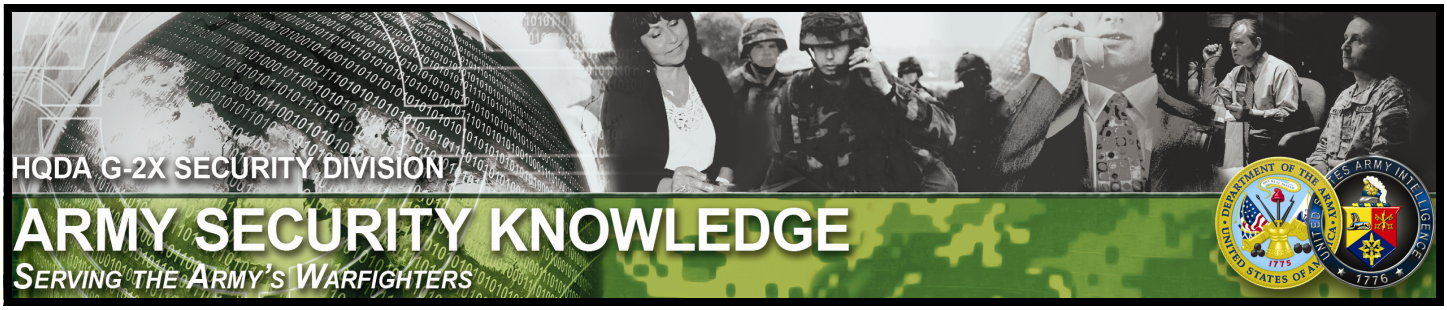

Senior Security Advisor Announcement

It is my pleasure to introduce Mr. Karl Borden to the Army community. Karl came on board May 24, 2010 as the Chief of the Security Division. Karl comes to us with a wealth of multi-disciplinary security experience. He has held leadership positions with the Navy, NASA and ManTech Corporation. I know you all will welcome him to our Army family. We will formally receive him at the upcoming 2010 Worldwide Security Conference in August.

Sincerely,

Patricia P. Stokes
Senior Security Advisor, DISL

Message from the Security Division Chief

I am pleased to revitalize the Annual HQDA, DCS, G-2 Security Award Program. Established in July 2004, the Security Award program was designed to recognize an Army security professional and an Army Command for establishing a dynamic and effective security program. The HQDA, DCS, G-2 Security Award Program consists of two awards: the Thomas Dillon Security Professional of the Year and the Security Center of Excellence.

The "Thomas Dillon Security Professional of the Year" Award was designed to provide award recipients the opportunity to be recognized by their peers and the Army security community as personifying the highest standards of leadership and security excellence. These recipients are security professionals who have demonstrated outstanding, innovative individual performance and contributions in fulfilling security duties or establishing security programs that further the Army security posture.

The HQDA, DCS, G-2 "Security Center of Excellence" Award showcases the Army Command that best illustrates the development and deployment of a dynamic and effective Command security program. This award allows the HQDA, DCS, G-2 to recognize the uniquely important contributions and achievements made by the Army Command. The Award is designed to recognize the importance of leadership and participation in the establishment and sustainment of an effective Command security program.

Commanders and Directors of Security for Army Commands (ACOM), Army Service Component Commands (ASCC), Direct Reporting Units (DRU), Field Operating Agencies (FOA), US Army Reserves, Army National Guard, Program Executive Offices (PEO) and direct reporting Program Managers (PM) may forward a nomination packet to HQDA, ODCS, G-2 (DAMI-CDS) for consideration. Award criteria, nomination information and form completion instructions will be posted to the HQDA, ODCS, G-2 website, soon. The HQDA, DCS, G-2 point of contact is Ms. Luisa Garza, SETA Program Manager.

Individually and collectively, both the Thomas Dillon and Security Center of Excellence Awards remind us that our Nations Security is paramount and being recognized for security excellence is an amazing acknowledgment. Let us all strive for Security Excellence!

