The Purple Dragon

Volume 25 | Joint Information Operations Warfare Center
Joint OPSEC Support Element (JOSE)
"A Chairman's Controlled Activity" | Spring 2013

From the Dragon's Mouth

Comments from the Chief, Joint OPSEC Support Element

Douglas Hall
LTC, USA

Protecting Critical Information in Times of Budgetary Reductions

Greetings! I am honored to be the new Joint OPSEC Support Element Chief. I took over the position in November 2012 and look forward to working with all the OPSEC professionals working hard to protect our critical information.

As you are all aware, like most organizations within DoD, the Joint Information Operations Warfare Center (JIOWC) has also been hit by the sequestration cuts. Fortunately, we were able to execute missions in the first quarter of FY'13 without a problem. Unfortunately, in the 2nd quarter we were not able to execute all of the Surveys and MTTs in support of Global Combatant Commands requests and we will be impacted by sequestration into the 3rd and possibly 4th quarters. We will try as best we can to reschedule cancelled support but may not be able to get to all of them this year.

I can guarantee you that we will support every Combatant Command, Joint Force headquarters and joint program manager with support and subject matter expertise remotely and have developed some initiatives to make sure we do just that, including weekly OPSEC awareness videos, OPSEC Program Management reviews, review of OPSEC tabs to OPLANs, increased open source research of your areas of concern, and assisting in facilitating your OPSEC Working Groups (especially if by DCO). I've started to call this our "OPSEC DOUBLE CHECK" (gesturing optional- but we welcome your recommendations for a unique move that may be used in a future public service announcement). Please contact us if you are interested in this support or have other suggestions.

So that's what we are doing here at the JIOWC, but we will not be successful in our mission without command emphasis. The sequestration cuts and their impacts have been broadcasted throughout the world and may have exposed critical information and vulnerabilities of our forces. It is vital that Commanders re-evaluate their OPSEC programs and ensure every member of their command knows and practices proper OPSEC procedures as a continuous, disciplined habit in order to ensure our adversaries do not take advantage of us as we work through this fiscal crisis.

Continued on Page 2

Inside This Issue

Joint Information Operations Warfare Center
Joint OPSEC Support Element (JOSE)
2 Hall Blvd, Suite 217
JBSA LACKLAND, TX 78236-7074

Editorial Staff – Email: jiowc.jose@us.af.mil
Phone: (210) 977-3839 DSN 969-3839
http://www.facebook.com/JIOWC.OPSEC.Support

Chief – LTC Doug Hall
Deputy – Mr. Lee Oliver

Protecting Critical Information in Times of Budgetary Reductions Continued from Page 1

To protect sensitive information, Commanders must review and update their organizations OPSEC Critical Information List (CIL) and consider the budgetary planning information that require protection, specifically information that is sensitive and deals with a command's intentions, capabilities, vulnerabilities and limitations. Next, Commanders must assess their threat and vulnerabilities, and train forces on what to protect and how to protect it. Remember, a command's information is placed at risk when transmitted unencrypted or communicated through unsecured means.

The JIOWC Joint OPSEC Support Element challenges commanders and leaders to make OPSEC a priority. Lives and mission accomplishment are at risk and OPSEC is a risk mitigator.

Robust New DoD Communications System Fielded?

Mr. Dave Swartwood
Joint OPSEC Support Element

Have you heard about the newest world-wide communications system that DoD has fielded to every member? It allows users to rapidly communicate with a few simple strokes of their computer's keyboard, send images, even share mission planning and operational data in real time. It's easy to use, already in place, mission use is expanding daily, and the comments coming in from the field are outstanding!

Are you wondering what system I'm referring to? How about if I told you this system cost the DoD nothing to implement, nothing to maintain, and nothing to train its users on how to operate? As a matter of fact, it's not even a DoD owned system.

But wait… didn't I just say it was used for operational DoD mission planning and operations? Is your OPSEC alarm sounding loud and clear in the back of your mind? The system we're talking about is Facebook. Over the past year, the Joint OPSEC Support Element has noticed a disturbing trend of DoD members using Facebook's chat/messaging feature to communicate with co-workers. Numerous survey interviews reveal users "talk" with peers and co-workers who are both on base (often in the same building or even the same office space) and those who are deployed around the world using the Facebook chat feature. Often times these chat sessions include discussions about operational mission data with potentially critical information.

The ease of Facebook chat sessions, a general lack of threat awareness, wide-spread access to Facebook (both on government systems and personal devices), and the misconception of "no one is watching what I say here" leads to a significant vulnerability to our critical information.

