



# The Purple Dragon



Volume 26

Joint Information Operations Warfare Center  
Joint OPSEC Support Element (JOSE)  
"A Chairman's Controlled Activity"

Summer 2013

## From the Dragon's Mouth

Douglas Hall, LTC, USA

Chief, Joint OPSEC Support Element

### OPSEC & Furlough Considerations

Operations Security (OPSEC) must remain a priority as commanders conduct business with civilian furloughs starting this month. During this period, commanders should work with their OPSEC Program Manager and utilize the 5-step OPSEC process to identify any new threats, indicators, and vulnerabilities created by their planning and implementation of civilian furloughs. Commander's must review their current OPSEC measures for effectiveness, and if necessary develop and implement new OPSEC measures to prevent disclosures.

How commanders conduct business during the next several months will be of great interest to our adversaries who are continually monitoring our effort and seeking new avenues to gain sensitive and critical information. To successfully mitigate unacceptable risk to activities, intentions and capabilities, the following is a list of items that commanders should consider adding to their critical information list:

### Inside This Issue

- 2 "OPSEC within an Exercise" or "OPSEC of an Exercise"
- 4 Upcoming OPSEC Training
- 6 Which Paper Shredder Should I Use to Destroy Critical Information
- 7 JOPES Deep Sixed
- 8 Is Your Organization OPSEC Training Tailored?
- 10 OPSEC Universal Joint Task List Incorporation Into Surveys and Exercises

- Information related to organization's mission areas affected by furloughs
- Information regarding loss of capability or degradation
- Changes or modifications to techniques, tactics, and procedures
- Duty rosters, manpower shortages, or changes
- Changes to schedules and timetables
- Limitations or reduced capabilities
- Changes in force composition or disposition

Commanders should also consider:

- Directing members to not discuss operational limitations related to furloughs outside of work spaces
- Ensuring members are aware that social media sites should not include work related information
- Placing emphasis on members encrypting e-mails that contain sensitive information

Strong OPSEC measures are a key to denying adversaries access to sensitive information.

**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](mailto:jiowc.jose@us.af.mil)  
Phone: (210) 977-5192 DSN 969-5192  
<http://www.facebook.com/JIOWC.OPSEC.Support>

Chief – LTC Doug Hall  
Deputy – Mr. Lee Oliver

## “OPSEC within an Exercise” or “OPSEC of an Exercise”

---

Mr. Dave Swartwood, Contractor  
Joint OPSEC Support Element

If you've read the title of this article and you're slightly confused... welcome to the world of integrating OPSEC into a military exercise. Many times throughout the year, the Joint OPSEC Support Element (JOSE) participates in Combatant Command and Joint Task Force level exercises. Most of these exercises are command post exercises which involve notional forces deployed to the field and provide a command staff the opportunity to practice their battle rhythm and processes. Other exercises actually involve forces deployed to the field to conduct military maneuvers. You've heard the old adage “train the way you fight” and these exercises are no different. Many times, these exercises provide DoD an opportunity to train on new equipment or test new procedures; things that will make us better warfighters in the future. I hope it's clear to our readers how important good OPSEC would be to these exercises and the ramifications of an adversary exploiting our OPSEC weaknesses.

Over the past year I've had the opportunity to participate in several of these training events by providing both external OPSEC survey support and through duties as an OPSEC Planner within the Joint and/or Coalition Exercise Control Group (J/CECG). After a bit of confusion on my part, I clearly began to see a difference between integrating/evaluating “OPSEC within the exercise” and implementing/evaluating “OPSEC of an exercise.” So what's the difference?

First, let's look at “OPSEC within an exercise.” How do you incorporate OPSEC play into your training event? Is OPSEC specifically listed as a training objective? If not, how can you factor successful OPSEC into your organization's training objectives? I'd suggest good OPSEC should play a role in every training objective you have. Next question would be are there any OPSEC specific or related inject/events planned for the exercise? This can be an entertaining role to accomplish as an OPSEC Planner within the exercise control group.

