



Fort Belvoir Security Newsletter

Directorate of Plans, Training, Mobilization, and Security (Security and Intelligence Division)



April—June 2009, 3d QTR FY09

Newsletter Contents

Installation Security Manager's Message	1
Security and Intelligence Division	2
Information Security	3
Security Education Training and Awareness, and Operations Security	4
Industrial Security and Foreign Representatives	5
Personnel Security	6

Upcoming Events

**12 May: INFOSEC
Annual Refresher**

**13 February: OPSEC
Annual Refresher**

**7-8 July: Information
Security Orientation**

**4-12 August:
Information Security
Management**

For more information and an up-to-date schedule of future security training opportunities, events, or activities, contact the Security Education Training and Awareness Program Manager (*check the contact page*)

Message from the Installation Security Manager

Greetings,

Please enjoy our latest Security newsletter. The Security and Intelligence Division works hard towards providing Security Managers across Fort Belvoir with useful tools and information to improve their organization's Security Programs, and we hope the newsletter helps attain that goal. This edition has lots of great and useful information. If you or your subordinate security specialists need refresher training on Information Security, check out Page 4 to get information on our upcoming courses.

Margie Ritchie

Installation Security Manager

The upcoming conversion to the **Defense Civilian Intelligence Personnel System (DCIPS)** will affect many Department of Army Security Specialists. DCIPS was originally created in 1996 by Congressional authorization in order to address the unique needs of Civilian employees in the Defense Intelligence Community. In 2004 DCIPS evolved with a new performance management and pay banding system, similar to the National Personnel Security System (NSPS). In July 2009, the Army will begin converting applicable security and intelligence Civilian employees to DCIPS. To find out more about DCIPS, contact your servicing CPAC, or visit:

<http://www.cpol.army.mil/cgi-bin/permis/tree.cgi?MainSection=DCIPS>

Security and the Law

32 CFR § 2001.82q

"Security-in-depth" means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

Any private or commercial product, service, or information presented in this newsletter is provided for the awareness of the security professionals receiving it, and does not constitute an official government endorsement. Please submit your comments and/or suggestions regarding this newsletter to: john.davis@conus.army.mil

Security and Intelligence Division Overview and Staff

Security and Intelligence Division

The Security and Intelligence Division includes Information Security (INFOSEC), Industrial Security (IS), Security Education Training and Awareness (SETA), and Personnel Security (PERSEC). We also support Foreign Representative Visitor Requests, the Installation Operations Center, and the Force Protection program.

Note: If you have classified material that needs to be destroyed and you do not have GSA approved equipment, contact our office so that we can help coordinate destruction.

Under the Army INFOSEC Program, the security office provides Staff Assistance Visits (SAVs), courtesy inspections, and other INFOSEC mechanisms to Garrison and supported tenant organizations. We are here to help any organization on the Installation improve its INFOSEC program.

We are currently planning for our next Security Manager's Meeting. Any Security Officer or Specialist that would like to attend needs to provide their information to the Installation Security Manager at the number below. The next meeting will cover any recent changes in security policy, as well as a review of information from the Department of Army Security Manager Collaboration Forum in St. Louis, MO, 23-26 February 2009.

Feel free to contact any member of the security team at the numbers below.

ATTENTION!!!

If you missed the latest Information Security Annual Refresher Training (a requirement under AR 380-5 for all Army personnel, military or civilian), please contact the Security Education Training and Awareness (SETA) Program Manager at 805-3058, or 805-5243.

Staff

Installation Security Manager: 703-805-4012

Lead Information Security: 703-805-2416

Information Security Program Manager: 703-805-5243

Information Security Specialist: 703-805-2613

SETA Program Manager: 703-805-3058

Industrial Security and Foreign Representatives: 703-805-5262

Fax: 703-805-4010

Lead Personnel Security: 703-805-2952

Personnel Security Specialist: 703-805-4006

Personnel Security Specialist: 703-805-3515

Personnel Security Specialist: 703-805-4015

Fax: 703-805-4017

Installation Security
Manager
Location:
Bldg 269, Room 30A

Office Hours
Monday-Friday
0730-1630

Information Security
and Intelligence Office
Location:
Bldg 269, Room 030

Office Hours
Monday-Friday
0730-1630

Personnel Security
Location:
Bldg 269, Room 129

Office Hours
Monday-Friday
0730-1630

★ Classified documents must be destroyed using GSA approved high-security shredders, disintegrators, pulverizers, or by burning.

Information Security

Reminder: Information Security (INFOSEC) is covered under AR 380-5, and is everyone's responsibility. This program is primarily designed to implement controls and measures for protecting and safeguarding classified information from unauthorized disclosure. Army personnel are required to receive an initial INFOSEC briefing upon arrival to a new organization, and annually for refresher training. Contact the INFOSEC Program Manager regarding security concerns in your organization.