So what's the best countermeasure? The simple answer we often hear is denying DoD members access to social networking sites (SNS) such as Facebook. Of course, this is not a viable solution; we can't make this problem go away by ignoring it nor can we impose that much control over an employee's personal life (to include what their family does).

The most effective measure may be the simplest: increased training and awareness for our DoD employees and their families. Instead of the routine, and often boring and outdated OPSEC awareness briefings we conduct, why not focus on this issue and educate our personnel on the dangers of using SNS chat/messaging tools to discuss operational DoD information. Some of the specific points to train our personnel on include:

- ✓ The non-secure nature of social media and how easy it is for an adversary to intercept these messages.
- ✓ The extent of the cyber threats DoD faces on a daily basis.
- ✓ The specific critical information that your organization handles that may be exposed by using these chat features.
- ✓ DoD policy to not use commercial networks to transmit sensitive data.
- ✓ Historical examples of adversaries using SNS to gain intelligence.
- ✓ Your organization's regulations and policies concerning social media usage.

E-Mail Encryption

Having Trouble Opening Encrypted E-mail?

When attempting to view encrypted or send a signed Secure/Multipurpose Internet Mail Extensions (S/MIME) e-mail message in Outlook, you receive the error message: "Your Digital ID name cannot be found by the underlying security system." The problem normally occurs If you have received a new CAC, have not published your new certificates to the Global Address List (GAL) and you are trying to open old encrypted emails. The normal cause of this error message is that your computer device is unable to locate your digital certificate used to process the e-mail message. Either the CAC-based certificates are not loaded into the Windows certificate store or you haven't published your new CAC certificates to the GAL.

Remember, encrypted e-mails can only be opened with your private encryption key. When your CAC is replaced, previously encrypted email messages are not accessible with the new the CAC because it contains a new private e-mail encryption key. To enable access to e-mails encrypted and access to your previous CAC's encryption key, you need to recover the e-mail encryption key that was associated with your previous CAC.

Follow the instructions below for recovering your old encryption certificates:

Type one of the following URLs into the Web browser's address bar:

https://ara-3.csd.disa.mil/ara/Key or
https://ara-4.csd.disa.mil/ara/Key

At the Web site, you will be prompted to select your Identity certificate (the one that does not reflect e-mail in its description.) Highlight it and click **OK**.

If prompted, enter your CAC PIN; then click **OK.**

Read the US Department of Defense Warning screen, and then click **OK.**

You will receive notice that the Web site is gathering a list of escrowed keys pertaining to you. It may take a few seconds for the list to appear**.**

Review the list of keys to find the dates that match the timeframe of the key to be recovered. Click the **Recover** button next to that key.

Click **OK** when prompted to acknowledge the … *DoD subscriber for this escrowed ke*y…

A Web page displays a 16-character password. Copy (handwrite) the password exactly as shown. Once copied, click on the **Download** link.

You will be prompted to choose **Save** or **Open;** click **Open. (Save** may be chosen for transfer to an additional computer or for personal archive. The key may be imported later to the browser by double clicking on the file.) The following steps will be the same after double clicking the file.

At the *Certificate Import Wizard* window, click **Next***.*

The next prompt indicates the *File to Import*; click **Next***.*

Enter the 16-character password copied earlier, and then click the box for the first option: **Enable strong private key protection**, ***uncheck*** the **Mark this key as exportable** box; then click **Next**.

At the next prompt (Certificate Import Wizard), select **Automatically select the certificate store**, and then click **Next***.* 14. On the **Completing the Certificate Import Wizard** screen, click **Finish***.*

Click the **Set Security Level** button.

Select the **High** security level; then click **Next***.*

At the next prompt, create a password to use with the recovered key. A PIN may be used here. The password or PIN must meet Operating System requirements with the required number of characters (Vista requires 16 characters). Enter it twice and click **Finish.** At the next prompt, click **OK.**

At the **Completing the Certificate Import Wizard** window, click **Finish**.

A window stating the import was successful will display; click **OK**.

The key is now installed and ready for use. Outlook automatically selects this key when opening any e-mail previously encrypted with that key

To verify the key is in the certificate store, open **Internet Explorer.**

1. Click **Tools**, then select **Internet Options** from the dropdown menu.
2. Click on the **Content** tab.
3. Click on the **Certificates** button.
4. Under the *Friendly Name* column on the *Personal* tab, the certificate with a **CN** and Last Name is the recovered key.