Your roll is to develop exercise events that the training audience must react to and solve. Think of how many creative ways you can simulate an adversary exploiting our vulnerabilities! How about if the training audience doesn't react properly or in time and you've built in follow on events that demonstrate the ramifications of poor OPSEC? Maybe a convoy is ambushed because their route was disclosed? Maybe an aircraft is shot down because their time over target was passed in the clear? How about a network intrusion because someone sent their login/password or network architecture in an unencrypted e-mail? The possibilities are endless. Remember, exercise scenarios involving OPSEC problem sets should be sent to all levels and sections of the training audience – not just to the OPSEC manager or coordinator. You want to ensure OPSEC issues are identified/remedied at the lowest levels but also properly reported up the chain of command to leadership and OPSEC program managers. By building OPSEC into the exercise scenarios, you're providing realistic training to your organization and helping ensure your OPSEC program is tested and adequately protects your critical information. But that's only half of your concerns; what about protecting the actual exercise and subsequent results themselves?

This is where “OPSEC of the exercise” comes into play (no pun intended). Do you think an adversary would like to see how you “train the way you fight?” Do you even want your adversaries to know you conducted an exercise? How about your results? Did you meet your training objectives? Did you identify areas that need improvement, or worse yet, that your unit is simply not mission-ready to accomplish certain tasks at this time? I hope you can see the difference between these two aspects of OPSEC and your training exercises. Too often we focus on one and not the other or we try to blend them together into one thought process. From experience, OPSEC programs that clearly separate these two aspects during an exercise have a stronger OPSEC program and provide better training and protection of their critical information.

# Actions for OPSEC Program Managers and OPSEC Planners to Consider for Integrating OPSEC into Exercises

## OPSEC within an Exercise

- ✓ Are there specific OPSEC training events built into your exercise scenario?
- ✓ Are there specific OPSEC objectives identified in your training goals?
- ✓ How can OPSEC be factored into all of your training objectives?
- ✓ How would an OPSEC problem impact the successful accomplishment of your organization's mission?
- ✓ Do your training directors and organization leaders understand how OPSEC improves their mission effectiveness and the planning process?
- ✓ Have you educated your training audience on what critical information to protect within the exercise scenarios (i.e., the CIL for the OPLAN being exercised)?
- ✓ Have you educated your personnel on what OPSEC countermeasures are available within the exercise scenario?
- ✓ Does your training audience know how to identify, resolve and report OPSEC problems they encounter during the scenarios?
- ✓ Are your training objectives based on Universal Joint Task List items for your Command?

## OPSEC of an Exercise

- ✓ Who, at the very earliest stages of exercise planning, makes the decision on what information requires protection?
- ✓ How sensitive is your exercise and how important is it to protect the fact you're even conducting this training event?
- ✓ Have you educated the training audience on the real-world critical information to protect concerning this exercise (i.e., a list of items they shouldn't disclose about the exercise itself and OPSEC measures to protect the information)?
- ✓ Do you need to publish and disseminate another small CIL (or possibly update your standing unit CIL) about your exercise participation?
- ✓ Have you specifically trained your personnel to protect the results (good or bad) of the exercise?
- ✓ Have you considered having a dedicated team observe your organization while the exercise is underway to report how your indicators and signatures have changed?
- ✓ Does the exercise control group need specialized OPSEC training above and beyond that of the exercise players?
- ✓ What are your vulnerabilities during the exercise planning events (conferences, meetings, etc)?

# UPCOMING OPSEC TRAINING

## OPSEC ANALYSIS AND PUBLIC RELEASE DECISIONS COURSE (OPSE-1500)

22 JUL 13, CAMP CASEY, SOUTH KOREA

5 AUG 13, COLORADO SPRINGS, CO

12 AUG 13, SAN ANTONIO, TX

19 AUG 13, HONOLULU, HI

7 SEPT 13, DJIBOUTI, AFRICA

8 SEPT 13, MANAMA, BAHRAIN

23 SEPT 13, GRAFENWOEHR, GE

7 OCT 13, SAN ANTONIO, TX

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)

22 JULY 13, CAMP CASEY, SOUTH KOREA

5 AUG 13, COLORADO SPRINGS, CO

7 AUG 13, SAN ANTONIO, TX

21 JUN 13, MIAMI, FL

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)