Karl Borden
Chief, Security Division

Arrivals

Karl Borden (Security Chief) - May
Allan Polk (ARTPC) - June
Donald Rhoads (SAP) - June

July 2010
Inside This Issue

ARTPC POC

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

Critical Program Information and Supply Chain Risk Management are Not the Same Thing

In the January 2010 issue of ASK Newsletter, we discussed what should be done if Critical Program Information (CPI) was identified after the Milestone B Review. In this edition of the newsletter, we would like to build upon that knowledge and introduce some additional information about when CPI may be identified. We will also introduce you to Supply Chain Risk Management (SCRM) and explain how these two different areas must work together to ensure a technical and tactical advantage to the Warfighter.

CPI Identification
DoDI 5200.39 not only requires the identification of CPI early in technology development but also to refine CPI at each milestone. This requirement continues throughout the lifecycle of all military systems. Ensuring security engineering and protection is integrated into Army systems as early as possible allows us to place protection into military systems while designing the system. Adding protection after the system has been designed can incur added cost, physical changes and additional operating procedures based on the add-on security mechanisms.

In a nutshell, that means that protection measures for old CPI should be reviewed and assessments for new CPI should be performed any time there is a significant change to the system or if the system will be deployed in a new way. The identification and protection of CPI is a never ending process that should continue throughout the lifecycle of the system.

Previously, Army systems would go through the development process and the only thing that was required was maintaining the system until it was replaced by a new system. Today's Brigade Combat Teams are supported by an incremental development approach that ensures capability packages are fielded rapidly to meet Army mission requirements. The ARTPC can assist program managers in the identification of new CPI within capability packages and ensure that CPI previously identified is still afforded proper protection.

Supply Chain Risk Management
Counterfeit electronic components have become an increasing problem in the last few years for all of us as consumers but it is also affecting industry and the government. SCRM is the management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport).

The Navy requested the U.S. Department of Commerce examine the extent counterfeits have infiltrated U.S. industrial and defense supply chains in June of 2007. The Department of Commerce published the "Defense Industrial Base: Assessment of Counterfeit Electronics" in January 2010. The assessment surveyed 378 commercial companies and government organizations from 2005-2008. 39% of those surveyed encountered counterfeit electronics. The counterfeit electronics were identified within original component manufacturers, distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and DoD agencies. The assessment also identified an increase of counterfeit incidents from 3,868 incidents in 2005 to 9,356 incidents in 2008.

Congressional inquiries led to a Government Accountability Office (GAO) "Defense Supplier Base" report dated March 2010. The GAO report stated: "**Almost anything is at risk of being counterfeited** including fasteners used on aircraft, electronics used on missile guidance systems, and materials used in body armor and engine mounts. Counterfeit parts have the potential to cause a serious disruption to DOD supply chains, delay ongoing missions, and even affect the integrity of weapon systems. Counterfeits are not limited to the DOD supply chain and exist in other government entities, such as the National Aeronautics and Space Administration and the Department of Energy, as well as in many commercial settings as diverse as software, commercial aviation, automotive parts, and consumer electronics and can threaten the safety of consumers."

ASA(ALT) is currently working with Industry, DoD agencies and the other military services to standardize existing requirements to identify and mitigate counterfeit parts from entering the supply chain.

Different but Complimentary
CPI and SCRM are two distinctly different areas that help protect critical information. Although separate they are interrelated. For example, let us assume that we have a guidance system inside a missile. A portion of the guidance system is a military grade circuit that has CPI programmed into it. If a civilian grade replacement circuit was purchased and then reprogrammed as part of the guidance system there could be some serious problems. A civilian grade circuit may be unable to withstand the operating environment that the missile is subjected to and its failure could cause the missile to never reach the intended target. This is an example where the proper application of SCRM would prevent the introduction of the lower grade circuit, thus supporting the protection of CPI directly. SCRM can also support CPI indirectly. SCRM should be used to prevent a faulty computer hard drive from entering the Army supply system that might be used to archive CPI documents for a program. SCRM is one means that is used to protect CPI by ensuring that authorized parts and components meet military specifications that enable the WARFIGHTER to accomplish the mission.