Multi-Functional Devices Present an Operations Security (OPSEC) Risk When Hard Drives are Not Removed

The following is an incident that involved the preparation for turning in several multi-functional devices (printer/scanner/copier) to a vendor without the hard drives being removed. This OPSEC observation was identified during an OPSEC Survey conducted by the Joint Information Operations Warfare Center (JIOWC) Joint OPSEC Support Element (JOSE) and is reported to increase OPSEC awareness. Command names have been removed, but details are factual.

The Incident

Recently, a command decided to turn-in several copiers that were leased from a local vendor. In preparation of the turn-in, the command information technology (IT) personnel removed all classified hard drives from the classified multi-functional devices, but did not remove the unclassified hard drives located in unclassified multi-functional devices based on their supervisor's guidance. Based on the supervisor's decision to turn in the copiers with the unclassified hard drives still intact we can only assume the decision was made without regard to the possible sensitive information contained on the device hard drives. Compounding the situation, the supervisor was likely unaware of their command's policy to remove all hard drives from multi-functional devices. Finally, disposition of removed hard drives varies according to higher headquarters guidance. Luckily, the incident did not result in any loss of sensitive unclassified information typically contained on the multi-functional device hard drives because an OPSEC survey team observed the incident and informed leadership.

Many multi-functional devices manufactured today have hard drives capable of storing documents that have been scanned, printed or faxed as digitized images. These machines are used throughout DoD and often contain sensitive information when connected to DoD networks or used as a standalone device.

Personnel responsible for turning in multi-functional devices must remember those that wish to do us harm or want our information. Multi-functional devices manufactured in the last several years often employ hard drives that store digital images and vast amounts of information that could be sensitive or contain operational information. The amount and type of information on each device will vary depending on where the device is located inside your command. While it was not determined what exactly was on the hard drives that were removed, the devices were used to process all of the command's sensitive unclassified operational information at an overseas deployed location.

Most DoD copiers, printers and scanners are either leased from a vendor or government-owned. In either scenario, the possibility of sensitive information loss presents challenges when equipment is repaired or turned in for replacement. Commanders and OPSEC Program Managers must ensure personnel are trained and guidance is in place to protect the command from inadvertent OPSEC disclosures involving the release of sensitive information such as information on command's Critical Information List or Personal Identifiable Information (PII).

Lessons Learned

Organization's must be knowledgeable of risks associated with multi-functional devices. The JOSE recommends the following best practices:

- ✓ Be knowledgeable of Service and higher headquarter guidance involving turn-in procedures for multi-functional devices
- ✓ Develop and disseminate to staff local guidance regarding the turn-in and disposal of unclassified (and classified) multi-functional devices
- ✓ Remove hard drives from multi-functional devices before returning to a vendor and physically destroy or erase hard drives using approved methods or turn in to the appropriate agency/organization
- ✓ Place a sticker or placard on the multi-functional device with the following: "Warning: IAW (local policy) this device uses a hard drive that must be physically removed and disposed of properly before turn-in"
- ✓ Read DoDM 5200.01-V3, Enclosure 7, Paragraph 6, *Disposal of Computer Media*

UPCOMING OPSEC TRAINING

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

22 APR 2013, SAN ANTONIO, TEXAS

29 APR 2013, COLORADO SPRINGS, COLORADO

13 MAY 2013, WIESBADEN, GERMANY

3 JUN 2013, SAN ANTONIO, TEXAS

29 JULY 2013, CAMP ARIFJAN, KUWAIT

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 and Internet Based Capabilities Course (OPSE-3500)

8 APR 2013, YONGSON, KOREA

29 APR 2013, COLORADO SPRINGS, CO

This course introduces OPSEC practitioners to common threats, vulnerabilities, and countermeasures associated with Internet-based Capabilities (IbC).It will allow OPSEC practitioners to better assess the risk when considering IbC. Upon completion, students should be able to:

(1) Understand OPSEC concerns raised by IbC
(2) Understand the differences in motivations, skills, and activities of adversaries and how they constitute a threat to IbC
(3) Understand the risks inherent to public IbC and appropriate countermeasures required to reduce those risks
(4) Be familiar with functions, benefits, and vulnerabilities of emerging IbC technologies
(5) Understand best practices to defeat commonly used attack techniques

Prerequisite: Understanding of OPSEC fundamentals (for example OPSE-1300/1301

*****NOTICE*****

Due to the continuing uncertainty of the DoD budget, please check www.ioss.gov or contact the JOSE for updates to our training schedule.

Class dates can change or be cancelled at any time.

OPSEC Analysis and Program Management Course (OPSE-2500)

9-12 APR 2013, YONGSON, KOREA

23-26 APR 2013, SAN ANTONIO, TEXAS

30 APR – 3 MAY 2013, COLORADO SPRINGS, CO

14-17 MAY 2013, WIESBADEN, GERMANY

4-7 JUN 2013, SAN ANTONIO, TEXAS

30 JUL – 2 AUG 2013 CAMP ARIFJAN, KUWAIT

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.

