The Purple Dragon

Volume 23 | Joint OPSEC Support Element (JOSE) | Summer 2012

From the Dragon's Mouth

Comments from the Chief, JIOWC OPSEC Support Division

Donald P. Taylor, Jr
COL, USA

Integrating OPSEC into AT/FP Programs

The risks of terrorists exploiting your unprotected critical information and those that are willing to do your command harm have not gone away. This is why it is crucial that Commanders and Antiterrorism Officers (ATOs) continue to integrate Operations Security (OPSEC) into their Antiterrorism and Force Protection (AT/FP) programs.

Recent events around the globe and stateside continue to remind us of the need to protect sensitive information. Many nations, organizations and nefarious individuals actively conduct operations against the United States and its Armed Forces. This is especially true of terrorist organizations. Collection can come from a variety of sources such as unencrypted e-mails, discussing privileged information on unsecure telephones or inadvertent disposal of sensitive information in the trash. Protection of AT/FP sensitive information is essential to overall mission assurance and to the success of the AT/FP program. Therefore, Commanders must continually assess their organizations' OPSEC posture to enhance the protection of US, Allied and coalition operations from an ever-evolving threat.

OPSEC helps reduce friendly force vulnerabilities, particularly adversary exploitation of critical information. OPSEC countermeasures are applicable across the entire range of military operations and activities, to include force protection planning and information sharing while in garrison or deployed around the world. One must think before he or she speaks, does the person I am speaking with "have the "need-to-know."

Continued on Page 2

Inside This Issue

Joint Information Operations Warfare Center
Joint OPSEC Support Element (JOSE)
2 Hall Blvd, Suite 217
San Antonio, TX 78243-7074

Editorial Staff – Email: jiowc.jose@us.af.mil

https://www.intelink.gov/sites/jiowc/Divisions/OS/default.aspx

http://www.facebook.com/JIOWC.OPSEC.Support

Chief – Donald P. Taylor, Jr., COL, USA
Deputy – Lee Oliver, DAFC

Continued from page 1

It's a known fact that when Commanders and ATOs integrate OPSEC into their force protection programs and effectively apply its use, they can deter, discourage, dissuade and deny an adversary sensitive critical information, thereby disrupting their collection efforts.

This is why Commander's, ATOs and personnel supporting AT/FP programs must be actively engaged in protecting unclassified sensitive AT/FP information, such as antiterrorism working group meeting minutes, random antiterrorism measures, security measures, maps, diagrams, layouts, photos, after action reports, known vulnerabilities, "For Official Use Only" information or information found on their higher headquarters or command's critical information list.

How do ATOs protect sensitive information they work with on a day-to-day basis? Quite simply, they must incorporate sound OPSEC principles and counter- measures into their overall antiterrorism and force protection programs. The integration of OPSEC into antiterrorism planning and execution addresses potential risks to operations and mission effectiveness.

Integrating OPSEC into AT/FP programs ensures personnel and mission critical assets are protected from potential threats. When OPSEC is integrated into a command's antiterrorism program and force protection program, the command is postured to execute effective OPSEC measures and mitigate the risk of inadvertent critical information disclosures.

Here are some questions Commanders and ATOs should ask themselves to determine if OPSEC is adequately integrated into their AT/FP programs:

- Does the ATO and the command OPSEC representative work together to protect sensitive information?
- Has an OPSEC annex been included in the antiterrorism plan?
- Does the antiterrorism plan allow for coordination with the installation and command OPSEC Program Manager?
  Has the command developed a critical information list to facilitate and focus efforts to deny information to adversaries?
    - Is AT/FP information incorporated into this list?
- Are command and higher headquarters critical information lists distributed to all personnel responsible for supporting AT/FP program (civilian, military and contractors)?
- Has the antiterrorism plan identified the threat and techniques an adversary may use to collect information?
- Have OPSEC countermeasures been established to prevent an adversary from readily obtaining critical information (e.g., proper disposal of paper documents through the use of crosscut shredders or burn bags and encrypting AT/FP sensitive unclassified emails)?
- Is the ATO using encryption or other counter measures to protect electronically transmitted e-mails?