Protecting with SCRM does not require CPI to be involved. SCRM can protect anything that enters the Army supply chain. Boots, shoes, uniforms, tires and all other items in the Army have specifications that must be met. SCRM is a method to ensure that items that enter the supply chain meet those specifications and function properly. Think of SCRM as a potential protection countermeasure in the indemnification of Critical Program Information (CPI) while integrating and coordinating RTP and program protection activities Army wide.

Click below for copies of the documents in this article:

Department of Commerce published the "Defense Industrial Base: Assessment of Counterfeit Electronics"

Government Accountability Office (GAO) "Defense Supplier Base"

If you have any questions, comments or suggestions regarding this article, please feel free to contact Mr. Jay Prather, (703) 601-1576, jay.r.prather@us.army.mil or Mr. Gary Gansauge, 703-601-1923, gary.gansauge@us.army.mil. We look forward to hearing from you.

COMSEC / TEMPEST / ISSM POCS

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

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

Technical Security Team

By Harry Byrd

Our most significant achievement since the last edition of the newsletter is the publication of AR 380-27 Control of Compromising Emanations. It was published on 19 May 2010 with an effective date of 19 June 2010, and is available on the APD Website at https://akocomm.us.army.mil/usapa/epubs/DR_pubs/DR_b/pdf/r380_40.pdf. It is a complete revision of TEMPEST policy, published at the UNCLASSIFIED, For Official Use Only level. It supersedes the entire TEMPEST portion of AR 381-14 Technical Counterintelligence (TCI) dated 30 September 2002. The DCS G2 Technical Security Team takes great pride in this announcement due to the complexity of the technical issues involved and the diligence required in accomplishing this objective.

AR 380-53, Communications Security (COMSEC) Monitoring has been formally staffed and all comments have been adjudicated. As of 12 March 2010 the draft was submitted to the Office of the Judge Adjutant General (OTJAG) and the Army Office of General Counsel for review. It is our intent to have AR 380-53 submitted to Army Publishing Directorate (APD) within 60 days of approval by OTJAG.

1. Another responsibility of the Technical Security Team is the publication of AR 380-40, Policy for Safeguarding and Controlling Communications Security—COMSEC Materiel. AR 380-40 has now been resubmitted for formal staffing as of 18 May 2010. Currently, we are collecting comments from the various Army Commands and in turn will adjudicate the comments prior to submission to OTJAG and OGC.

The Technical Security Team has completed all of it's scheduled staff assistance visits (SAVs) for this fiscal year and are currently working to identify the commands to be visited next year as well. Let us know if you would like the Technical Security Team to visit your command. The commands in which we visited this year include The Army Test and Evaluation Command (ATEC), United States Army Special Operations Command (USASOC) and United States Army Training and Doctrine Command (TRADOC). We want to express our appreciation for the professionalism afforded to the HQDA DCS G2 Technical Security Team while conducting the SAVs at each of these commands. We would also like to commend the commands on their existing programs and diligence in remaining compliant with Army policy.

The recent Global Information Partnership Conference (GIPC) held at Ft. Huachuca, AZ from 5-9 May was very productive. The Team led workshops concerning black key operations, IIA-002-2010, Controlled High Value Products and various COMSEC related topics. In addition, the Team participated in the Policy and Procedures workshop and received valuable comments from the field for better methods to conduct COMSEC operations. These comments were beneficial and several have already been incorporated into the revision of the AR 380-40.

The Technical Security Team continues to host video-teleconferences (VTCs)/telephone conferences (TCONs) on a quarterly basis, to ensure information is relayed to security professionals in the field and to solicit input from commands. We have been fortunate to have strong attendance and participation and encourage your continued support. The conferences serve as a conduit to ensure the needs of the security professional are heard and in turn incorporated into Army policy. Our next VTC is scheduled for 15 September 2010.

In closing, the Technical Security Team remains committed to addressing the needs of the Army and ensure the security professional's mission is successful. Therefore, we welcome comments concerning this article. Feel free to contact Rick Niederkohr or Harry F. Byrd Jr. with questions, comments or suggestions or if you would like to have any particular topics addressed during our VTCs or in future newsletters.

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

What's in the Fridge?