## OPSEC Advocacy and Outreach Support to U.S. Army South

*Continued from page 4, "UPCOMING OPSEC TRAINING"*

### OPSEC ANALYSIS AND PROGRAM MANAGEMENT COURSE (OPSE-2500)

23-26 JULY 2013, CAMP CASEY, SOUTH  
KOREA

13-16 AUG 13, SAN ANTONIO, TX

20-23 AUG 13, HONOLULU, HI

3-6 SEPT 13, DJIBOUTI, AFRICA

9-12 SEPT 13, MANAMA, BAHRAIN

24-27 SEPT 13, GRAEFENWOEHER, GE

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](https://www.iad.gov/ioss/index.cfm) OR  
CONTACT THE JOSE AT: [JIOWC.JOSE@US.AF.MIL](mailto:JIOWC.JOSE@US.AF.MIL)

JIOWC/JOSE brought OPSEC advocacy and outreach support to the U.S. Army South (ARSOUTH) Morale, Welfare, and Recreation Day on 28 June 2013. The JIOWC/JOSE's Mr. Troy Richardson and Mr. Tomas Ovalle collaborated with ARSOUTH OPSEC Program Manager (OPM), Mr. Daniel Arias, and Joint Base San Antonio OPMs, Mr. Mark Magalski and Mr. Don Wyman, to present OPSEC awareness to over 250 members and their families and friends. Awareness activities included face-to-face discussions and offerings of pens, lanyards, brochures, and lip balm – all appropriately OPSEC themed.



**ARSOUTH Family and Friends  
Learn about OPSEC**

The ARSOUTH leadership praised the JIOWC/JOSE and Joint Base San Antonio collaboration and continued efforts to enhance and advance OPSEC awareness. When people ask questions and talk about OPSEC mission, assurance and effectiveness are positively impacted. One ARSOUTH member was overheard saying to his teen children, "This (OPSEC) is why I tell you not to post details about my travels online...so Dad comes home safe!"

**Like US on Facebook!**  
[facebook.com/JIOWC.OPSEC.Support](https://www.facebook.com/JIOWC.OPSEC.Support)

## **Which Paper Shredder Should I Use to Destroy Critical Information?**

The Joint OPSEC Support Element (JOSE) is often asked, "What shredder should I use to destroy information found on my organization's critical information list (CIL)?"

The DOD OPSEC manual does not state the type of shredder to use to destroy sensitive unclassified information, but does state the methods and the end result in Enclosure 5, Paragraph 3.b. of DoDM 5205.02-M, DoD Operations Security Program, which states: "The preferred method to destroy critical information is by shredding or burning. If these methods are not available critical information shall be destroyed in a manner that prevents routine recognition or reconstruction."

Disposal methods are considered adequate if the documents are rendered unrecognizable or beyond reconstruction. When it comes to what shredders should an organization use to destroy sensitive documents, it comes down to what is their higher headquarters guidance and can the shred be easily put back together as in the case of some strip shred.

While shredding is arguably the safest means of disposal, the use of burn bags remains a viable option in classified areas in which the documents might be pulverized or burned. Regardless of the method of destruction, the key thing to remember is to ensure the documents are "rendered unrecognizable beyond reconstruction."

While there is no policy specifying the type of shredder to use for destroying sensitive documents, it is highly recommended and considered a best practice to always use a cross cut shredder. On numerous OPSEC surveys conducted by the JOSE, team members have pieced back together paper strips that contained sensitive information. On several occasions, the straight cut shredder paper corresponded to the actual rows of information. As a result, none of the sensitive information had been destroyed.

The DoD manual does not address shredder residue size. As a best practice, refer to the National Institute of Standards and Technology (NIST) Special Publication 800-88, "Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology," issued September 2006, which states: "Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32-inch security screen (reference NSA Disintegrator EPL)." The National Security Agency Evaluated Products Lists (EPL) for shredders can be found at: [www.nsa.gov/ia/\\_files/government/MDG/NSA\\_CSS-EPL-02-01-Z.pdf](http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-02-01-Z.pdf). Remember, the choice of a shredder must make paper documents containing sensitive information unrecognizable beyond reconstruction

### **Want a Safe, Secure Way to Transfer Files?**

**DoDIIS One-Way Transfer Service (DOTS)**  
<https://dots.dodiis.mil>

**DOTS is a Defense Intelligence Agency-sponsored solution to perform one-way, up-domain transfers. It allows users to send files from NIPRNet to SIPRNet, from NIPRNet to JWICS, and from SIPRNet to JWICS.**

