

OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

What You Need to Know

- Training Agenda
- Primary Mission
- Requirement
- What OPSEC is
- What OPSEC is not
- OPSEC Transformation
- OPSEC Compromises
- Your Responsibilities
- References

Bottom Line:

Practicing good OPSEC contributes to LEAD mission success.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

Letterkenny Mission / Vision

Mission:

The Letterkenny Army Depot, One team, serving the Community wherever they live, work, or play by providing sustainable base operations support, quality of life programs, and environmental stewardship to facilitate the sustainment of vital national interests.

Vision:

To build a compassionate, people valued, sustainable Letterkenny Army Depot Community through open communication, team work, partnerships and the delivery of outcome based services. "One Team, One Mission"

Letterkenny Army Depot Requirement

To ensure LEAD Operations Security (OPSEC) program is in compliance with AR 530-1 all DOD contractors are required to complete mandatory OPSEC training on an annual basis



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

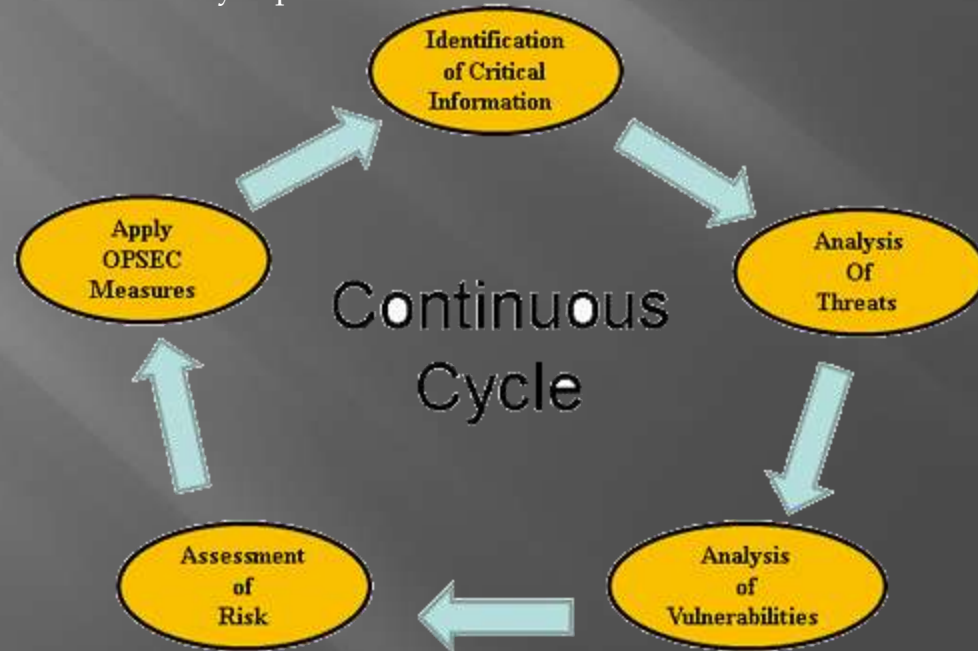
What is OPSEC?

OPSEC is the process of analyzing friendly actions attendant to military operations and other activities to:

Identify those actions that can be observed by adversary intelligence systems.

Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive Critical Information in time to be useful to adversaries.

Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

OPSEC Misconceptions

OPSEC is not:

- An Intelligence (G-2) function
- How to mark, handle, store classified documents
- How to handle computer hardware and software
- How to classify or declassify information
- How to transfer information from SIPR to NIPR
- How to manage General Officer itineraries / travel
- How to properly lock up your office at night
- How to configure computer networks
- How to conduct classified briefings in hotels

Not a valid excuse:

- "But it's already out in open source, why can't I use it?"
- "But I'm not over in Iraq or Afghanistan, why does it matter?"
- "Why would anybody be interested in what I'm doing?"



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

15 Years Ago:

Leadership Controlled Information

- Information flow S L O W
- Leadership controlled
- Workforce/Troop access restricted
- Document access restricted
- Distribution controlled (paper)

Today:

Individuals Control Information

- Information flow FAST
- Individually controlled
- Workforce/Troops easily accessible
- Documents easily accessible
- Unlimited/uncontrolled distribution



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

OPSEC Challenges

- Human Nature
 - Natural instinct to take short-cuts
 - Natural instinct to "help" others
 - Natural instinct to "impress"
- Lack of training and situational awareness
- Technology (computers, cell phones, PDAs, wireless, thumb drives...)
- Blogs, personal websites, private email (Hotmail)
- Photographs on the Internet
- Media