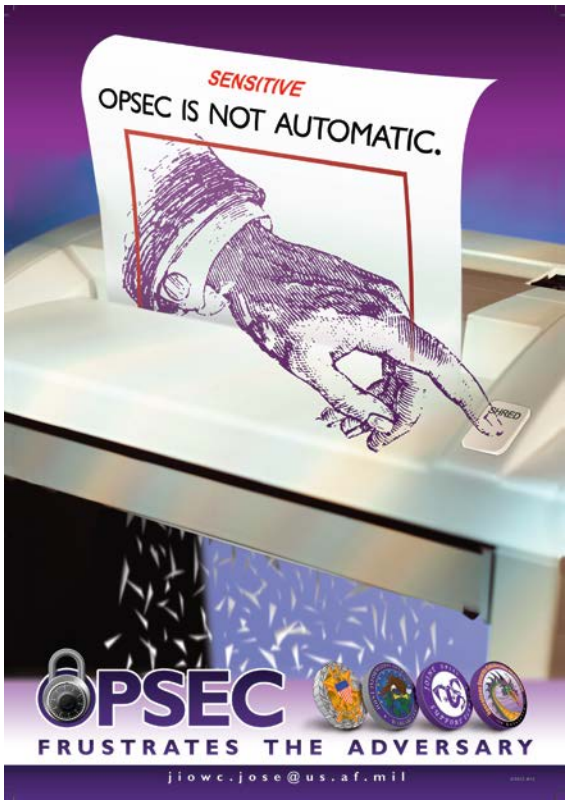
Prerequisite: OPSEC Fundamentals (OPSE-1301) or equivalent

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

OPSEC REMINDER: Photocopying of military identification cards:

Recent incidents regarding the photocopying of military identification cards and common access cards (CAC), by commercial establishments to verify military affiliation or provide government rates for service, have been reported. Personnel are reminded that photocopying of US government identification is a violation of title 18, US code part 1, chapter 33, section 701and punishable by both fine and/or imprisonment. Organizations that are exempt from this restriction are for the following purposes: military medical services or military police tickets.



How to See the Encrypt Icon in Microsoft Outlook 2010

To see the Encryption icon for new email messages in Microsoft Outlook 2010, users must now click on the Option ribbon to see the icon.

To always see the Encrypt icon, users can tailor the ribbon and place the Encrypt icon back on the primary Message ribbon by following the steps below:

- In Outlook 2010, under the Home tab select **"New Email"**. This will open a new untitled message window
- Right click anywhere in the Message ribbon, and select **"Customize the Ribbon"**
- In the panel on the right-hand side, ensure "**New Mail Message"** (first entry under Main Tabs) is selected/highlighted. (This is typically the default selection.)
- On the left-hand side of the window, use the pull-down arrow for "Choose commands from" and select **"Main Tabs"**. In the panel below, expand the **"Options"** section. Select/highlight **"Permission"** and click **"Add"**
- The Permission Group will be added at the bottom of the Main Tabs section in the right-hand panel. Click **"OK"** to close the **Customize the Ribbon** window.
- The Permission Group that contains the Sign and Encrypt commands should now be visible on this New Message ribbon and any future new Messages.

Purple Dragon 6

Tips to Prevent Sensitive Information Disclosures Today

Family members play a vital role in protecting sensitive information: Our family members are involved in handling unclassified but sensitive information about our profession of arms. Raising our family members OPSEC awareness (for example: providing OPSEC awareness materials) will enhance mission effectiveness while reducing OPSEC disclosures.

Identify and inform personnel on what unclassified information must be protected and the countermeasures used to protect the information from getting into the wrongs hands: Inform personnel on the organization and higher headquarters Critical Information List (CIL). Make sure the list is distributed throughout the organization and personnel are aware of where to find it if not immediately available. Remember: we aren't looking to remind or train personnel to protect all unclassified information, just the critical information the commander or director wants to protect. People must be aware of what to protect in order to protect it.

Identify where critical information resides: This sounds simple, but is it? For starters, computer systems and networks hold much of our information--servers, desktops, laptops, and external hard drives. Then you have mobile devices, mobile phones, and personal digital assistants. After this come other gadgets such as digital cameras. Finally, you have to identify all the people and the processes involved with storing and sharing information—contractors and partners.