#### **Supported File Types/Extensions**

**Archives: .zip**  
**HTML & XML: .htm, .html, .xhtml, .xml**  
**Images: .bmp, .gif, .jpeg, .jpg, .png, .tif, .tiff**  
**Microsoft Office: .doc, .docx, .ppt, .pptx, .xls, .xlsx**  
**Adobe Documents: .pdf**  
**Text: .csv, .txt, .utf8**  
**Video: .3gp, .3gp, .asf, .avi, .mov, .mpeg, .mpg**

## JOPEX SOON TO BE DEEP SIXED, APEX IN

Mr. Greg M. Hochstrasser, Contractor  
Joint OPSEC Support Element

**REF:** CJCSM 3130.03 APEX Planning Formats and Guidance, 31 August 2012

Information Operations/OPSEC Planners, take note. Major changes are evolving in how contingency and crisis action planning are being accomplished within a Joint DoD and IA (Inter-Agency) environment. Joint Operations Planning and Execution System (JOPEX) is slowly being phased out as the Adaptive Planning and Execution (APEX) is phased in. APEX is the “web based client application” planners will primarily utilize for participation in any joint planning cycle/mission.

**JPES Framework (JFW):** JPES (Joint Planning and Execution Services) is the back end component that provides data services to APEX. JFW is a suite of software and infrastructure components and services to support management, storage, and access control to the JPES data as web services enabled data objects as well as data distribution, synchronization, data business rule enforcement, and workflow management in support of JPES capabilities.

**APEX:** Provides extensible resources including:

- Exposes JPES data objects as web services (SOAP/HTTPS)
- Automatic authentication using PKI certificates

- Data access authorization
- DoD/Joint C2 Architecture compliant
- Leverages Enterprise and other common services

**IRCs Redefined:** Information Related Capabilities (IRCs) have been redefined in the APEX environment. Per REF CJCSM 3130.03, IRCs and other capabilities are now categorized as:

### Core IO Capabilities:

- MISO
- MILDEC
- OPSEC
- EW

### IO Supporting Capabilities:

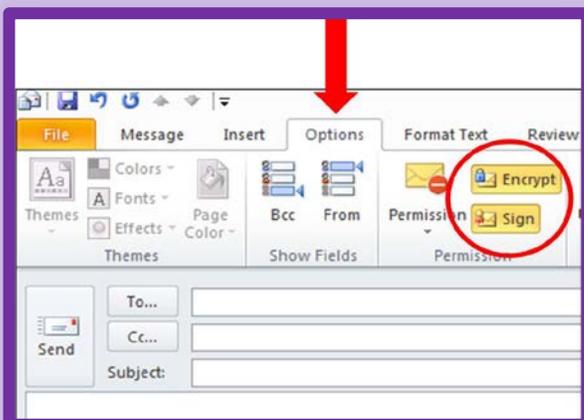
- Cyberspace Operations
- Information Assurance
- Physical Security
- Physical Attack
- Counterintelligence
- Combat Camera

### IO Related Capabilities:

- Public Affairs
- Civil Affair

---

## E-MAIL ENCRYPTION TIP



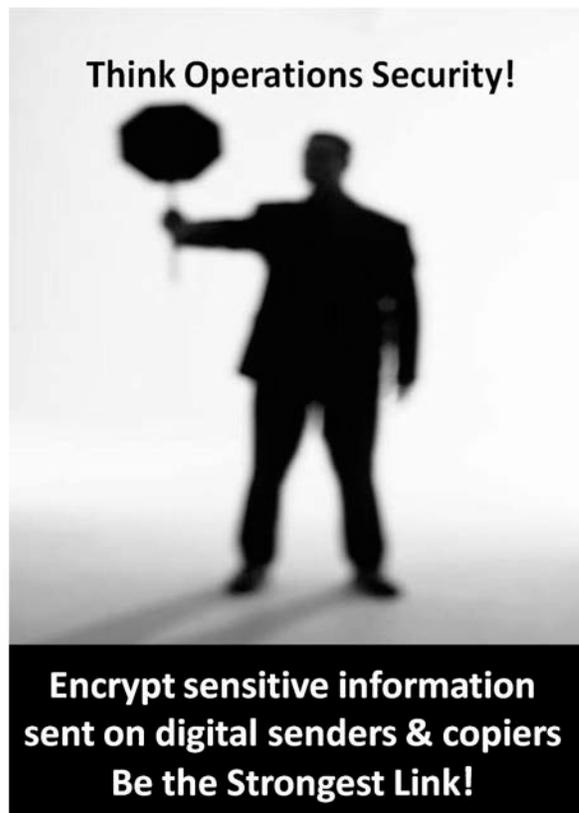
In Microsoft Outlook 2010, the digital encryption icon does not show when a new e-mail is created. In order to see the icon for encryption, you must click the “Options” tab, then the “Encryption” button to encrypt an e-mail.

