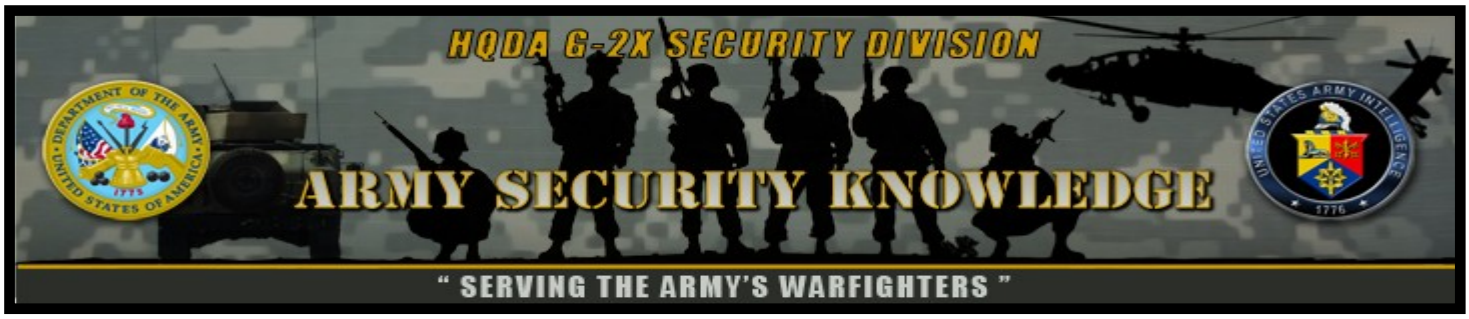


Director's Message

As we reflect on the unfortunate tragedy of Ft. Hood, we are vividly reminded of the importance of our national security, the security of our installations, and our personal reporting responsibilities. I remember a time when Subversion and Espionage Directed Against the Army (SAEDA) reporting and training was a pivotal part of our Army culture. It was, and still is, not only an annual training requirement for all Army military and civilian personnel, but also revered as one of the most critical daily responsibilities of Army employees.

I ask that we all take pause and reinstitute, revitalize, and re-energize our Command reporting awareness programs and assist our Commanders in educating the workforce with regard to the importance of their personal reporting responsibilities. As security professionals, we must emphasize the recently published guidance from the Chief that identified indicators of potential terrorist or insider threats. Personnel should be reminded that oftentimes, they are the first line of defense. Pay particularly close attention to the upcoming rewrite of AR 380-12 which has been renamed from SAEDA to Counterintelligence Awareness and Reporting. This regulation will be re-published shortly.

On a lighter note, I am pleased to welcome to our Army G-2 security senior leadership team, Mr. Scott Schultz. Scott reported in late December assuming the role as our Foreign Disclosure and Information Security Branch Chief. He comes to us with over 20 years of senior leadership experience to include a 30-year career as a former Marine reserve officer. I am also happy to announce the reassignment of Mr. Paul Watkin as our Special Access Program Chief. Both of these gentlemen possess the requisite skills that will contribute to the continued establishment of a strong security leadership team. Please feel free to reach out and contact them with your issues and/or concerns in their functional areas of responsibility.

The G-2 staff continues to work several critical issues. We are in full support of the Chief of Staff of the Army reviewing our personnel screening policies. We are looking closely at the enhanced utility of our Army Investigative Enterprise Solution as we continue to deploy this across the Army.

This newsletter has received rave reviews and we strive to continue our communication campaign with the field. Please provide us feedback on this product and let us know if we are missing something in our coverage and communications. I wish you all a happy, healthy and prosperous new year in support of our soldiers and the Army mission.

Sincerely,

Patricia P. Stokes

New Appointments

Mr. Dick Henson
Acting Chief, G-2 Security Division

Mr. Paul Watkin
Chief, Special Access Programs

Arrivals

Mr. Scott Schultz
Chief, Foreign Disclosure & INFOSEC

Congratulations:

The G-2 family congratulates Ms. Patricia Stokes on her new appointment as a Defense Intelligence Senior Leader. Ms. Stokes will retain her responsibilities leading the Army Security Program and assume the title of Senior Security Advisor. The G-2 Security Division Chief position will be backfilled and recruited in the next few months.