The key to protecting people and resources is to deny our adversaries the ability to collect and exploit our critical information. Incorporating OPSEC into a command's AT/FP program will greatly enhance the program's effectiveness; Of course, you can't just go through the motions and check the block. ATO's must work closely with the command OPSEC representative to have a successful program. Remember OPSEC is a mindset and leaders must educate and re-educate their subordinates on a continuious basis.

Like US on Facebook!
facebook.com/JIOWC.OPSEC.Support

HOW TO RECOVER
YOUR OLD E-MAIL ENCRYPTION KEYS

Encrypted e-mails  received can only be opened with your private encryption key. When your CAC is replaced, previously encrypted e-mails can only be opened using the previous CAC encryption certificates.

"Key Recovery" is a process that allows the recovery of the certificate/key that was held before getting a new CAC/certificate. Old keys can be recovered at:

https://ara-1.c3pki.chamb.disa.mil/ara/Key

https://ara-2.c3pki.den.disa.mil/ara/Key

2012 National OPSEC Conference

The more things change, the more they stay the same. This old adage may hold true to many things, but certainly not when it came to the 2012 National OPSEC Conference (NOC). Held this year at the Anaheim Marriot Convention Center in sunny Southern California, the NOC brought together an ever-growing number of OPSEC professionals. OPSEC Program Managers (OPMs), Anti-Terrorism Officers, and Command Security Officers from the Defense Department's Combatant Commands, Uniformed Services and other Departments to include Homeland Security were present. Moreover, security representatives from industry and academia, as well as federal, state and local law enforcement agencies participated in the conference.

This year's NOC held an even more special meaning to the Joint OPSEC Support Element (JOSE) as one of our very own, Mr. Lee Oliver, received the National Award for Individual Achievement by the National Security Agency's Interagency OPSEC Support Staff - National Awards Program.

The JOSE team also hosted many of the training sessions held throughout the week to include "Beyond the Three Ring Binder" hosted by Mr. Oliver, "Internet Based Capabilities" hosted by Mr. Troy Richardson, "OPSEC in Exercises" hosted by Mr. Anthony Maybrier, "OPSEC Planning Workshop" hosted by Mr. Carl Garbelotti and LTC Richard Millikan.

OPSEC support organizations distributed a wide array of awareness products to include handbooks, videos and posters. Many program managers relayed that the NOC provided them a chance to acquire OPSEC awareness items and, in turn, use them to enhance OPSEC at their organizations or inspire ideas to generate their own.

When asked what they felt was the most valuable aspect of the NOC, many attendees firmly felt that simply being immersed in the culture of OPSEC and attending a wide variety classes, training and focused discussions allowed many of them to develop a plan of action to raise their own programs to the next level.

Many program managers mentioned that in spite of their units facing ever-shrinking budgets and limited access to travel funds, the NOC continues to make their Commander's short list of "must attend" events highlighting the value and importance commanders place on OPSEC. Additionally, despite best intentions/efforts, many units were unable to dedicate funds to obtaining awareness products. The NOC provided those OPMs an opportunity to acquire free OPSEC awareness items for use in follow-on training at their units.

Joint OPSEC Support Element booth at the 2012 National OPSEC Conference

At the end of the day, active engagement amongst fellow OPSEC professionals exchanging best practices and lessons-learned was the most important aspect of the national conference. Next year's NOC location is yet to be determined, but the National OPSEC community looks forward to meeting once again to advance the protection and control of sensitive unclassified critical information.

UPCOMING OPSEC TRAINING

OPSEC Analysis and Public Release Decisions Course (OPSE-1500)

27 JULY 2012, CAMP ARIFJAN, KUWAIT

30 JUL 2012, CAMP CASEY, KOREA

20 AUG 2012, YOKOTA AB, JAPAN

20 AUG 2012, SAN ANTONIO, TEXAS

24 SEP 2012, GRAFENWOEHER, GERMANY

15 OCT 2012, CAMP HENRY, KOREA

15 OCT 2012, SAN ANTONIO, TEXAS

3 DEC 2012, SAN ANTONIO, TEXAS

This course addresses OPSEC issues that should be considered when reviewing information for public release and public access. Lessons can be applied to preparing information for release in all forms of media (e.g., print, web postings, and public speeches). After completing this course, the student will be able to: edit information to be posted, written and spoken by applying OPSEC principles and achieve the originator's objective without compromising critical information. This course is taught at the unclassified level.