## Is Your Organization's OPSEC Training Tailored?

Mr. Aaron DeVaughn  
Joint OPSEC Support Element

The Joint OPSEC Support Element has conducted numerous OPSEC surveys over the last eight years and has identified one common training observation among newly assessed commands, which is "Initial and annual OPSEC training is not tailored for \_\_\_\_\_."

If this fits your organization, put your name on the line and read on to correct it. Don't pass "Go" or collect any money until you read this article. Let's get started. If you're going to increase the OPSEC awareness level within your organization, your OPSEC training must be continuously tailored to your mission and critical information. It's acceptable to use standardized service or higher headquarters OPSEC training, but this training does not relieve you, the OPSEC Program Manager, of having to provide tailored OPSEC training to your organization. Tailored OPSEC training, as a minimum should include, identification of local OPSEC policies and procedures, critical information list, OPSEC measures, individual responsibilities and OPSEC point of contact(s) as a baseline. Training should also address the threat and techniques employed by adversaries attempting to obtain sensitive information. Ensure training is focused on what employees need to know rather than going through the motions as a check in the box.



All Services and DoD publications follow the same common guidance and best practice as stated below in their governing guidance: Department of Defense Manual, DoDM 5205.02-M, *DoD Operations Security Program Manual*, Enclosure 7, paragraph 3a. states, "All personnel in the organization shall be provided an initial orientation to the organization's OPSEC program." And paragraph 3b. states, "Initial orientation at a minimum shall include an explanation of OPSEC, its purpose, threat awareness, the organization's

critical information, and the individual's role in protecting it. Paragraph 3d. states, "As a minimum, all personnel shall receive annual refresher OPSEC training that reinforces understanding of OPSEC policies and procedures, critical information, and procedures covered in initial and specialized training. Refresher training should also address the threat and techniques employed by adversaries attempting to obtain classified and sensitive information."

Army Regulation 530-1, *Operations Security (OPSEC)*, paragraph 4-2, (2)b states, "At a minimum, all Army personnel must receive an annual OPSEC

awareness training briefing provided by the unit or organization's OPSEC Officer. This training must be updated with current information and tailored for the unit's specific mission and critical information."

Air Force Instruction 10-701, *Operations Security (OPSEC)*, paragraph 5.1, states that organizational specific training will be provided in addition to the training Air Force personnel receive through AF Advanced Distributed Learning Service to ensure all personnel in the Air Force are aware of local threats, vulnerabilities and critical information unique to their duty assignment.

Navy Instruction OPNAV 3432.1A, *Operations Security (OPSEC)*, paragraph 1.c.(3)(b), states “OPSEC awareness training at least annually to include review of the five step OPSEC process, CI list(s), current threats and vulnerabilities, site OPSEC plan, and results of OPSEC assessments and survey.”

Marine Corp Order 3070.2, *The Marine Corps Operations Security (OPEC) Program*, paragraph (9)(b) states, “Develop and implement OPSEC programs tailored to the command’s needs.”

**Who** should receive organizational-specific and tailored OPSEC training? The answer is quite simple, everyone who directly or indirectly comes in contact with critical information or works in your area of responsibility. OPSEC training is for everyone, from the Commanding General to the lowest enlisted member, deploying and redeploying individual and family members. Your training must also take into consideration contracts and contractors, and partnered nation personnel. Check with your Foreign Disclosure Officer prior to releasing training materials to partner nation personnel even if it’s unclassified. It’s important for the workforce to understand what to protect, how to protect it, and the risks and consequences of adversary collection of sensitive unclassified information.