January 2010
Inside This Issue

ARTPC POC

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

Is YOUR CPI Optimally Protected?

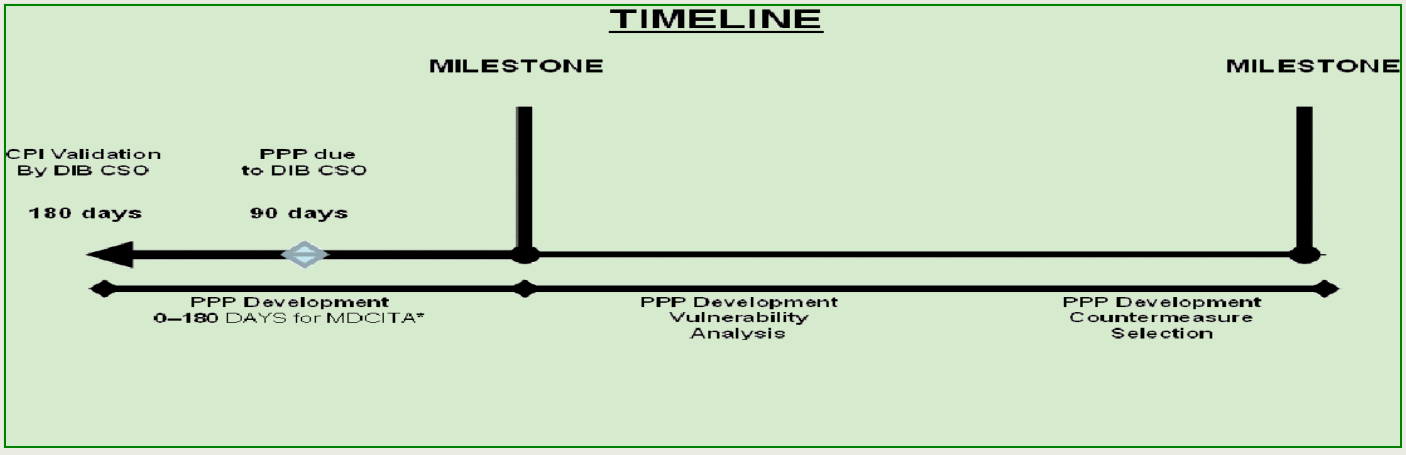
According to a policy memorandum signed by the Acting Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)) on 11 February 2009, the Defense Industrial Base Cyber Security Office (DIB CSO) within the Office of the ASA(ALT) is responsible for validating Critical Program Information (CPI) resident in Acquisition Category programs, not the Program Managers (PM). PMs must submit a list of their CPI to the DIB CSO for validation no less than 180 days prior to Milestone B Review and the associated Program Protection Plan (PPP) 90 day prior to that review.

Permit me to pose one of the many possible real acquisition development scenarios. When a PM is approaching Milestone B Review and the selection of the prime contractor will occur immediately prior to or after the review. The PM has not leveraged or inherited CPI from any research project. Since the development of the technology will take place after Milestone B, it may be premature to conduct a CPI assessment of the program until the critical design review (CDR) has been completed. Therefore, at Milestone B Review, the PM has not identified any CPI resident within the program.

Milestone C Review now becomes the next required event for the validation of CPI and submission of a PPP. Let's assume CDR occurs 24 months prior to Milestone C and the PM's Integrated Product Team (IPT) identifies CPI. According to the policy memorandum, the requirement for the PM to submit the CPI list and PPP to the DIB CSO is six months and three months prior to the next milestone. In this scenario, the time period between CPI identification and validation is 18 months, which represents a potential gap in optimum protection of the CPI through the application of countermeasures. Additionally, the three-month period between validation of the CPI and submission of the PPP is insufficient to address specific elements of the plan, such as the Counterintelligence Threat Assessment, vulnerability analysis and countermeasures which are conducted in sequence.