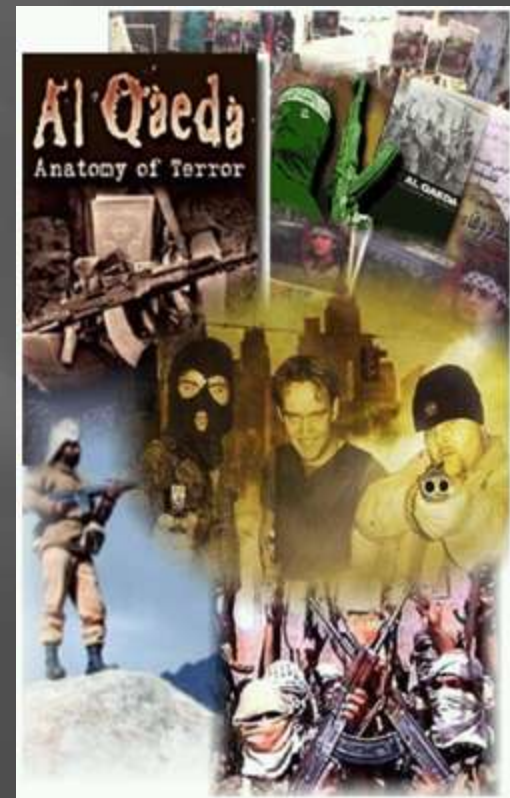
OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

What do Adversaries Want?

They are looking for:

- Names / photographs
- TTPs, equipment vulnerabilities
- Present and future capabilities
- Insights into national / military morale
- Meetings of top officials / diplomatic efforts
- Important government places
- Information about military facilities:
 - Location
 - Units
 - Weapons used
 - Fortifications & tunnels
 - Amount of lighting
 - Exterior size and shape
 - Number of personnel
 - Ammunition depot locations
 - Leave policies
 - Brigades and names of companies
 - Degree & speed of mobilization



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

OPSEC Guidance

KEY POINTS

- OPSEC is a chain of command responsibility
- It is serious business and we must do a better job across the Army
- The enemy aggressively 'reads' our open source information and continues to exploit such information for use against our forces
- Such OPSEC violations needlessly place lives at risk and degrade the effectiveness of our operations

Jihadi Information Battalion orders members to practice OPSEC

- Stop communicating with one another by email entirely and instead use the JIB web-forum
- Only use public computers that cannot be linked to them
- Use anonymous IP address websites to mask their identity while navigating
- Do not publish any of their identifying information in online forum registrations or posts



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

Social Networking

Social Networking Sites (SNS) allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

Revised Statement of Rights & Responsibilities

- "You own all of the content & information you post."
- "You specifically give us the following permission, subject to your privacy and application settings, to use any content that you post on or in connection with Facebook."
 - Non-exclusive
 - Transferable
 - Sub-licensable
 - Royalty-free
 - Worldwide license
- "We may collect information about you from other users."
- "Sometimes we share aggregated information with third parties."



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

Personally

- Entertaining
- Maintain Relationships
- Network
- Centralized information

Professionally

- Marketing/recruiting
- Public Relations
- Connect with customers
- Solicit ideas and feedback

The Danger

Bad guys use it too.

- Stalkers
- Thieves
- Terrorist
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on...

Al-Qaeda communique December 2009:

"The affair with the U.S. Navy began several years ago, when the lions of Al-Qaeda struck the destroyer U.S.S. Cole, in Yemen; now, with Allah's help, all the American vessels in the seas and oceans, including aircraft carriers, submarines, and all naval military equipment deployed here and there that is within range of Al-Qaeda's fire, will be destroyed...

"To this end, information on every U.S. naval unit — and only U.S. [units]!! — should be quietly gathered [as follows:] [the vessel's] name, the missions it is assigned; its current location, including notation of the spot in accordance with international maritime standards; the advantages of this naval unit; the number of U.S. troops on board, including if possible their ranks, and what state they are from, their family situation, and where their family members (wife and children) live; what kind of weapons they carry; the [vessel's] destination...; which naval units are closest to Islamic countries; which naval units are close to Western countries in general; searching all naval websites in order to gather as much information as possible, and translating it into Arabic; search for the easiest ways of striking these ships...

"My Muslim brothers, do not underestimate the importance of any piece of information, as simple as it may seem; the mujahedeen, the lions of monotheism, may be able to use it in ways that have not occurred to you."



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

Social Networking Websites and Your Security Clearance

The following is a security awareness statement signed by the Chief of Security, Pentagon Chief Information Officer, OSD Network Directorate:

"Social sites risk security clearance. If you hold a security clearance or if you ever want to apply for one, be mindful of your postings and contacts online, particularly on social networking sites such as Facebook and Twitter. These sites pose risks to gaining and keeping a security clearance. **Question 14 of the National Agency Questionnaire (SF-86) asks for names of your relatives and associates. The term associate is defined as any foreign national that you or your spouse are bound by affection, obligation, or close and continuing contact.**



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



Do: Remember Computer Security

Do not be an easy target for computer crimes

Hacking

- Theft
- Planted code vs.
- Antivirus software
- Firewalls
- Strong Passwords
- Permission Settings



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



Do: Verify All Friend Requests

Social engineering and "conning" starts with a friend request

Adversaries can get the data from:

- Free people search engines
- Other SNS's
- Your posts/profile
- Your friends posts/profile

Verify Requests Before Approving!

