon.mil/site/seta/default.aspx) as a communication tool to stay current on all SETA/SPeD news and future effort. The SETA website was created with the intentions of providing security professionals access to SETA information from the comforts of their own home. Website contains security program elements, training opportunities, security events, and a security toolbox. The SETA website also provides the latest updates on SPeD activities and newsletters.

Request to the Field

The Army G-2 makes every attempt to keep our SETA website updated and accurate, however we are requesting that the field notify us (SETA@mi.army.mil) if they have any information that they would like to post on the site, such as:

* Upcoming Events (title of event, date, place, target audience - ensure we have at least three weeks notice)
* Useful Information Pertaining to Security Programs
* Training / Courses for Security Professionals

**NOTE: The SETA website is on a public domain, therefore all website suggestions will be reviewed.

Looking to the Future

In keeping our promise, the SETA website will be undergoing several updates and changes in order to provide you with the latest information. We are working diligently to create both a public website accessible to all and a mirrored, secured website where we can post classified information (i.e. regulations and manuals). Stay tuned!

2011 Worldwide Security Conference

The 2010 Worldwide Security Conference will be held the end of July/beginning of August. Specific dates and hotel locations TBD. Allocations will be similar to last years conference and will be managed by the HQDA G-2. Please check the SETA website for updates!

Want SETA Updates?

Subscribe to the SETA RSS Feed! Instructions on subscribing to the RSS feed can be found on the SETA website and our previous newsletter.

SETA VTC

A SETA VTC (UNCLASS) will be held on Tuesday, 1 February 2011, from 1330 to 1500. If your Command would like to participate, please send your Command Site ID to SETA@mi.army.mil. Agenda will be forthcoming.

RETRACTION:

The July 2010 newsletter mentioned the re-vitalization of the Thomas Dillon Award and the Security Center of Excellence Award. The awards have gone through several changes and will be consolidated into a single G-2 Security Award. This award will recognize a security professional who personifies the highest standards of leadership and security excellence who has made unique and important contributions to the Army. More information soon to follow.

QUESTIONS / COMMENTS / CONCERNS
— EMAIL US AT SETA@MI.ARMY.MIL —

SPēD (Security Professional Education Development)
There continues to be a significant level of activity with the DoD SPēD certification program and I wanted to make sure you are aware of present and future activities and goals. Mr. Reginald Lockhart has recently joined G-2 and will be working alongside me to develop and implement the Army SPeD program.

Army Beta-Test Status
The test period began 1 September and will end on 30 December 2010. The Defense Security Service (DSS) mobile testing team is coordinating with select sites to test Army personnel. We have tested over 239 candidates at Fort Hood, Aberdeen Proving Grounds and Redstone Arsenal.

Future training opportunities are ongoing in the National Capital Region, Fort Leavenworth, Fort Bragg, and Fort Sam Houston, Fort Campbell, Fort Knox and the Pentagon. We continue to work directly with DSS and interested sites to coordinate mobile testing where possible. Please visit the SETA website for other joint testing events.

SPēD - Future Events
DSS and Army will provide on-site SPēD information and testing:

- DSS SPeD Pacific Campaign: Hawaii - Feb 2011
- Germany, Garnish May 9-11 2011 European Security Conference
- DoD World Security Conference last week of July or first week of August, 2011.

Implementation
The draft implementation manual, DoD 3305.13, is in the final stages of coordination. Once the draft is approved, Army will coordinate with Commands to identify positions, map certifications and develop workforce management within SPēD.

Additionally, SPēD is now included in the ACTEDS Training catalog http://cpol.army.mil/library/train/catalog/ch03cp35.html. Take advantage of the no-cost online training available for the first certification, Security Fundamental Professional Certification, offered exclusively through DSS.

Thank you for all the support and we truly look forward to the "roll-out" of SPēD in the Army.

More information on SPēD is available at the Army SETA website http://www.dami.army.pentagon.mil/site/seta/ and DSS SPēD website http://dssa.dss.mil/seta/sped/sped.html.

Army SPeD Program POCs

Ms. Luisa Garza
luisa.garza1@us.army.mil
703-944-1796

Mr. Reginald Lockhart,
Reginald.lockhart1@us.army.mil
703-824-4130

Security Starts with YOU !!