This course is specifically designed for individuals involved in determining what information should be released to the public, such as public affairs officers, web masters, Freedom of Information Act review staff, speech writers, speakers, classification review personnel and OPSEC coordinators.

Prerequisite: None. However, (OPSE-1301) OPSEC Fundamentals course is recommended.

OPSEC Analysis and Program Management Course (OPSE-2500)

31 JUL – 3 AUG 2012, CAMP CASEY, KOREA

21-24 AUG 2012, SAN ANTONIO, TEXAS

21-24 AUG 2012, YOKOTA AB, JAPAN

25-28 SEP 2012, GRAFENWOEHER, GERMANY

16-19 OCT 2012, CAMP HENRY, KOREA

16-19 OCT 2012, SAN ANTONIO, TEXAS

4-7 DEC 2012, SAN ANTONIO, TEXAS

This course addresses the basic skills and knowledge needed to conduct an OPSEC risk analysis (apply the five steps) and to implement an OPSEC program. The student is afforded the opportunity to apply OPSEC tools and lessons through a variety of practical exercises and case studies. Upon completing this course, students will be able to:

(1) Apply the systems analysis methodology to their organizations and activities;
(2) Identify sources of information and support materials for OPSEC practitioners;
(3) Conduct an OPSEC analysis of their program, activity or operation;
(4) Market an OPSEC program;
(5) Develop an organizational OPSEC policy; and,
(6) Implement and manage an OPSEC program.

This course is designed for individuals performing in the roles of OPSEC Program Manager. This course is taught at the unclassified level.

Prerequisite: OPSEC Fundamentals (OPSE-1301) or equivalent

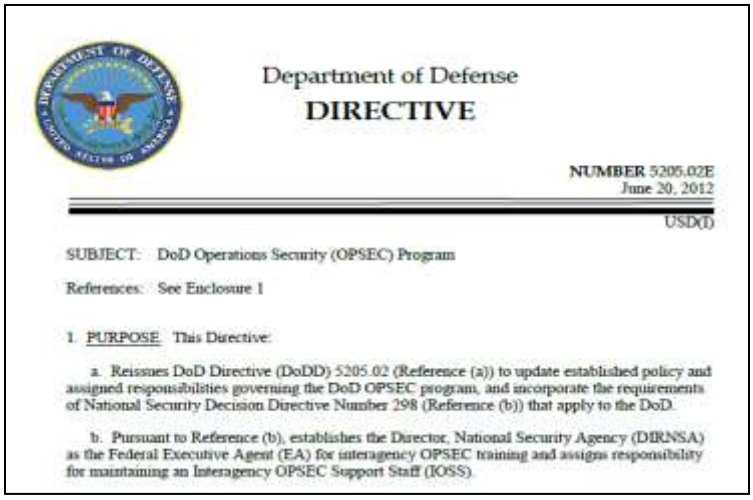
FOR COURSE REGISTRATION AND ADDITIONAL OPSEC COURSES GO TO:

HTTPS://WWW.IAD.GOV/IOSS/INDEX.CFM OR CONTACT THE JOSE AT: JIOWC.JOSE@US.AF.MIL

New DoD OPSEC Publications

New OPSEC publications have hit the street: CJCSI 3213.01D, *Joint Operations Security* dated 7 May 2012 and DODD 5205.02E, *DoD Operations Security (OPSEC) Program* dated 20 June 2012. Both documents can be found on NIPRNET at http://www.dtic.mil/cjcs_directives/cdata/unlimit/3213_01.pdf and http://www.dtic.mil/whs/directives/corres/pdf/520502e.pdf. The following is a summary of changes for CJCSI 3213.01D:

- Includes OPSEC considerations in contracting, in the review procedures prior to public release of information, and during Freedom of Information Act (FOIA) requests
- Broadens the scope of OPSEC training and expands the audience to include DoD family members and others
- Discusses the relationship between military deception (MILDEC) and OPSEC
- Provides guidance on social media, OPSEC enforcement, and funding for OPSEC programs
- Discusses the requirement for a full-time OPSEC program manager at the command level and expands the responsibilities
- Includes specific duties for the OPSEC planner
- Defines responsibilities for the Joint Information Operations Warfare Center (JIOWC); Commander, U.S. Special Operations Command; and all DoD Component personnel.
- Shifts joint OPSEC oversight responsibility from Commander, U.S. Strategic Command, to the Chairman of the Joint Chiefs of Staff
- Includes items for inclusion in critical information list



Department of Defense
DIRECTIVE

NUMBER 5205.02E
June 20, 2012
USD(I)

SUBJECT: DoD Operations Security (OPSEC) Program

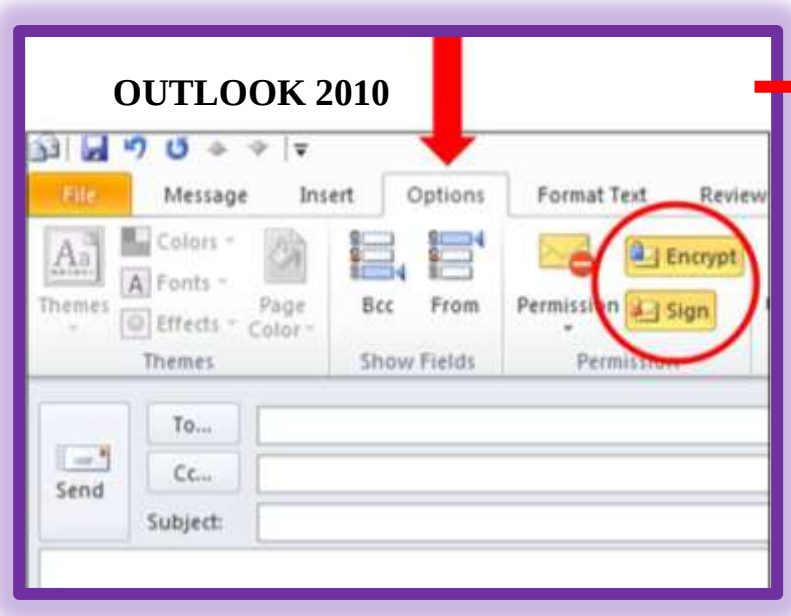
References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues DoD Directive (DoDD) 5205.02 (Reference (a)) to update established policy and assigned responsibilities governing the DoD OPSEC program, and incorporate the requirements of National Security Decision Directive Number 298 (Reference (b)) that apply to the DoD.

b. Pursuant to Reference (b), establishes the Director, National Security Agency (DIRNSA) as the Federal Executive Agent (EA) for interagency OPSEC training and assigns responsibility for maintaining an Interagency OPSEC Support Staff (IOSS).

E-MAIL ENCRYPTION TIP



In Microsoft Outlook 2010, the digital encryption icon does not show when a new e-mail is created. In order to see the icon for encryption, you must click the "Options" tab, then the "Encryption" button to encrypt an e-mail.

How to Protect Sensitive Information on FaceBook

1. Control Your Friend Lists. *Only establish and maintain connections with people you know and trust.*

- Go to the Friends Area of your Facebook
- Review your "Friend List"
- Configure your list according to your needs

2. Avoid Photo/Video Tags. *Avoid posting or tagging images of you or your family that clearly shows your face.*

- Go to the Profile Privacy Settings Page
- Click on "Edit Settings" for "How tags work" For "Profile Review", select "Enable" to turn on. This will create a manual review before any picture is posted to your profile. "Tag Review" creates a manual review for friends that tag your pictures before adding to their posts.
- Maximum Profile Visibility. For posts you are tagged in, recommend no higher setting than "friends", but you can customize to smaller select lists.
- For "Tag Suggestions", you have two choices: Friends or no one. If you have enabled manual reviews above, then setting is not a concern, but if you prefer never being tagged, then select "no one."
- For "Friends can check you into places", select "Disable" to turn off.