Do not trust who you cannot see and verify. It is not hard to establish accounts and to fake information to target people.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



Do: Utilize All Available Privacy Settings

Customize available settings to be
as secure as possible

- "Everyone" may be accessed by anyone with access to the internet
- How many security settings are available on Facebook?

Over 120



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

Do: Watch Your Friends Settings

Sure your profile is secure, but what about your 115 friends profile settings?

All the privacy settings in the world mean nothing if someone in your network of friends does not have any privacy settings. Be careful of what you and your friends post and make available to the world.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



Do: Closely Monitor Your Children's Use of the Internet

- Cyber-bulling
- Kidnapping
- "Sexting"
- Stalking
- Pedophiles

- 500,000+ registered sex Offenders in the USA
- 95,000 registered sex offenders profiles on Myspace

Children are especially vulnerable on the internet and make easy targets. Monitor closely children's use the internet to insure they are not posting critical and personal information.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



of Social Networking

Do: Verify Links & Files Before Executing

Would you follow a link in e-mail? Would you download and run an attachment?
Then why do you do these things on SNS's?

- Phishing scams
- It is serious business and we must do a better job across the Army
- Malicious coding
- Viruses
- Scareware

Verify before executing!

The same threats that exist in your inbox exist in social networking sites and any download. Verify links and websites before accessing and executing.

Do not follow links provided in emails, go through a trusted link that you know to be good. Call your bank and verify that the information they are requesting or sending is legitimate. Often times a bank will not contact you via email for account changes.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



Do: Blog with Caution

- Avoid details, don't get personal
- Who is reading your blog?
- Lessons learned 101 for the adversary

Blogs, and the internet in general are a great source for information. People tend to post the most intimate details about themselves in a typically completely unsecure, wide open public forum. This is horrible OPSEC. Lessons learned 101 for the bad guy is as simple as goggling IED damage to vehicles. The above battle damage assessment photos were pulled right off .mil sites. What can the adversary learn just by studying these photos? What do these images tell the adversary about the effectiveness of their attacks?

Military spouse blogs are a great way to learn all kinds of information, including the kids ages, names, school district, deployment schedules, duty days, smoking/eating habits and on and on – too many details.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



of Social
Networking

Do: Understand the Risks Associated with Geotagging

Location/GPS data attached to photos

Feature in Smartphones and digital cameras

Lat/Long

Device details

"Check-in" feature

Facebook Places

Google Latitude

Foursquare

Gowalla

Geotagging on social networking sites is increasing in popularity. From virtual check-in's to simply uploading photos with geographical information included in the data, users are posting detailed physical location data online for the world to see. The technology for geotagging now comes standard on newer digital camera's and smartphones, and is easily extracted with a simple software package that can be downloaded free in many cases.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



of Social Networking

Do: Be an Informed User of a SNS

- How much personal information do you broadcast?
- Are you very careful about what details you post?
- Do you understand data aggregation issues?
- Are you willing to find and learn all the security settings and keep up with them as they change?



Are you willing to accept the risk?

Be an informed user. Know the terms of use, the changes to the site, and all of the different settings that are available. Make your site as secure as possible, understand that data collection is the job of many – from marketing campaigns to adversaries. Regardless of settings, never post details – details make you vulnerable.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



Do: Have a Contingency Plan

- KIA, MIA, POW
- What details will the adversary have to use against you?
- What information will the media have access to?
- Power of Attorney
- Memorial pages

In the event of death or capture have a power of attorney in place to allow family members to delete or change your social networking profile. Protect your personal details from the media and adversaries.



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors



of Social
Networking

Do: Assume the Internet is FOREVER

- There is no true delete on the internet
- WWW means World Wide Web
- Every Picture
- Every Post
- Every Detail

FOREVER!



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

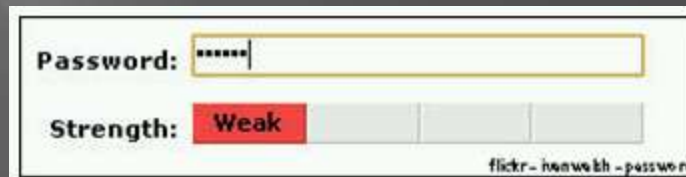


Don't: Use the Same Passwords

- Hackers count on users using the same passwords for multiple accounts
- Password1 is not a strong password

Password strength is key to protecting yourself on the internet.