**Continue** to update your local OPSEC training as changes to mission, threat, vulnerabilities, countermeasures may occur. A garrison critical information list (CIL) and applicable countermeasures are not the same as when a unit is deployed. OPSEC training must be tailored for the geographical location and mission of the organization. All too often, OPSEC Program Managers present from initial to annual, generic OPSEC training. As technology and missions change, threats to sensitive information change and adversaries adjust their collection efforts. Your organization’s OPSEC awareness training must reflect this reality. To know if your OPSEC training is effective, consider asking yourself these questions:

- ✓ Is my OPSEC training generic and not tailored for the organization? If you are seeing the same training for both initial and annual, develop tailored OPSEC training for your unit.
- ✓ Is the only OPSEC training I’m using for my organization a service or higher headquarters provided OPSEC training? If “Yes”, then go back to the first question.
- ✓ Does my organization’s OPSEC training inform employees of our local OPSEC guidance and where to find it?
- ✓ Does initial and annual OPSEC training inform employee of the content of the organization’s critical information list and how to apply it?
- ✓ Does civilians, contractors, and military (guard, reservist, ID) receive initial and annual OPSEC training?
- ✓ Does your organization’s contracts reflect some form of minimum OPSEC training requirements for contractors?

OPSEC training’s purpose is to reinforce command policy to protect sensitive information. By helping the workforce understand how they process sensitive information and discussing ways to protect it, you can create a strong fundamental understanding about protecting sensitive information locally and not just go through the motions.

OPSEC within an organization is only as strong as to what the people are trained to do, their retention of the training information, and their actions to protect critical information from getting into the wrong hands.



## **OPSEC Universal Joint Task List Incorporation into Surveys and Exercises**

---

One of the issues an OPSEC Program Manager (OPM) may face is trying to establish validity for their programs beyond the additional duty required by a policy letter. One method is to make OPSEC a measureable task for the command by including OPSEC in the command's Joint Mission Essential Task List (JMETL). How does the OPM get OPSEC into the JMETL? It begins with the Universal Joint Task List (UJTL). OPMs can use UJTLS to develop exercise scenarios and move their OPSEC program beyond the halls and walls and just focus on annual training completion numbers.

The approved PDF version as of April 2013 of the UJTL can be found at [http://www.dtic.mil/doctrine/training/ujtl\\_tasks.htm](http://www.dtic.mil/doctrine/training/ujtl_tasks.htm). The UJTL is a menu of tasks in a common language, which serves as the foundation for capabilities-based planning across the range of military operations. The UJTL supports DOD in joint capabilities-based planning, joint force development, readiness reporting, experimentation, joint training and education, and lessons learned. It is the basic language for development of a JMETL or Agency Mission Essential Task List (AMETL) used in identifying required capabilities for mission success.

The individual tasks that comprise the JMETL are Mission Essential Tasks (METs). METs are evaluated every month through the Defense Readiness Reporting System (DRRS). By including OPSEC METs, the commander and his staff will be required to measure the effectiveness or performance of OPSEC. METs also serve as the basis for training objectives for exercises.

The following UJTL's address OPSEC and can be incorporated into a command's Mission Essential Tasks (METs). UJTL's are broken into separate categories based on the level of your organization. "SN" references strategic/national level tasks, "ST" references strategic tasks (COCOM's), "OP" references operational tasks (COCOM and Joint Task Force), and "TA" references tactical tasks for tactical level of operations. As an OPM, assess your program and subordinates against UJTLS for your level of operations.

The UJTL is not directive in nature, but is a 'shopping list' for a command to select tasks that the command decides are required to accomplish their mission. Under each UJTL are measures that describe actions to be accomplished associated with each UJTL. Again, these are not directive or all inclusive, but a shopping list of measures that can be used to define Measures Of Effectiveness (MOE) for each UJTL.

## **Consider Your Sensitive Data Before Giving Your Personal Computer Away**

---

When you decide to upgrade and get a new computer, odds are you won't throw your old computer away, but may decide to give it away.

