



Fort Belvoir Security Newsletter

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



January-March 2009, 2d QTR FY09

Newsletter Contents

Installation Security Manager's Message	1
Security and Intelligence Division	2
Information Security	3
Security Education Training and Awareness	4
Industrial Security and Foreign Representatives	5
Personnel Security	6
Operations Security	7

Upcoming Events

10 February: INFOSEC Annual Refresher

11 February: OPSEC Annual Refresher

9-20 March: Security Specialist Course

TBD: Security Manager's Meeting

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 Newsletter readers,

I hope you enjoyed our inaugural Fort Belvoir Security Newsletter (October 2008). This edition focuses on some key information concerning the security disciplines supported by the Fort Belvoir Security and Intelligence Division. You will find some useful information on reproducing classified material, upcoming training opportunities and security awareness products, recent news on industrial security, and other information about personnel security program and operations security.

If you are a security manager, we look forward to seeing you at our next Security Manager's Meeting. We'll send out the final date, time, and location soon.

I hope you enjoy the newsletter this quarter, and if you have any comments or feedback, please share it.

Make Security Awareness a part of your day-to-day operations! Thank you.

Margie Ritchie

Installation Security Manager

Check out the Information Security section (Page 3) for information on **Department of Army Intelligence and Security Programs Oversight and Management (DAISPOM)**.



**DEPARTMENT OF THE ARMY
INTELLIGENCE AND SECURITY PROGRAMS
OVERSIGHT AND MANAGEMENT**

Protecting the Nation and Preserving its Spirit



Or go on the web at <https://daispom-odcsint.us.army.mil/index.asp>.

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: franklin.c.barrett@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 a security container requiring locksmith service to open it, please notify our office so that we can help identify and support any security requirements for the material inside.

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.

In the future, the Fort Belvoir population will see a new focus on Security Education Training and Awareness. We are presently preparing for an upcoming higher headquarters assessment from the Installation Management Command (IMCOM). Details will be provided to applicable security managers across the installation.

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 Program (SETA) Manager at 805-3058, or 805-5243.

Staff

Installation Security Manager: Margie Ritchie, 703-805-4012

Lead Information Security: John Davis, 703-805-2416

Information Security Program Manager: Dargely Maxwell, 703-805-5243

Information Security Specialist: Franklin Barrett, 703-805-2613

SETA Program Manager: Glenn Betha, 703-805-3058

**Industrial Security and Foreign Representative Program Manager:
Richard Cautle, 703-805-2817**

Fax: 703-805-4010

Lead Personnel Security: Michael Anderson, 703-805-2952

Personnel Security Specialist: Najam Gul, 703-805-4006

Personnel Security Specialist: Balena Lloyd, 703-805-3515

Personnel Security Specialist: John Ridley, 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

★ Give access to classified material only to people with appropriate clearance and need-to-know

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.

INFOSEC Tip: When reproducing classified documents, keep the following rules in mind:

- Use machines for which classified reproduction has been authorized and so designated
- Ensure latent images will not cause compromise
- Limitations, safeguarding and control procedures that apply to the originals must also be applied to the copies



- Always check the copier to ensure no classified originals or copies are left in it
- Place poor copies in an authorized container and destroy them as soon as possible. Merely placing the poor copies in a burn bag will not suffice.
- *Contractors:* Obtain authorization from the contracting activity for Top Secret unless specified in the contract. Maintain a record of reproduced Top Secret (2 years).

Department of Army Intelligence and Security Programs Oversight and Management (DAISPOM)

Mission: DAISPOM supports Army security professionals (military, civilian and government contractors) who desire knowledge of Army security programs, policies, reports, databases, related products and services.

Functions:

- Promote security products and initiatives to enhance the Army security posture
- Serve as a clearinghouse, disseminating security products and information Army-wide, and facilitate product integration into Army security programs
- Act as office of primary responsibility for Army DAISPOM products and information
- Represent the DCS, G-2, as the Army representative to DoD, National, other Agency, and Services security forums and meetings
- Identify and develop Army DAISPOM products to satisfy Army security awareness and training requirements
- Identify Army security program shortfalls and develop appropriate material to help alleviate the shortfall
- Assist Army components in developing and/or conducting DAISPOM activities

Security Education Training and Awareness (SETA)

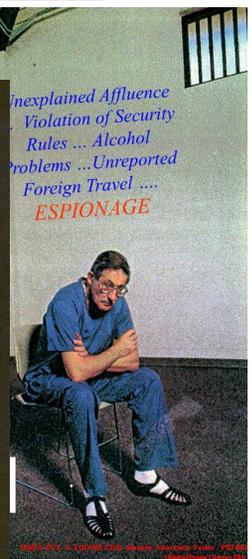
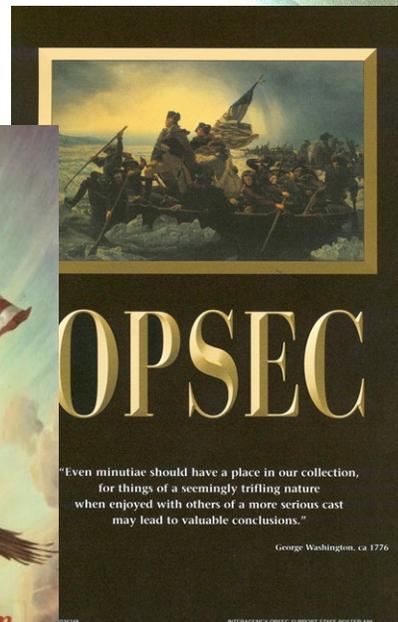
SETA Tip: Establish an effective security education program. If your security education program consists of an abbreviated initial security briefing and one hastily put-together annual refresher briefing, you are sending employees a signal: that you do not care about security. The true metric for measuring the effectiveness of your security education program is how well the employees understand security procedures and their responsibilities. (JPW Security Newsletter, Dec 08)