Understanding your responsibilities in preventing and responding to security incidents or compromises (including classified spillages).

According to AR 380-5, Paragraph 10-1a, the compromise or loss of classified information can cause damage to our national security. If classified material is lost, it cannot be determined if the information has been compromised. When loss or compromise of classified information happens, immediate action is required to minimize any damage and eliminate any conditions that might cause further compromises. Each incident in which classified information or material may have been lost or compromised must be the subject of a preliminary inquiry as described in AR 380-5, Chapter 10. The purposes of this preliminary inquiry will be to:

- Determine whether classified information was compromised and, if so, whether there is damage to the national security.
- Determine what persons, situations, and/or conditions were responsible for or contributed to the incident.

For more information on preliminary inquiries and other responsibilities when responding to actual or potential security incidents, check out Chapter 10 in AR 380-5, or contact the Installation Security Manager.

Understanding Your Responsibilities with Destruction of Classified and Unclassified Information

All information in the Army is categorized in some way. Whether you are handling classified or unclassified materials, every category of information has its own destruction requirements.

If your organization handles classified information or materials, your security policy should address how the organization meets the destruction requirements set forth in applicable information security regulations (AR 380-5 for Army, and DoD 5200.1R for DoD Agencies). But many organizations, activities, or offices do not handle classified materials. So, what is Fort Belvoir's policy for destroying information that is **UNCLASSIFIED**?

- **Unclassified** unofficial paper materials (such as flyers, newspapers, etc) WILL be recycled, according to Fort Belvoir Policy Memorandum #2, Fort Belvoir Qualified Recycling Program.
- **Unclassified** official documents generated during day-to-day business—including email printouts, memoranda or other official correspondence, operational orders and plans, standard operating procedures and continuity books, presentations, reports, organizational charts or official personnel documents, official surveys (complete or blank), or official forms (not including blank copies of unclassified forms)—regardless if they do not contain any protective marking (such as FOUO, Law Enforcement Sensitive (LES), Sensitive but Unclassified (SBU), Controlled Unclassified Information (CUI), or Privacy Act), will be destroyed internally using a standard office shredder, or through the Garrison's Shred Run Program (Contact 703-805-1075 for more information). Shredded waste that is 1/4" by 1/2" or larger can still be recycled.

NOTE: For information on proper destruction or disposition of record FOUO documents, consult AR 25-400-2, Paragraphs 3-1, 4-4, 7-1, 7-2, and 7-4. For other documents considered exempt for the Freedom of Information Act (FOIA), including Privacy Act documents, consult AR 25-55, Paragraph 4-501.

Security Education Training and Awareness (SETA)

Fort Belvoir DPTMS, Security and Intelligence Division will host two Information Security Courses over the next few months. Contact the SETA Program Manager at 703-805-3058 for more details.



Additionally, there is online computer-based training available through the Defense Security Service Academy (DSSA). Go to https://enrol.dss.mil/enrol/lang-default/SYS_login.asp to login and enroll for excellent training opportunities.

According to AR 380-5, Paragraph 9-1, "Commanders will establish security education programs. These programs will be aimed at promoting quality performance of security responsibilities by command personnel, and will be tailored, as much as possible, to the specific involvement of individuals in the information security program and the command's mission." In order to accomplish the aim of security education programs, there are various types of briefings security managers need to develop for their organizations, including: initial orientation for both cleared and uncleared personnel, upon refusal to sign a Non Disclosure Agreement (NDA) SF 312, annual refresher, and foreign travel (in conjunction with AR 525-13).

Operations Security (OPSEC)

One of the most important individual responsibilities in OPSEC is understanding how to recognize suspicious attempts by unauthorized individuals to elicit information. According to a recent advisory from US Army North (ARNORTH), there have been a number of reported incidents involving email solicitations of US Service Members and Family Members as well as social networking intrusions soliciting personal information.

Information suggests criminal elements, extremists and terrorists will use the Internet social networks, email solicitation and other cyber-related venues to gain personal and military related information on US forces and their family members. US Military personal and family members must be aware of operations security (OPSEC) concerns when posting pictures, messages or when identifying themselves as a military employee.

There is a multitude of vulnerabilities that could be used by terrorist organizations, extremists or criminal elements to exploit US Military Personnel, family members or DOD Civilians. There is cause to be concern that these elements are actively engaged in this type of activity, which has been reported through law enforcement and intelligence channels.