Identify who has access to critical information: The smart answer is only those that need access. In reality, this may be a more complex problem than you first realized. This is all about figuring out who has access—and who needs access. Chances are, more people have access to your computer files due to improper security settings. Identify who has access to your information when using the web. Verify security settings are correct.

Remove access to files and folders where personnel don't have a need-to-know. Even though the information is unclassified, not everyone needs access to all your critical information from the web or internal shared drives. Remove access where it makes sense, and reduce the risk.

Identify when and how critical information leaves the organization: If critical information is sent off site—whether as a backup tape, portable drive (in or out of laptop), or CD ROM—it should be encrypted.

Protect the endpoint: What do people lose or get stolen? Laptops, mobile phones, thumb drives and CDs. These devices must be protected encrypted.

Protect critical information in motion: Unencrypted e-mails are the number one risk to critical information transmitted electronically. When personnel don't know how to encrypt or their device or system are not configured properly, people are more likely not to encrypt. It's much easier to train personnel in your organization on how to encrypt when you, as the OPSEC Program Manager or Coordinator, know how to do it yourself.

Revisit how paper documents are destroyed and handled: A good majority of OPSEC disclosures still come from improper disposal of paper documents in the trash and recycling containers. Critical unclassified information has to be properly destroyed and destruction methods must be checked on a regular basis to ensure compliance. Place cross-cut document shredders near photo copiers and outside of meeting rooms. Don't forget to review recycling procedures for improper disposal of sensitive information.

Revisit how systems and devices are disposed: How are laptops, mobile devices, copier, printers and digital scanner hard drives and servers that contained unclassified sensitive information disposed of? Is the data on those adequately erased or hard drives recovered or disposed of during turn-in.

How to Protect Your Privacy on FaceBook

1. Control Your Friend List. *Establish and maintain connections with ONLY people you know and trust.*

- Go to your Timeline profile page
- Click and review your "Friends" list
- Mouse over "Friends" and edit as needed

2. Avoid Photo/Video/Post Tags in Timeline.

- From the far right icon, select "Privacy Settings" and click on "Timeline and Tagging"
- Under "Who can add things to my timeline?" Go to "Review posts friends can tag you in before they appear on your timeline?" Click edit and select "Enabled" to start. This creates a manual review before posting to your timeline
- Under "Who can see things on my timeline?" go to "Who can see posts you've been tagged in on your timeline?" Review and select category of friends to allow or customize.
- Under "Review what other people see on your timeline" offers a public and specific friend view of your timeline
- Under "How can I manage tags people add and tagging suggestions?" go to "Review tags people add to your own posts before the tags appear on FB?" Next, click edit and select enabled.
- For "Who sees tag suggestions when photos that look like you are uploaded?" recommend clicking edit and selecting "no one"

3. Protect Your Photo Albums.

- Go to your timeline and click on your photos
- On **each** of your self-titled photo albums, select "Friends" or customize (e.g. only me, individuals, etc…) to your desire
- With a "public" default setting, FB does not afford protection for "Cover Photos". Post in this album at your own risk
- For photos under "Mobile Uploads", "Profile Pictures", and "Timeline Photos" you must open the album and set privacy for each photo individually

4. Limit Historical Postings

- Go to Privacy settings and under "Who can see my stuff?" go to "Limit the audience for posts you've shared with friends of friends or public?"
- Click on "Limit Past posts" and then click on "Limit old posts" For future timeline postings, ensure to select desired level of audience for each post.

5. Stop Embarrassing Wall Posts. *This is an individual risk assessment depending on your situation and the friends you keep. Assume anyone can see activities associated to your personal or professional life you've posted*

- Go to Privacy settings and click on "Timeline and Tagging"
- Under "Who can add things to my timeline?" click on "Who can post on your timeline?" then click "edit" and choose either "Friends" or "Only me"

6. Keep Your Friend(s) List Private

- Go to your Timeline profile page and click on your "Friends"
- Near the top right of page, click on "Edit"
- Under "Who can see your friend list?" Click the arrow and select your desired category

7. Limit Facebook Search Results

- Go to Privacy Settings
- Under "Who can look me up?" click on "Who can look up your timeline by name?" then click on "edit" select "Friends"

8. Remove Your Facebook Profile from Google & Other Search Engines

- Complete Step #7 above
- Next, click on "Do you want other search engines to link to your timeline?" and ensure the box, "Let other search engines link to your timeline?" is unchecked

9. How to deactivate or delete your account

- To deactivate go to Account Settings and on the left hand side click on "Security"
- Next, click on "Deactivate your account"
- To delete your account, go to the following URL and fill out appropriate form: https://www.facebook.com/help/delete_account

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

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

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