3. Protect Your Photo Albums.

- Go to your profile and click on your photos
- On **each** of your photo albums, set setting on "Only Friends" or customize (e.g. only me, individuals, etc…) to your desire

4. Stop Published Application Stories

- Go to Privacy settings
- Click on "Past Post Visibility" under "Limit the Audience for past posts". Click on "Limit Past posts". For future posts, select desired level of audience for each post.

5. Stop Embarrassing Wall Posts. *This is an individual risk assessment depending on your friends. Assume anyone can see your activities, personal life, or professional life that you post or share.*

- Go to Privacy settings
- Click on "Edit Settings" for "How you connect"
- Make selection next to "Who can post on your wall?" "Friends" or "Only me"

6. Keep Who Your Friends are Private

- Go to your profile page
- Mouse over top of friends list, a pencil icon should appear. Click on the pencil icon to edit family, friends list, and relationships
- Select "only me" and save changes

7. Remove Your Facebook Profile From Google & Other Search Engines

- Go to Privacy Settings
- Click on "edit settings" for "Apps and Websites"
- Click on "edit settings" for "Public Search"; uncheck enable public search

8. Remove from Facebook Search Results

- Go to Privacy Settings
- Click on "Edit Settings" for "How you connect"
- Next to "Who can look up your profile by name or contrast information" select "Friends"

9. Do not link to other SNS or 3rd party sites

- Do not share your information freely by using "Facebook Connect" that may aggregate your information

10. Do not post sensitive information about you, your family members, and friends on social networking sites.

- If you would not give the information to those that would do harm, don't post it for all to see.

Getting Serious About OPSEC

By LCDR Kurt Fischl
Joint OPSEC Support Element

After more than ten years of war, Operations Security should be a no-brainer for all of us. As war fighters, we are adapt at recognizing threats posed from various weapons such as missiles, torpedoes, IEDs and machine guns. Understanding their capabilities and limitations gives us the ability to develop and train countermeasures to defeat them. However, some continue to have trouble identifying and mitigating threats to our critical information. We continue to have OPSEC disclosures that put our service members, families and missions at risk. We must ask why this is. OPSEC is more than just a program in a binder that is dusted off and reviewed for your next inspection. It must be ingrained in our culture and practiced in all aspects of our operations in the same way that safety and maintenance is practiced. Would you operate your aircraft, ship or weapons system without reviewing your safety and maintenance procedures?

It should come as no surprise that there are people in this world that want to do us harm, either personally or as a nation. Whether it is the criminal threat that targets DoD personnel and our families for monetary gain, Foreign Intelligence Services that seek to gain strategic and operational advantages or terrorist organizations that want to kill us at home or abroad, we face a multi-facetted, sophisticated and ever-evolving threat. If we do not understand how these adversaries operate and the latest Tactics, Techniques, and Procedures they use, how can we have a successful OPSEC program?

Speaking of threats, if we do not stay abreast of the latest technology, especially in the rapidly expanding cyber domain, how can we identify all the vulnerabilities we may be susceptible to? Technology is changing at an extremely fast rate and our critical information can become vulnerable in unexpected ways. Is your command aware of the latest physical and cyber vulnerabilities? Terabytes of sensitive critical information can be at risk due to lax security procedures, bad business practices, or just plain ignorance. We must stop making it easy for the adversary.

How can you make OPSEC not "just another program"? It all starts with the commander. If the commander has "buy in" and makes OPSEC a command priority, the rest of the command will fall in line. As OPSEC professionals, we must be ready to make the case and convince our leadership that OPSEC is necessary. OPSEC has a proven track record and numerous historical examples are available to illustrate OPSEC at work. With command guidance and authority in hand, your OPSEC working group can develop, implement and assess countermeasures to mitigate vulnerabilities. Working groups should include elements from all parts of your organization. Your information assurance personnel, public affairs and contracting office should be part of the solution, as they're aware of what information is critical to the mission.