NOTE: To report suspicious activity, contact Fort Belvoir Directorate of Emergency Services (DES) at 703-806-3105/3106. To report elicitation attempts, contact the 902d National Capital Region Field Office at 703-805-3008, or 1-800-CALL-SPY.

Industrial Security

Security of classified contracts performed on Army Installations.

According to AR 380-49, Industrial Security Program, the Installation Commander will provide for the security of classified contracts performed on the installation. Exceptions are when:

- The contractor activity has been designated a contractor facility.
- The Installation Commander has elected not to perform the security functions listed in paragraph 1–108b of the DOD 5220.22–R, the Industrial Security Regulation (ISR).

The installation commander continues to retain overall responsibility for the security of the installation. Specific installation security requirements will be included in contracts, as applicable.

Fort Belvoir Supplement to AR 380-49 provides specific procedural guidance to Defense Contractors supporting Fort Belvoir and Tenants.

Security Compromise/suspected compromise:

- The Installation Security Manager (ISM) will be notified during normal duty hours at (703) 805-4012/2416/5262 in the event of an actual or suspected security compromise. During non-duty hours, or during emergencies, the ISM must be contacted through the Installation Operations Center (IOC) at (703) 805-4002.

Security Investigation:

- Preliminary investigation reports involving an actual/suspected security compromise will be staffed by the organization Security Manager (SM) IAW the guidance contained in DoD, DA, IMCOM, NERO directives and this regulation. The SM will copy furnish the ISM all correspondence, notifications and reports pertinent to violations, compromises, or suspected compromise investigations.

DD Forms 254:

- Garrison and Tenant organizations with classified contracts will provide copies of all Department of Defense Forms 254 (DD 254s), including changes, to the ISM.

Foreign Representative Program

As a reminder, organizations with an approved Department of Army Foreign Visit Request (see AR 380-10) needs to coordinate installation access validation through the Installation Security Office at 703-805-5262 or 703-805-2416. For more information, review FB Reg. 380-10 at <http://www.doim.belvoir.army.mil/pubs/Belvoir/Reg/380-10.pdf>.

Personnel Security

Derogatory Information and Security Clearances—What do I do?

Army Regulation 380-67, Chapter 8 provides guidance on handling unfavorable administrative actions as they pertain to Personnel Security. One of the key tools to support these actions is the process of reporting unfavorable information. Paragraph 8-101b(1) of AR 380-67 requires Commanders to immediately notify CCF when credible derogatory information about a subordinate Soldier or Civilian employee is discovered. Years ago, prior to the use of the Joint Personnel Adjudication System (JPAS), this process was accomplished by forwarding a DA Form 5248 to Army Central Clearance Facility (CCF).

Today, Personnel Security specialists are equipped with electronic “Incident Reports” in JPAS. Initial reports will be submitted in a timely manner, indicating details of the credible derogatory information and actions to be taken to resolve the incident. Follow-up reports will be submitted every 90 days until a final action has occurred; final reports will be submitted along with the findings of any inquiries or investigations, and a recommendation by the command concerning the restoration or revocation of the individual’s security clearance.

The only instance when DA 5248 will be used in lieu of electronic notification, is when a “No Person Record” is discovered in JPAS. When submitting supporting documentation to a JPAS “Incident Report,” send by Fax at 301-677-2706 (DSN 622-2706), or email the documents to incidentreport@ccf1.ftmeade.army.mil.

NOTE: According to AR 380-67, Paragraph I-4b, spillages of classified information on to the unclassified domain **could** be a disqualifying adjudication factor. Instances of this activity should be reported to CCF as a “Security Violation” reportable incident in JPAS.

Investigations

The Office of Personnel Management (OPM) released an updated manual for Requesting OPM Personnel Investigations in July 2008, available at: <http://www.opm.gov/extra/investigate/IS-15.pdf>.

Page 6 of the manual provides information on the specific forms required to request an investigation, depending on the individual’s status and the sensitivity of the position.

The Fort Belvoir PERSEC Office assists Garrison and supported tenant personnel with any of these forms or requests, and processes the following investigation types: *National Agency Check and Inquiries (NACI)*, *Child Care NACI (CNACI)* for public trust and non-sensitive positions of new employees and contractors, *National Agency Check with Law and Credit (NACLIC)* for active duty military personnel in national security and sensitive positions, and periodic reviews for military and civilians, *Access NACI (ANACI)* for new federal employees requiring a Secret clearance, and *Single Scope Background Investigations (SSBI)* for military or civilians requiring a Top Secret clearance. For up to date information, contact the PERSEC office.

JPAS Information

Joint Personnel Adjudication System (JPAS) Access

If you are a security manager that is responsible for your organization’s personnel security, and you do not have a current JPAS account, contact the Personnel Security Office at 805-2952 or 805-4006.