Understanding the Relationship between AKO and Foreign Disclosure

by Dave Grob

As a parent, few things gall me more than opening the fridge to find the last slice of pie or hunk of pot roast gone. The guidance to my kids was clear… these are mine, they are not for you. My wife is not a fan of pie or pot roast and Barney the Beagle has yet to learn how to open the refrigerator, so Jacob and Mary became the prime suspects. When I put them under the bright lights and questioned them as to what happened to my food , Jacob informed me that his friend Nathan ate the pot roast and Mary confessed that Grace and Jessica split the pie. If this scenario sounds familiar, then you are well on your way to understanding the relationship between AKO and foreign disclosure, you just may not know it.

The communities of interest are the ODCS G-2 who provides foreign disclosure guidance and the CIO/G-6 who is the proponent for AKO. In keeping with the above scenario, the disclosure community sets policy on what foods (information) are available to particular individuals. The CIO/G-6 controls the access the refrigerator (AKO) where the food and beverages reside.

The disclosure community provides its guidance in the form of a Delegation of Disclosure Authority Letter (DDL) and policy resident in AR 380-10. The AKO/disclosure issue centers on unclassified information and a certain population of *"non-U.S. citizens acting in an official capacity for their home country"* (FLOs, MPEPs, CPPs, ESEPs etc…). AR 380-10, paragraph 2-9 already grants local commanders and agency heads the authority to disclose unclassified information through the supporting DDLs that they approve. DDLs are required for FLOs, MPEPs, CPPs, ESEPs, etc as a condition of approving their Request for Visit Authorization (RVA). As a result, the disclosure community has already provided guidance to support access to AKO for this population of *"non-U.S. citizens acting in an official capacity for their home country"* as part of the RVA process. In other words, the permissions for what they can eat have already been established.

The relationship between "the fridge" and the "food" is articulated in AR 380 -10, paragraph 1-10. c where the CIO/ G-6 is charged with the responsibility *to "Formulate, establish, and disseminate policy and procedures for access to computer networks, to include foreign representatives and nationals."* The CIO/G-6 controls this access to the fridge (AKO) through guidance in AR 25-2 and supplemental AKO/DKO Procedure # AKO-PRC-0031 dated 15 March 2010. This population of *"non -U.S. citizens"* is addressed as Account Application Category 8. One of the provisions for Category 8 applicants is for a DDL. As you can see the DDL issue is resolved prior to the approval of the RVA process. The approved RVA is also utilized as an authoritative document necessary for the issuance of a common access card (CAC).

The command or organizational/ installation FDO has the responsibility of ensuring that if access to AKO is required by a Category 8 applicant, that this requirement is accounted for in the supporting DDL from the outset. They should also plan to work with the supporting installation Information Assurance Manager and others to coordinate the Category 8 application. The FDO should also make sure their command/activity understands that approval for access to the "fridge" is not a call they can make at a local level. The sponsoring organization/activity can only provide a recommendation and supporting justification. That recommendation must be made with some sort of risk assessment in mind. AKO, like the refrigerator, may provide certain individuals access to things they were never intended to consume.

Getting back to the pie and pot roast, I knew my kids had friends in the house all the time and the fridge was always a center of gravity. As such, I probably would have been better served by placing a note with some restrictive marking on food in question. FDOs should remind their organizations of things along similar lines as they consider posting or providing information for inclusion on AKO. Until such a time as they build a "refrigerator" with swipe access to the crisper or other separate access controlled storage area, we will have to assume risk for any "food" we place in there.

The disclosure community must also deal with a problem set I don't have with food in the fridge. Unlike food, information resident in AKO has no shelf life. This "non-perishability" must also be factored in as part of the risk assessment/recommendation and justification process when sponsoring a Category 8 applicant.

At the end of the day, whether it's leftovers or access to AKO, we have a responsibility to understand that in both cases we are dealing with two separate but related issues… access/ control and contents/consumption. When we don't understand this from a risk/benefit perspective and work the issue as a community of shared stakeholders, we should expect someone is not going to be happy with what's in the fridge or what happens with unauthorized consumption. None of this sits well with my stomach. How about yours?