Question: How does the PM optimally protect CPI and satisfy this policy requirement?

Answer: Immediately after the IPT identifies CPI, they will identify countermeasures, that can be implemented after the PM' s approval. The PM will forward the request for validation of the CPI by the DIB CSO and not wait for the 180-day submission date prior to the next milestone review. During the validation period the PM would initiate a Protection IPT to institute and implement the countermeasures into the PPP. Contact the local G-2 Army Research and Technology Research Center, Technology Protection Engineer or the ARTPC HQ at **(703) 601-1930** to assist.



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

Communications Security/TEMPEST/ Information Security Systems Monitoring

Today's Army is changing at a pace in which policy can become virtually outdated by the time it is promulgated and published for the Soldier in the field. The main focus of the COMSEC/TEMPEST/ISSM Team is to ensure the Soldier's interests are heard and addressed in order to give the Soldiers policy they need to function effectively. Accordingly, the following issues are being worked diligently to ensure objectives are met in a timely manner.

Currently AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, is being staffed for final revision through appropriate Army staff elements. Afterwards, revisions deemed necessary will be incorporated and forwarded to the Army Legal Staff for approval prior to being published. During the staffing process two significant changes have been identified. The first changes the current threshold for entry into the Department of the Army Cryptographic Access Program (DACAP) from individuals with a Top Secret clearance to all individuals with a Secret or higher clearance. This will bring Army policy in line with current National policy. The second is the acceptance of formal LCMS training certificates issued by other Department of Defense Training Institutions. This revision will provide immediate benefits to the field by allowing COMSEC accounts to function without interruption to operations. Both changes will be reflected in the revised edition of AR 380-40.

AR 380-27, Control of Compromising Emanations (TEMPEST), has been approved by the Army Administrative Law Branch, and the Army Office of the General Counsel. Coordination with the Army Publishing Directorate is going well and AR 380-27 is expected to be released by 31 December 2009. Army TEMPEST policy was previously included in classified AR 381-14, Technical Counterintelligence (TCI). AR 380-27 will be unclassified For Official Use Only and now includes the Army Protected Distribution policy.

An updated draft of AR 380-53 is in Army-wide staffing. Once the regulation has been through the staffing process and the necessary changes have been made, the regulation will be forwarded to the Army Office of the General Counsel for final administrative law review prior to being published.

Another matter pertaining to AR 380-53 is the biennial request for Certification of Information Systems Security Monitoring, which was due no later than 15 July 2009. Commands that have received certification have been notified accordingly and the approval period is effective from 1 October 2009 until 30 September 2011.

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 the time and view this site if searching for recent changes concerning COMSEC related issues.

In closing, the COMSEC/TEMPEST/ISSM Team remains dedicated to the success of the Army and the Soldier's mission and welcome comments concerning this article. If you have any comments or suggestions, please feel free to contact Mr. Richard 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 POCs

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

Home Cooking by Dave Grob

Office pot-luck lunches are great. Many of the dishes and treats originate from trusted family recipes. Still others might be new creations or variations of those time honored delights. I think it's safe to assume that we would not consider putting an ingredient into the mix or recipe without knowing what it tasted like or how it affected the final product. While ground paprika and cinnamon are both spices and may look the same, only one of them probably belongs in grandma's pumpkin bread.

Much the same thing can be said for how we understand and account for the eight (8) categories of Classified Military Information (CMI). When writing, evaluating, and implementing Delegated Disclosure Authority Letters (DDLs), it is imperative that the FDO clearly understands the totality of the information/data set they are working with. The disclosure professional has to be able to account for all information and data by first aligning it to a category of CMI. Categories matter because NDP-1 and the disclosure authorities the Army exercises for each country are category and level of classification dependant.