The average user has over 15 accounts and 4 different passwords. Do not use the same password for every account, that is an easy way to be taken advantage of.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



Don't: Depend on SNS's Security Settings

But it's set to private ... right?

Hackers

Incorrect or incomplete settings

Sale of data

Upgrades/site changes

"Risks inherent in sharing information"

"USE AT YOUR OWN RISK. We do not guarantee that only authorized persons will view your information."

Never forget — the true purpose of a SNS from the creators POV is data aggregation for profit



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



Do's

Don'ts

of Social Networking



Don't: Trust Add-On's or Applications

Plugins, Games, Applications

Third Party Software

Applications designed to collect data

Malicious code

Separate terms of use & privacy

"We are not responsible for third party circumvention of any privacy settings or security measures."

Add-on's and applications are third party software. This includes games like farmville, mafia wars etc.

These applications have their own terms of use and often do not comply with the privacy settings of the host website.

Facebook stats:

"We are not responsible for third party circumvention of any privacy settings or security measures."

Every month more than 70% of Facebook users use a platform application

More than 500,000 active applications currently on Facebook platform

More than 250 applications have more than 1 million monthly active users

Facebook Platform: "A standards-based web service with methods for accessing and contributing Facebook data... Making the web more social!"

Facebook Platform: "We do not own or run the applications and websites that you interact with through Facebook Platform, and while we try to enforce standards to protect your information, we cannot guarantee that they will follow our rules.:"



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



of Social Networking

Don't: Grant the Same Access to Everyone

Don't treat all Friends equally

Control & customize individual access

Do create groups

- Poker club
- Family

Set permissions for everything:

- Your status
- Photos
- Postings

Permissions and groups are available to further customize permissions and restrict access.

Not everyone in your friends list is your "best friend", restrict the amount of data that everyone in your network is able to access.

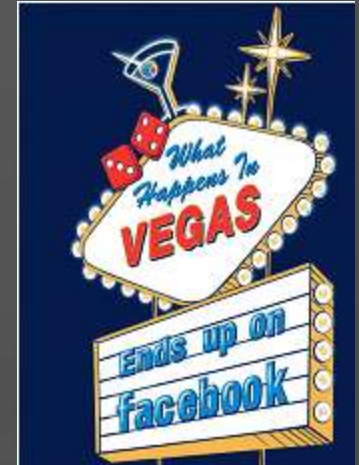


OPSEC TRAINING

FY 2012 OPSEC Training for Contractors



of Social Networking



Don't: Discuss Details

Never post anything you would not tell directly to the enemy

Never post private or personal information- no matter how secure you think your settings are

Assume the information you share will be made public

Details make you vulnerable

Don't discuss or post details regardless of security settings. There is no truly secure computer with access to the internet- keep that thought in mind at all times and keep details to yourself.



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

Your Responsibilities

- Know your organization's sensitive information
- Be aware of the sensitive information to which you have personal access and how to protect it
- Implement OPSEC measures as determined by your OPSEC Officer
- Actively encourage others to protect sensitive information
- Do not disseminate information without proper authorization (chain of command, OPSEC review, ...)
- Use secure communications whenever possible (CAC encryption)
- Stay in your lane
- If in doubt — stop and ask someone



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

Conclusion

Safeguarding our sensitive information is vital to success

- The threat is real
- What you do matters

"You can't measure your worth and your importance by your proximity to the battlefield."
General Cody

SO WHAT FACTOR:

- Compromise of Critical Information
- Free Intelligence to the Adversary
- Not retrievable when Send Button is touched
- Can be manipulated and exploited by anyone who has reason or cause
- Impact on mission that may be detrimental



OPSEC TRAINING

FY 2012 OPSEC Training for Contractors

References

DoD Directive 5205.2 dated 06 March 2006

AR 530-1 (Operations Security) dated 19 April 2007

FM 3-13 (Information Operations) dated 28 November 2003

Army OPSEC Support Element - <https://opsec.1stiocmd.army.mil> (Requires AKO user ID and password)

Interagency OPSEC Support Staff - www.iooss.gov

G-2: AR 380-5 (Information Security) dated 29 September 2000

G-6: AR 25-2 (Information Assurance) dated 24 October 2007



Points of Contact

Mail:

OPSEC Officer:

LTC Robert Leasure

(717)267-8260

robert.k.leasure.mil@mail.mil

Alternate:

Charles L. Jenkins

(717)267-9484

charles.l.jenkins3.civ@mail.mil



OPSEC TRAINING

FY 2012 OPSEC Training
for Contractors

*Congratulations! You've completed the Letterkenny
Army Depot OPSEC Training for Contractors*

Get a Certificate - Print the Certificate from the next slide. Enter your name and date and present it to your supervisor.



OPSEC TRAINING

Certificate of Completion
Completed by

Name

Date