Industrial POCs

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

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

James S. Cogswell Outstanding Industrial Security Achievement Award

By Pam Spilman

There is no question that the entertainment industry award shows (Emmy, Oscar, Tony and Grammy's) are widely popular due to being surrounded with drama and intrigue. Who will be deemed the best actor or actress this year? Who is the best new artist? Who wrote the best musical score in a hit movie? What are the celebrities wearing on the red carpet? Have you ever thought about the best cleared contractor facility in the National Industrial Security Program? The Cogswell Award is the Emmy, Oscar, Tony or Grammy of Industrial Security. So, what exactly is the Cogswell Award?

The Cogswell Award is the most prestigious honor the Defense Security Service (DSS) may bestow upon cleared industry. Of the nearly 13,000 cleared contractor facilities, less then one percent are selected annually to receive this award.

The Cogswell Award was established in 1966 and was named in honor of the late Air Force Colonel James S. Cogswell, who was the first chief of the unified office of Industrial Security. Colonel Cogswell was responsible for the underlying principle of the Industrial Security Program. That principle is the need for a true partnership between industry and government to ensure the protection of classified information, materials and programs.

The criterion for the award focuses on the principles of industrial security excellence. The principles include establishing and maintaining a security program that goes well beyond the basic National Industrial Security Program requirements and providing leadership to other cleared facilities to set high security standards. To receive consideration for the award, a cleared facility must be nominated by the DSS Industrial Security Representative assigned to the facility, receive two consecutive superior industrial security review ratings and show a sustained degree of excellence and innovation in their overall security program management, implementation and oversight. The cleared facility also must have responded to the annual Personnel Security Investigation (PSI) survey.

The nominees go through a vigorous national vetting process which includes external vetting by a national review team. The national review team consolidates and ranks the nominations. The ranked listing is then submitted to the Director of DSS for final approval. DSS only presents the Cogswell Award to those nominees who epitomize industrial security excellence and have a reputation for integrity and lawful conduct in their business dealings.

On 16 June 2010, DSS announced nine cleared contractor facilities selected to receive the 2010 James S. Cogswell Outstanding Industrial Security Achievement Award at the NCMS 46th Annual Training Seminar in Reno, Nevada. This year the Cogswell Awards were presented to Honeywell Technology Solutions, Inc., Lexington Park, MD; Aerospace Corporation, Albuquerque, NM; UH Maui High Performance Computing Center, Kihei, Maui; Amsec, Virginia Beach, VA; The Camber Corporation, Huntsville, AL; L-3 Unmanned Systems, Easton, MD; L-3 Services, Inc., Colorado Springs, CO; Northrop Grumman Information Technology, Inc., Niceville, FL; and Lockheed Martin Corporation – Missiles and Fire Control, Chelmsford, MD.

As the entertainers are revered for their accomplishments and recognized for their talents; cleared contractor facilities are respected for excellence in the security community. It is an honor to be acknowledged and recognized for outstanding security measures and best practices. The prestigious Cogswell Award is a testament to dedication in maintaining world-class security standards.

Congratulations to all the winners!

INFOSEC POC

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

Controlled Unclassified Information

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 of sensitive unclassified information. The first step will be the issuance of an Executive Order that will outline the basics of the program. The secondary effort will be the issuance of specific policy agreed upon by the national level working groups and then finally the issuance of agency specific policy.

The Defense Security Service Academy (DSSA) has developed a short web-based course on CUI awareness to provide an overview of the CUI framework. This online course will help prepare DoD personnel for the expected implementation of CUI. The training is hosted on the DSSA website at https://enrol.dss.mil/courseware/cui. We encourage you to ensure all personnel working with sensitive unclassified information take this training.

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

Security Clearance Reform News

In accordance with the Joint Security and Suitability Reform Team (JSSRT) Goals to improve the Security and Suitability Process, the Office of Personnel Management (OPM) will deploy the new SF86 in the electronic Questionnaire for Investigations Processing (e-QIP) system in December 2010. The new SF86 will support an improved data collection methodology, which includes expanded questioning based on the applicant responses. The expanded data collection will automatically flag background investigations to trigger certain investigative requirements. The new SF86 e-Application contains improved validation logic and will reduce the need for manual review or data correction. The new form will help facilitate the complete, accurate and timely initiation of requests for investigation.