The definitions for the various categories of CMI can be found in AR 380-10, pages 8-10. They are:

Category 1: Organization, Training, and Employment of Military Forces
Category 2: Military Munitions and Material
Category 3: Applied Research and Development Information and Material
Category 4: Production Information
Category 5: Combined Military Operations, Planning, and Readiness
Category 6: U.S. Order of Battle
Category 7: North American Air Defense Command
Category 8: Military Intelligence

The FDO is required to know more than just the names of these categories. Think about someone sorting mail with each letter having to be assigned to a particular box. If the letter can't be assigned to a specific box, then it's considered undeliverable. Foreign disclosure is no different. If you can't determine or assign something to a category of CMI, then how do you deliver an informed and judicious disclosure decision on it?

Consider this example. You are reviewing a briefing being presented to the Government of Upickistahn. Annex A of NDP-1 shows that the Army currently has these delegated disclosure authorities for Upickistahn and CMI originated by the Army.

Category 1: Secret
Category 2: Secret
Category 3: None
Category 4: None
Category 5: Secret
Category 6: Secret
Category 7: Confidential
Category 8: Confidential

The focus of the briefing is countering the Improvised Explosive Device (IED) threat. Each of the slides in the briefing is marked SECRET. Your boss says disclosure should not be a problem because all of this is only SECRET and is of an operational nature.

The first slide deals with tactics, techniques and procedures (TTPs) employed by U.S. Army forces to avoid IEDs and complex ambushes. **This is Category 1 information.**

The next slide covers the capabilities and operational characteristics of the electronic systems used to detect and counter the IED threat. **This is Category 2 information.**

The third slide depicts current readiness information and training assessments for both the US. Army and Upickistahni. This information will be used to drive future operational planning in theater. **This is Category 5 Information.**

The forth slide addresses current U.S. Army unit locations and strengths in theater. **This is Category 6 information.**

The final slide highlights TTPs employed by insurgents to provide early warning for and to trigger IED attacks and complex ambushes. **This is Category 8 information.**

Here we have five slides containing five different categories of CMI. They're all of an operational nature, but there is no one *"catch all"* category of CMI for operational issues or information. More importantly, one of the *"ingredients"* in this briefing (CAT 8), should not be included without obtaining additional disclosure authority. As it stands now, what we do have is a recipe for disaster. Sort of like paprika in pumpkin bread.

Take the time to master the categories of CMI. Force yourself to sort or assign all information or data in a DDL into one of the eight categories. Make sure the requisite authority is in place for the Army and your organization as it relates to the specific country, category and classification level. If you do all of these things all the time, daily disclosure issues won't end up leaving a bad taste in your mouth. Paprika in pumpkin bread? I think I'll pass.

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

Information Security Update

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.

On December 29th, President Obama issued Executive Order 13526, Classified National Security Information, replacing EO 12958. The EO contains a number of new requirements, and establishes a National Declassification Center within the National Archives staffed by those agencies which created the classified documents held by the National Archives. The Center is being established to centralize declassification efforts under one roof and will be managed by the National Archives. Specifics on staffing 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 within the Army in addition to involvement in the National Declassification Center.

Additionally, all Original Classification Authorities (OCA) will be required to receive training annually, while 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. Derivative classifiers will now be required to add their name to the document or email (this already exists for the most part if you consider that any email will have the senders name and that most memorandums and letters have a point of contact noted). The Army will be required to review all existing classification guides within two years to ensure they conform to the tenants of the new order.

The next step in the process will be the issuance of an implementing directive from the Information Security Oversight Office (ISOO). That directive may contain additional requirements. A draft of the directive is expected for comment in late January. We will keep you informed as the process continues.

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

DD Form 254's Leaving You Dazed?

If the DD Form 254 is leaving you dazed and delirious, follow the 4 D's to help you decipher and deduce the disorientation:

1. Determine – Determine the type of contract (classified or unclassified)

2. Develop – Develop the security requirements of the contract

3. Deliver - Deliver the DD Form 254 to key personnel for review

4. Distribute – Distribute the DD Form 254 to appropriate agencies

A DD Form 254 is defined as: A Department of Defense (DoD) Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to provide original classification guidance and security requirements on a classified contract.