The good news is that you are not alone. The Joint OPSEC Support Element and individual service support elements are here to help. Whether you are conducting day-to-day "halls and walls" operations, operational planning/exercises, or conducting a tactical movement, OPSEC must be integrated from the beginning. While nothing can guarantee mission accomplishment in the face of a determined adversary, OPSEC can certainly help to mitigate vulnerabilities and greatly increase the likelihood of mission success by denying and frustrating the adversary.

Information Sharing Age

By Aja Bowser
Joint OPSEC Support Element

Why did the Encyclopedia Britannica halt print production? Better yet, when was the last time someone purchased a set? My guess is when Google became a verb. Technology has grown at such a rapid pace that it is becoming increasingly difficult to keep sensitive information under wraps.

The emergence of social media has made information sharing simple and user-friendly for anyone with access to the internet. The downside to this global phenomenon is individuals with malicious intentions can acquire sensitive information that "We" as DoD employees make readily available. It is known that adversaries actively collect emails that we send across the NIPRNET searching for bits of sensitive information which provide a picture of our operations. One effective way of protecting messages that are sent across the vast and seemingly endless internet is utilizing digital encryption, if employed properly…

There are usually two ends of the OPSEC encryption spectrum: OPSEC Program Managers (OPMs) who insist that personnel "Encrypt everything" or those who work in the "6 shop" (Communications/Electronics) who say "Don't encrypt, it takes up too much bandwidth." What is the solution? OPSEC SAYS: Encrypt emails that contain your sensitive unclassified information, which includes items from your Critical Information List (CIL). Think of an encrypted email as your own personal diary/journal which is kept under lock and key. Your nosey sibling, in this case the adversary, needs the key to unlock it if they want to read what you wrote. By locking down private thoughts, actions, and intentions (which could be potentially damaging to yourself or other people) you are practicing good OPSEC. If your sensitive information is left unencrypted, the adversary can potentially piece together a bigger story (even classified!) when combined with other available information, thus severely hampering mission effectiveness. This does not mean that the adversary can't glean information from you just because it's encrypted; it just makes them work a little harder.

The first line of defense in protecting government and personal sensitive critical information is YOU. The purpose of instructing personnel on email encryption is to prevent sensitive unclassified information from falling into the hands of the adversary. Understanding how to push the little "blue lock" is futile unless organizations recognize what information needs to be safeguarded. CIL training should be used in conjunction with email encryption instructions to raise awareness and increase mission effectiveness.

OPSEC instructions containing encryption:
--AFI 10-701. "Encryption serves as one measure to protect critical or sensitive information transmitted over unclassified networks. Encrypt all e-mail messages containing critical information, OPSEC indicators, and other sensitive information."
--AR-530-1. "When an Encryption feature is available on unclassified networks, encrypt e-mail messages containing sensitive information. Encryption serves as an OPSEC measure to protect sensitive information transmitted over unclassified networks."

So while encyclopedias may have gone the way of the dinosaur, your online presence and what you say online (posts or emails) will be there forever more. Be vigilant in protecting your information!

Adversary's Corner

I would like to thank you for making my job so easy! Social networking sites such as Facebook and Twitter have such a plethora of both personal and professional information from the United States military. Please, continue to post pictures of yourself trying to look important at work especially the ones while you are deployed. You and your "friends" have given me a personal tour of your forward operating bases (I prefer looking in the background of your pictures). I also enjoy following your check-ins and posts of your whereabouts when you are in garrison; it makes it easier to know when your home has been left unattended--it's cheaper to borrow your laptop and big screen for an extended amount of time than to buy my own. I'll bring them back, I promise! Furthermore, I noticed your child has an interest in playing basketball at the court down the street from your home. I love a great pickup game! With my level of patience and your zest for sharing your life with 500 of your closest friends, I feel like I was there with you when you took those photos…I'm very excited to see your posts!

Your Friend, The Cyber Adversary

CAC E-Mail Encryption

OPSEC FRUSTRATES THE ADVERSARY

jiowc.jose@us.af.mil