Operation Warfighter and Security Clearances

By Monique Hampton

On 18 March 2010, the Under Secretary of Defense for Intelligence issued guidance to support the DoD Operation Warfighter Program. The DoD Operation Warfighter Program and other similar programs support our wounded Soldiers by providing temporary assignments/internships while they convalesce at military treatment facilities throughout the US. Many of the internship positions require security or intelligence related skills and as such requires a security clearance.

Wounded Warriors who receive conditional offers of employment with any DoD entity, DoD contractor, or other Federal Government position will be processed for the requisite security clearance as an expedited service to the Office of Personnel Management (OPM). In the event the perspective employer is an outside agency who requires that the investigation be submitted through their investigative service provider, every effort will be made to facilitate this process to ensure minimal impact to the Wounded Warrior. Wounded Warriors pending a Medical Evaluation Board (MEB) and/or a Physical Evaluation Board (PEB) will be processed for a security clearance, to include the requisite background investigation, regardless of an impending separation.

Security Managers processing security clearance investigations in support of Operation Warfighter will follow the instructions below:

1. Investigations should be identified to OPM as PRIORITY SERVICE cases. Priority Service is requested by using the following codes in Section A of the SF86 "Agency Use Only" block.

- NACLC: Case Type 08A
- ANACI: Case Type 09A
- SSBI: Case Type 30A
- SSBI-PR: Case Type 18A
- Phased PR: Case Type 19A

2. Section B of the SF86 "Agency Use Only" block MUST be populated with EXTRA COVERAGE CODE WW. This will ensure expeditious scheduling and facilitate rapid completion.

3. Upon submission of an investigation, it is requested that OPM be notified via e-mail to operationwarfighter@opm.gov. The e-mail should contain subject's full name and the e-QIP Request ID Number, as well as the name of DoD's point of contact should OPM need additional information.

If a Wounded Warrior possesses a security investigation but does not have the appropriate adjudication, a Request to Research/Upgrade Eligibility (RRU) will be submitted through the Joint Personnel Adjudication System (JPAS). RRUs should identify the Soldier as a WW and request an expedited adjudication. Once the RRU is submitted, the Security Manager can call the CCF Help Desk, (301) 677-7075, for a clearance status update. Any questions about RRUs for Wounded Warriors can be directed to Mr. Timothy Schroeder at timothy.l.schroeder@us.army.mil.

Wounded Warriors have given so much and the Office of the Army Deputy Chief of Staff, G-2 is committed to ensuring that these Soldiers are provided outstanding security clearance care to ensure a successful return to duty or transition to another employment opportunity.

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

Update On SCIF Construction Policies Intelligence Community Directive (ICD)705/ Intelligence Community Standard (ICS) 705-1

By Cliff McCoy

Recently, the Director of National Intelligence (DNI) took another step in unifying more stringent physical security standards within the Intelligence Community by signing and releasing ICD 705. ICD 705 is the policy directive which establishes SCIF compliance requirements within the Intelligence Community. This directive will be followed by the Intelligence Community Standards (ICS) 705-1, which will set forth the physical and technical security standards that shall apply to all SCIFs. ICS 705-1 will enable uniform and reciprocal use across all IC elements and assure information sharing to the greatest extent possible. The Deputy Director of National Intelligence for Policy, Plans and Requirements has a mandate to issue the ICS no later than 90 days after the effective date of ICD 705.

The SCI Policy staff is working with the Defense Intelligence Agency (DIA) Policy Office and the DIA SCIF Support Branch to develop implementation guidance applicable to the ICD/ ICS. The proposed implementation guidance being worked at this time identifies a 180 day window which serves as a buffer between the time the ICS is expected to be released in August and the anticipated effective date in February 2011. We anticipate the language to read as such, "SCIFs at or beyond 30% design as of 24 February 2011 will continue compliance with DCID 6/9 and all others must comply with ICS 705 for construction and modification". As you all know, this office along with the DNI Special Security Center and the rest of the Intelligence Community has been aggressively working on this replacement policy directive to DCID 6/9 for several years and we are on the verge of deliverance.