The Security Agreement (DD Form 441), executed between the government (Defense Security Service) and all cleared facilities under the Executive Order 12829, National Industrial Security Program (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" in classified contracts and solicitations, to include the Statement of Work (SOW) or related requirements document. The DD Form 254 provides the specific security requirements for each classified contract.

At a minimum, the Federal Acquisition Regulation (FAR) clause must be included in all SOWs or related security requirements documents for classified contracts. See FAR 52.204-2, Security Requirements for additional information: http://www.acquisition.gov/far/current/pdf/FAR.pdf

The 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. It is as important as any other specification in a contract. It provides the contractor with the security requirements identified in the Security Section of the SOW or related security requirements document necessary for the contractor to adequately safeguard the classified information while performing on the contract. When preparing the DD Form 254, only state the current contract security requirements (not projected requirements). If the contract develops into a higher or lower classification level, a revised DD Form 254 will be prepared.

The key personnel in the preparation of the DD Form 254 are the program/agency security personnel, technical personnel and the contracting office representative (COR). The security personnel recognize the security requirements that the contractor will need to follow. The technical personnel understand what information/ equipment in the program requires protection, and the COR can ensure the contractor complies with the DD Form 254 by incorporating it and any special clauses into the contract.

The DD Form 254 is required to be reviewed every two years or when the contract is modified (such as a delivery order or task order). The designated Industrial Security Specialist (ISS) should perform this review to ensure that the existing security requirements are satisfactory.

If the review is performed and no changes are required, the ISS will provide the contracting office with a copy for review. The contracting office will then send to the contractor, in writing, notification that the DD Form 254 remains valid until the next review or a change occurs in the program.

If the review is performed and changes are required the ISS must provide the contracting office with a revised and signed copy. The contracting office will then incorporate the new DD Form 254 into the contract documents. The new DD Form 254 must be signed by all key personnel.

When filling out the DD Form 254, reasons must be provided for the classification level and the guidance should be written in plain English so it can be easily understood. Use additional pages to expand or explain guidance. Be as specific as possible and include information that only pertains to the contract for which it is issued. Avoid references to Army regulations or guidance, unless it is necessary or when the contractors are integrated/embedded with an Army Unit or Activity.

Provide the COR and Program Manager (PM) information in block 13 on the DD Form 254. It is preferred that the PM and COR sign in block 13 acknowledging they have reviewed the DD Form 254 and are in agreement; at a minimum the COR should sign.

In block 16 on the DD Form 254, enter the name, title, telephone number, address and signature of the designated ISS certifying that the security requirements are complete and adequate for performance of the classified contract. The Army Federal Acquisition Regulation (AFARS) delegates the security manager to sign block 16. The individual signing the DD Form 254 should be the designated ISS, but does not necessarily have to be the security manager. The ISS will ensure the DD Form 254 has been adequately staffed among the appropriate contracting, program, technical and security personnel.

Finally, when the DD Form 254 has been adequately staffed and approved with appropriate signatures, the COR is responsible for ensuring the DD Form 254 is forwarded to the appropriate offices listed in blocks 6c, 8 and 17.

The HQDA, G-2, Industrial Security Team is in the process of developing an Army DD Form 254 Handbook with additional guidance, stay tuned!

Have We Changed Enough?

- General George Casey, CSA

Visit this site to learn more about the G-2 Vision on MI Strategic Rebalance Strategy:

http://www.dami.army.pentagon.mil/site/g-2%20vision/.

This site uses informational podcasts, briefings, personal interviews and videos to communicate the Army's strategy to optimize intelligence support to Army full-spectrum operations.

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

Reporting Suspicious Behavior – It Is Not Tattletaling

As a child we learned "tattle-tailing" is not acceptable behavior. Adults and teachers may have asked, "Are you tattling or telling?" The difference is called "responsible informing." It is human nature to feel uncomfortable about reporting counterintelligence, security, or suitability concerns. No one wants an organization full of snitches, but we do want to prevent espionage and help colleagues before things get completely out of control.