Your choices to consider may be giving your old PC to a family member, school, church, or perhaps to someone who can't afford a new computer. No matter what you decide, you must think about the huge amount of personal data residing on the hard drive such as, family photographs, bank records, and other sensitive information before you give it away. For this reason as a minimum precaution to safeguard your sensitive information you should remove the hard drive. This might be the easiest way to protect your sensitive information from getting into the wrong hands. Now, I know it might be hard for the person who receives your computer without a hard drive, but you must consider the risk if you decide not to take any actions or use the right tools to delete your information. There are many tools on the market to help you delete your information, just find the one that works best for you. Remember, the bad guy is trying to obtain your sensitive information, don't make it easy!



# OSCAR Helpdesk News

## Reduction in Support

If you are having issues registering for an account, logging into your account or general questions about the Operations Security Collaboration Architecture or OSCAR, please feel free to continue to contact the OSCAR helpdesk at [oscar\\_riskmgt@alionscience.com](mailto:oscar_riskmgt@alionscience.com).

However, OSCAR helpdesk support has had a reduction in staff and the system administrators are encouraging all Army, Navy, Air Force, and Marine Corps OSCAR users to seek help from their Service Admin1s prior to contacting the OSCAR helpdesk. OSCAR's Admin1 points of contacts are located in the left margin of the next page.

The process for submitting a request/problem is simple and consists of a few pieces of information that is critical for administrators to assist you. When explaining a problem/request, include as much detail as possible, such as the web address (link) of the page you were on, the process in which the issue was produced and any specific error message received. It is also important to provide the first and last name used during registration (not titles or nicknames), DTIC LDAP UID that you use to login to OSCAR, and complete contact information (commercial callback number-OSCAR Helpdesk doesn't support DSN, SIPR and NIPR email addresses). This greatly helps OSCAR administrators, DTIC's helpdesk, and the developers to fully understand and correct for the issue.

The best way to contact the OSCAR helpdesk is to email [oscar\\_riskmgt@alionscience.com](mailto:oscar_riskmgt@alionscience.com). The OSCAR helpdesk will assist all users in the order in which the requests are received and execute the request as soon as possible. We will continue to approve new accounts within the 1 to 10 business day window. We appreciate our users and appreciate their patience during this time.

In addition to the reduction in helpdesk support, OSCAR outreach activities will also be reduced which will impact the frequency that the OSCAR Newsletter is published and disseminated. If anyone has any questions with regard to OSCAR, please feel free to contact your Admin1 or the OSCAR helpdesk and we'll return your correspondence as soon as we can.

*This article is taken from the May 2013 OSCAR Newsletter Vol. 4 No. 8.*

## OSCAR Affiliates

### OSCAR Working Group Chair

**Jim Magdalenski**

757-417-7100 x3

[james.magdalenski@navy.mil](mailto:james.magdalenski@navy.mil)

[james.magdalenski@navy.smil.mil](mailto:james.magdalenski@navy.smil.mil)

### Marine Corps Admin1

James J. Sydnor

Operations Security Program Manager

703-693-4293

[james.j.sydnor@usmc.mil](mailto:james.j.sydnor@usmc.mil)

[james.j.sydnor@usmc.smil.mil](mailto:james.j.sydnor@usmc.smil.mil)

### Navy Admin1

**Robert "Scott" Carey**

Naval OPSEC Support Team (NOST)

757-417-7100 ext 4

[Robert.s.carey@navy.mil](mailto:Robert.s.carey@navy.mil)

[Robert.s.carey@navy.smil.mil](mailto:Robert.s.carey@navy.smil.mil)

### Air Force Admin1

**Lawrence W. Wisdom**

AF Senior OPSEC Program Analyst

202-404-8443

[lawrence.wisdom@pentagon.af.mil](mailto:lawrence.wisdom@pentagon.af.mil)

[lawrence.wisdom@af.pentagon.smil.mil](mailto:lawrence.wisdom@af.pentagon.smil.mil)

### Army Admin1

**Reginald E. Smith**

HQDA OPSEC Program Coordinator

703-697-9902

[reginald.smith15@us.army.mil](mailto:reginald.smith15@us.army.mil)

[reginald.smith@hqda.army.smil.mil](mailto:reginald.smith@hqda.army.smil.mil)

## Web Links

OSCAR:

<https://oscar.dtic.smil.mil/oscar>

OSCAR Registration:

<https://reg.dtic.smil.mil/>

DTICRegistration/ OSCAR

Password Reset:

<https://reg.dtic.smil.mil/UpdateProfile>