DIA is in the early stages of developing training modules and automated tools to assist SSOs/SSRs in a variety of areas as we prepare for transition to the new policy. One of those training modules will assist security officers in developing a Construction Security Plan (CSP) which addresses the application of security to SCIF planning, design and construction efforts.

Upon release of the ICS in August, we will host another VTC and invite representatives from DIA to address any specific concerns you may have at that time.

Stay Tuned!

DIA's 2010 Worldwide Special Security Office (SSO) Conference

On 25 Jun, the Defense Intelligence Agency (DIA) released a message announcing the "2010 Worldwide DoD Defense Special Security System (DSSS) Conference" also known as the Worldwide SSO Conference. The conference will be held in San Antonio, TX, at the Marriott Riverwalk Hotel, from 30 November- 2 December 2010. All DoD Special Security Officers and Contractors performing SSO functions are invited to attend.

This year's conference theme is "Securing Intelligence Information - Today and Tomorrow." This will be the first SSO conference in three years and a great opportunity to review the current state of the DoD Special Security System, educate ourselves on recent changes, and to discuss and shape the way ahead. The conference will cover a wide range of SSO functions with a focus on cyber and insider threats. DIA is soliciting your input for agenda items, information briefings and workshops on specific SSO functions. You may provide your input via email to the NCSI website below NLT 31 Jul 10.

Lastly, the conference is being supported by National Conference Services, INC (NCSI), a commercial event planner, and there is a conference fee per attendee this year. The conference fee is $449.00 during early registration (thru 15 Oct 10), and thereafter, the fee will be $499.00. Registration is online at HTTP:// www.ncsi.com//dsss10//ndex.shtml. The final agenda will be posted to the NCSI website in August.

Hope to see you all there!

SETA: Security Education Training and Awareness

Security Professional Education Development (SPēD)

On 18 May, we held a VTC for the Command Career Program Managers (CPMs) to share information on SPēD and how it will impact our security careerist. CPMs will play an important role as the implementers in this program. One of the major events discussed was the "soft launch", which will give volunteers a "free swing" at the test. Details will be provided to the CPMs in the next couple of weeks for dissemination along with timelines and application process for volunteers.

The Defense Security Service Academy (DSSA) recently updated their website to include new information on SPēD. Visit http://dssa.dss.mil/seta/sped/sped.html to learn more. If you have Army-specific questions, feel free to contact the Army POC, Luisa Garza at SETA@MI.Army.mil.

SETA Website

We are into our fourth month already! Thank you for taking a look at the new SETA website. Please let us know how we can improve. If you haven't already done so, visit us at http://www.dami.army.pentagon.mil/site/seta/default.aspx. We've recently added new information related to TEMPEST, Personnel Security and Industrial Security. To help you stay connected to the latest information from SETA, subscribe to the RSS 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.

Why re-invent the wheel?

Here is a great resource for your threat awareness program. Scott Daughtry, Senior Counterintelligence Officer, publishes "The CI Shield". This weekly newsletter presents real world examples of threats posed against corporate proprietary and U.S. military technologies. To subscribe, send your request to scott.daughtry@kirtland.af.mil and include the name of your employer, your name / job title / phone number. Sample article topics: China's expansion of economic espionage boils over; Soviet spy map reveals Norfolk secrets Report: Canada's Ambassador to Tehran Was a CIA Spy; Chinese Attack On Google Seen As Cybertheft; Court Documents: Defense official's mom introduced him to Chinese spy; Buckle in for the Cyber 'Wilderness of Mirrors'; Keychain Car Key Security Spy Camera.