Security professionals are responsible for informing individuals that have been granted a security clearance about their reporting requirements. Reporting is not limited to individual self-reporting. All individuals have a responsibility to report suspicious behavior. Espionage cases or incidences of violence or harm have one thing in common…before these cases came to light, there were indicators present. In a number of cases, reporting of these indicators by a friend or co-worker helped catch a spy. More importantly, timely reporting helps valued employees solve their problems before they led to more serious problems. For more information on People Who Made a Difference, visit the Personnel Security Research Center at http://www.dhra.mil/perserec/products.html. This site provides security professionals useful tools, aids, reports, and other materials.

The Chief of Staff of the Army released a message to all Army activities on December 1, 2009, requiring all Soldiers to report indicators of potential terrorist or insider threat to their chain of command and the local counterintelligence (CI) office. These are also indicators of a security nature and must be reported to the Army Central Clearance Facility as an incident report using the Joint Personnel Adjudication System (JPAS).

Ten Key Indicators of Potential Terrorist Associated Insider Threats to the Army.

1. Advocating violence, the threat of violence, or the use of force to achieve goals that are political, religious, or ideological in nature.

2. Advocating support for international terrorist organizations or objectives.

3. Providing financial or other material support to a terrorist organization or to someone suspected of being a terrorist.

4. Association with or connections to known or suspected terrorists.

5. Repeated expressions of hatred and intolerance of American society, culture, government, or the principles of the U.S. constitution.

6. Repeated browsing or visiting internet websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes without official sanction in the performance of duty.

7. Expressing an obligation to engage in violence in support of international terrorism or inciting others to do the same.

8. Purchasing bomb making materials or obtaining information about the construction of explosives.

9. Active attempts to encourage others to violate laws, disobey lawful orders or regulations, or disrupt military activities.

10. Familial ties to known or suspected international terrorists or terrorist supporters.

In addition, we advocate that these indicators be included in security orientations, annual and refresher training, and be an integral part of the command Security Education and Training Awareness (SETA) Programs. Commands must ensure their security education programs are aligned with AR 381-12, Security and Espionage Directed against the Army.

Customizable Security Guide (CSG)

The CSG is a good source of material for security professionals preparing awareness briefings or articles for newsletters. Topics covered by the Security Guide include procedures for protecting both classified and sensitive unclassified information, standards of personal conduct, employee assistance information, foreign espionage threats and methods, risks associated with foreign travel and terrorism, counterintelligence indicators, computer vulnerabilities, vulnerability to communication intercept and eavesdropping, spy stories, and more…

For more information on CSGs visit the Personnel Security Research Center at http://www.dhra.mil/perserec/products.html.

Test your Security IQ on Reporting Requirements

1. When I accept the privilege of access to classified or other sensitive information, I am also accepting responsibilities that accompany this privilege.
TRUE or **FALSE**

2. My personal life and what I do on my own time is none of the government's business.
TRUE or **FALSE**

3. If I see a co-worker engaging in improper, unreliable or suspicious behavior, it is none of my business and probably wouldn't do any good to report it anyway.
TRUE or **FALSE**

4. I was detained by local law enforcement officials for possible violation of the law against trespassing. Even though I was later released and not charged, I still have to report this to the security office.
TRUE or **FALSE**

5. Serious depression is usually treated as a medical or performance problem, not a security issue.
TRUE or **FALSE**

6. A co-worker mentioned that he thinks people are following him. That's a little weird, but he seems reliable so I should give him the benefit of the doubt and not report to anyone.
TRUE or **FALSE**

7. If I seek assistance for an alcohol problem, a severe financial problem, or an emotional/mental problem, this will adversely affect my security clearance.
TRUE or **FALSE**

8. Anyone with a security clearance is strongly encouraged to report foreign travel plans to their security office, whether the travel is on official business or for pleasure, and even if the travel is only to Canada or Mexico.
TRUE or **FALSE**

9. If I obtain alcohol abuse counseling or treatment at my own initiative, through the Employee Assistance Program, I do not need to report this to the security office.
TRUE or **FALSE**

10. Any planned or actual outside employment or activity that could create a real or apparent conflict with your responsibility to protect classified information must be reported to the security office.
TRUE or **FALSE**

Go to http://www.dhra.mil/perserec/csg/quizzes.htm to check your answers!