Fort Belvoir DPTMS, Security and Intelligence Division will host the DSS Academy Security Specialist Course, 9-20 March 2009. Slots are still available, but this course will fill up fast. Go to https://enrol.dss.mil/enrol/lang-default/SYS_login.asp to Login and



enroll for this excellent training opportunity. Contact the SETA Program Manager at 703-805-3058 for more details. *Note:* There are online computer-based training prerequisites for this course. If you're interested, don't hesitate!. Registration will fill up quickly and the prerequisites must be completed before a student is officially enrolled.



For Security Awareness products like these, check out the following websites:
<https://daispom-odcsint.us.army.mil/posters.asp>,
and <https://www.ioass-catalog.org/apps/ioass.dll/ioass/demand/home.do>

Industrial Security

NISP

THE NATIONAL INDUSTRIAL
SECURITY PROGRAM

“Working Together to Protect
Classified Information and Preserve our
Nation’s Economic and Technological
Interests.”



Reminder from Defense Security Service – National Industrial Security Policy Operating Manual (NISPOM) Changed Condition Reporting Requirements and Financial Distress:

Cleared contractors are reminded that their classified security programs are governed by the NISPOM, including the reporting requirements found in NISPOM paragraph 1-302g regarding changed conditions affecting the facility clearance.

Financial distress can lead to a number of conditions subject to reporting. NISPOM paragraph 1-302g(4) requires reporting of actions to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the facility clearance. DSS recommends contractors notify their Industrial Security Representatives prior to taking any of these or other reportable changed condition actions.

In the event the contractor has a reduction or realignment of personnel, cleared employees must be properly debriefed. Contractors should take proactive measures to ensure proper out-processing procedures are in place, classified information is accounted for and customer notifications are completed in a timely manner.

If you have any questions regarding this posting, please contact your DSS Industrial Security Representative or your local DSS Field Office.

Defense Security Service, January 7, 2009

https://www.dss.mil/GW/ShowBinary/DSS/special_alerts/specialalert122308.html

For a briefing on completing a DD Form 254, which is used to convey security classification guidance and advises cleared defense contractors on handling procedures for classified materials received or generated, go to:

<https://daispom-odcsint.us.army.mil/pub/dd254.ppt>

Check out www.asisonline.org for information on the next American Society for Industrial Security (ASIS) International Annual Seminar (21-24 September 2009, Anaheim CA).



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 703-805-2817 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

Chapter 9 of AR 380-67, Personnel Security (PERSEC) Program, covers the continuing security responsibilities of managers, supervisors, and individuals. Paragraph 9-103b speaks to the responsibilities of individuals with access to classified information promptly reporting the following to their security office:

- Any form of contact, intentional or otherwise, with a citizen of a designated country (AR 380-67, App H) unless occurring as a function of one's official duties
- Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation
- Attempts by representatives or citizens of foreign countries to: cultivate a friendship to the extent of placing one under obligation that they would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value; obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact; coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country
- All personal foreign travel in advance
- Any information of the type referred to in AR 380-67, Paragraph 2-200 or Appendix I

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.

OPSEC

**80% of
information used
by our adversaries
is derived from
open sources**

OPSEC Supporting Organizations

*1st Information Operations Command
Operations Security (OPSEC) Support Element (OSE)*
(<https://opsec.1stiocmd.army.mil>)

Interagency OPSEC Support Staff (IOSS)
(www.ioass.gov)

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

As you know, OPSEC is a five-step analytic process designed to develop measures in order to deny our adversaries the information they need to affect our operations and activities. All Army and DoD personnel have OPSEC responsibilities. One of the most important aspects of OPSEC is understanding the threat: that is, who are our adversaries and what are their capabilities to collect information about us. The diagram below highlights general threats to any operation.

As a member of the military community, you must be familiar with how the major OPSEC threats (circled in red) can exploit our critical information and how your organization's OPSEC program mitigates the threat. If you have official OPSEC duties, remember how vital your role is protecting the force; but everyone must make OPSEC a priority.



In the early days of the Vietnam War, the US lost an alarming number of pilots and aircraft. To reverse that trend, a team was assigned to analyze US military operations. The team, "Purple Dragon," discovered that crucial planning information was being disclosed through routine patterns of behavior. Countermeasures were quickly initiated.

Purple Dragon's analytic process, called **Operations SECURITY** or **OPSEC**, was used by the military for the next 20 years. In 1988, President Reagan formalized its use throughout the government and created the IOSS to provide training and guidance to the national security community. (www.ioass.gov)

Why is it important that we learn about OPSEC?

The information that is often used against us is not classified information; it is information that is openly available to anyone who knows where to look and what to ask.

OPSEC is a tool that our adversaries believe in...and one that we in the US Government need to understand and integrate into our daily routines. Our work is information, and not all of it is classified. What we don't always realize is how much we are giving away by our predictable behavior, casual conversations, routine acquisitions and other internet information. We must be careful of what we are revealing—failure to do so could provide our adversaries with the information they need to execute additional terrorist acts. (www.ioass.gov/bulletin.html)



**2009 National OPSEC
Conference
11-15 May 2009
San Antonio, TX
(www.ioass.gov)**