Training

DSSA recently hosted its annual Industrial, Information, and General Security External Customer Training Program Review. HQDA, G-2 Industrial and Information Security represented the Army. The purpose of this meeting was to review and discuss DSSA's continuing efforts to support the training needs of the DoD, Industrial, Information and General security professional and practitioner. Topics discussed included:

Industrial:

- Update on the transition of the FSO Curriculums & Basic Industrial Security for User Agency Personnel Course
- Overview of current NISPOM Chapter 8 courses:
- NISPOM Chapter 8 Requirements (on-line course)
- NISPOM Chapter 8 Implementation (Instructor-led course)
- Planned development for NISPOM Chapter 8 courses
- Introduction to the NISP Certification and Accreditation Process

General and Information Security:

- SETA/DSSA Initiatives
- Current and future Web-based courses
- CAPCO Marking Scheme (pending policy completion)
- CUI (pending policy completion)
- Physical Security Planning and Implementation Course
- Containers and Storage Facilities Course
- Physical Security Virtual Environment Exercise
- Information and General Security Curriculum Analysis
- Wrapping Classified Information Video
- SAP Overview (e-Learning Course)
- Security Policies, Principles, and Programs Course
- Hip Pocket Deployment Tool

Physical Security Virtual Environment Exercise Development:
Carney, Inc., one of the contractors working with the DSS Academy on course development processes, is currently developing a virtual environment exercise. This exercise is focused on physical security, but may have applications across many of the disciplines of security. The environment requires students to complete the exercise by navigating through the various "worlds" evaluating the presence, or lack of, physical security equipment or procedures used to protect those "worlds." There are several areas currently under development including: a classified storage vault, arms room, general office area, conventional arms, ammunition, and explosives area and a nuclear weapons storage area.

DSSA has updated their DoD Security Specialist Training Courses to include basic industrial security. Students must complete the following pre-requisites:

- Introduction to Information Security (2 hours)
- Original Classification (1.5 hours)
- Derivative Classification (2 hours)
- Marking Classified Information (2 hours)
- Security Classification Guidance (2 hours)
- Developing a Security Education and Training Program (2.5 hours)
- Transmission and Transportation for DoD (2 hours)
- Introduction to Physical Security (1.5 hours)
- Physical Security Measures (2.5 hours)
- Risk Management for DoD Security Programs (3 hours)
- Introduction to Personnel Security Adjudications (3 hours)
- Introduction to Personnel Security (2 hours)
- Introduction to Industrial Security (1 hour)
- OPSEC Fundamentals (4 hours)
- Lock and Key Systems (1.5 hours)

Are you responsible for developing and implementing an organization's security awareness and education program?
DSSA offers two excellent courses that will prepare you for development of the program and to aid in developing solutions. "Developing a Security Education and Training Program" is an interactive web-based 2.5 hour course that provides a thorough understanding of the DoD and National Industrial Security Program (NISP) policy requirements, best practices and instructional methods for developing and implementing a security education and training program. After completing this course, the student will be familiar with the requirements for security education and training program and the knowledge to develop a program.

The Security Awareness for Educators (SAFE) course discusses how to create an effective security awareness and education program and identifies solutions for overcoming the challenges anyone tasked with security awareness and education duties faces. The course covers how security professionals can create a program on a limited budget, gain management support, motivate co-workers, promote themselves, and prepare and conduct effective security awareness presentations. The course is an interactive blend of presentations, group workshops, and practical exercises during which attendees work in groups tackling challenges and sharing solutions. It's a three day instructor-led course. The SAFE course is different in that there are no exams involved in the course. There are a number of practical exercises, but there is no pass/fail requirement for the course.

Everyone is encouraged to take advantage of these courses as we work with DSSA to develop additional curriculum to meet Army's security mission.

2010 Worldwide Security Conference

Army will be well represented at the upcoming 2010 Worldwide Security Conference to be held in Chicago on August 3-6. We maxed out the Army allocations with mid-to-senior level security professional across all Army commands. HQDA, G-2 Security Division has put together a full week of Army sessions and breakouts. The first session, Army Investigative Enterprise Solution, will be presented on 2 August at 1600, so plan accordingly. We have planned icebreakers and networking opportunities so be sure to bring your business cards. HQDA, G-2 Staff will be present at registration to welcome and assist you.

Ms. Luisa Garza
SETA Program Manager
1000 Army Pentagon (2D350)
Washington, D.C. 20310
Ph: (703) 695-9610
Luisa.Garza1@us.army.mil

"Motivation is key"