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

Contact with Foreign Nationals (Au Pairs)

Recently the Army G-2, SCI Policy Office received inquiries from SCI indoctrinated personnel who want to hire an Au Pair. An au pair (nanny) refers to either a young man or woman between 18 and 26 years of age from foreign countries that live with a Host Family while providing child care services in exchange for the opportunity to live in their country while learning the language and culture.

There are twelve sponsoring au pair agencies designated by the State Department. Sponsors are required to screen and select both host families and au pairs as program participants according to selection criteria stated in 22 CFR 62.9. Host families and au pairs must successfully pass a background investigation including employment and personal character references and sign Host Family-Au Pair Agreements prior to the au pair's placement with a host family.

As referenced in DoD 5105.21-M-1 (M-1), SCI indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or classified national security information.

Also, personnel with SCI access have a continuing responsibility to report, within 72 hours, to their immediate supervisor or local Special Security Office (SSO) security official, all contacts that are of a close, continuing personal association, characterized by ties of kinship, affection, or obligation with foreign nationals. An au pair living within your home is considered a cohabitant and falls within these guidelines.

SCI indoctrinated personnel considering participating in this program will contact your local SSO during the initial phase of these arrangements and provide details of the contact/relationship, to include foreign national's identifying information (name, date/place of birth, passport number, visa number, etc).

The SSO will ask the SCI indoctrinated personnel to fill out the Foreign Contact Questionnaire (APPENDIX F-ANNEX 7) referenced in the M-1. In accordance with ICPG 704.1, a National Agency Check, without fingerprint card, shall be completed for spouses or cohabitants (if applicable) except if already completed in conjunction with a previous or reinvestigation. OPM will electronically forward results of the National Agency Check (NAC) to the Central Clearance Facility (CCF) for adjudication and follow on review and action as appropriate. Lastly, SSO's will forward a copy of the Foreign Contact Questionnaire to the local supporting counterintelligence activity for review and retain an information copy in the individual's personnel file.

Reminder, failure to report foreign contacts, as required, may result in re-evaluation of eligibility for continued SCI access. These instructions are not intended to inhibit or discourage contact with foreign nationals. They are meant to ensure that the nature of the contacts and associations and all relevant information developed are properly documented and disseminated.

For more information on the au pair program visit http://exchanges.state.gov/jexchanges/programs/aupair.html Regulations pertaining specifically to the au pair program are found at (22 CFR 62.31).

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 the unusual situation
- Be mindful of the insider threat
- Be aware that the adversary is always watching
- Be prepared to respond to crisis situation

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

DoD Security Professional Education Development (SPēD) Certification Program

The SPeD program is a certification for DoD security professionals based upon established skill standards and job competency requirements that have been validated within the department The certification has four levels: Entry, Full Performance, Senior and Expert. All security professionals will share core competencies then branch out to specialty areas. 2009 ended with a productive "bang." Army Subject Matter Experts contributed extensively in refreshing the security skill standards. This effort resulted in the DoD-wide agreement on the Defense Security Skill Standards (DS3). The skill standards codifies DoD's expectations of what a security professional needs to know and be able to do to protect its personnel, information, activities, facilities, and operations. Continuing efforts in 2010 will include further definition of skill standards and specialty areas. These skill standards will lay the foundation for development of security certifications.

Accomplishments in 2009 include approval by the DoD Security Training Council (DSTC) members on the following: draft DoD 3305.13-M, DoD Security Accreditation and Certification Manual; the SPeD Certification framework; and the SPeD certification objectives for entry and full performance, levels 1 and 2 respectively. What does this mean? The DoD security community has agreed on the roles and responsibilities for implementing a DoD-wide security certification program. The draft manual will soon go into formal coordination and work will continue on developing implementation guidance. We are on schedule and looking forward to deployment of the pilot program in late summer or fall 2010.

Frequently Asked Questions (FAQs) about SPeD

Q: How do I prepare for the certification test or examination?
A: DSS Academy will be offering online and instructor lead courses to assist in preparing individuals for the certification. In the meantime, take advantage of the many basic online courses available 24-7.

Q: Will new employees be required to have certification?
A: Yes, once certification goes formal, all newly appointed employees, based on identified positions, will have a requirement to become certified within an established period of time. The Army will be developing an Implementation Plan, per the draft 3305.13-M, after it is formally approved. The Implementation Plan will be based on the defined community standards developed under the DSTC. Agencies have five years to fully implement the program.

Q: How is the information about SPeD going to be communicated to the Army Intelligence Community?
A: We will continue to provide updates via monthly newsletters and e-mail communications. We will also continue to conduct SPeD teleconferences as needed to provide updates and answer questions.

Q: ***Will there be grandfathering?***
A: Grandfathering means to allow an exception to a new rule or exempts those already involved in a regulated activity or business from the new regulations. The draft DoD 3305.13 Manual prohibits grandfathering. Certification requirements will apply to all positions that have been identified as having responsibilities for security capabilities and/or performing security activities. The DoD 3305.13 Manual further states that "incumbents will not need to meet certifications, identified as qualification requirements, to retain their defense security positions. Certification will be optional for affected incumbents."

Ms. Luisa Garza
SETA Program Manager
1000 Army Pentagon (2D350)
Washington, D.C. 20310
Ph: (703) 695-2644
Luisa.Garza1@us.army.mil

Training and Awareness on Security Clearances

Security professionals are often asked a myriad of security clearance questions. Fortunately, the DSSA has made available a product "How to receive and maintain your security clearance." This electronic pamphlet is available for downloading at http://dssa.dss.mil/seta/downloads.html. Use it to educate clearance holders of their obligations and reporting responsibilities. A list of potential security concerns is included that serves to help us all make "responsible informing" decisions. I invite you to use this product in your orientation and security awareness training. Reminder, annual security refresher training is a mandatory requirement for those of us that handle classified and sensitive information. This is an opportunity to ensure you are adequately protecting your organization through a sound and robust SETA program. Like in the real estate business... document, document, document.

Government Events in 2010

2010 DISA Customer Partnership Conference
Date: 3-7 May 2010
Gaylord Opryland Resort and Convention Center - Nashville, TN
http://www.disa.mil/conferences/

2010 National OPSEC Conference
Date: 3-7 May 2010
Gaylord Opryland Hotel - Nashville, TN
http://www.ioss.gov/index.html

2010 Worldwide Security Conference
Date: August 2010 - Chicago, IL
Hosted by the Defense Security Service, details TBD.
https://www.dss.mil

Army Event in 2010

HQDA, G-2 Foreign Disclosure Seminar
Date: 9-13 August 2010
Southbridge, MA
***** INVITATION ONLY *****

Industry Events in 2010

NCMS 46th Annual Training Seminar
Date: 15-17 June 2010
Silver Legacy Hotel & Casino, Reno, NV
https://www.classmgmt.com/Home/

2010 ASIS International 56th Annual Seminar and Exhibits
Date: 12-15 Oct 2010
Dallas, TX.
http://www.asisonline.org/

Training Opportunities

Defense Security Service Academy (DSSA)- http://dssa.dss.mil/seta/seta.html

Interagency OPSEC Support Staff (IOSS) - http://www.ioss.gov

Director of National Intelligence (DNI) Special Security Center
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
For course descriptions, cost and registration information go to http://nstii.org/index.html

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