The Purple Dragon

Volume 22 Joint OPSEC Support Element (JOSE) Spring 2011

From the Dragon's Mouth

Comments from the Director, JIOWC OPSEC Support

CAPT Mark Springer
Director
JIOWC OPSEC Support

"Raising a Purple Dragon: Evolution of OPSEC Support to the Joint Community"

Today's war fighter faces many challenges protecting information in today's ever changing information environment. It is easier for our current and potential enemies to collect the bits and pieces of data to construct their intelligence picture than ever before. Of course, this vulnerability is recognized, and one of the most effective tools to mitigate it is through the use of Operations Security (OPSEC). In the Joint arena, the Joint Information Operations Warfare Center's (JIOWC) Operations Security (OS) Directorate was created and is the nucleus for OPSEC support to the Joint community.

Known as the Joint OPSEC Support Element (JOSE), the JIOWC's OPSEC Support Directorate provides OPSEC support through three main avenues as defined in DOD Directive 5205.02, *DoD Operations Security Program*. These are training and program development; planning and exercise support; and the evaluation of OPSEC programs through OPSEC surveys. Primary customers for these services are the ten US Combatant Commanders and their task forces. Support over the years has also been provided to the Service components, other US government agencies, as well as allied and coalition forces. Support can be provided via reach back capability, or more likely than not, forward deployments across the globe, including combat zones in Iraq, Afghanistan and the Horn of Africa.

To place context on the scope of the demand for OPSEC support, in 2010 the JOSE , in meeting its DOD- directed tasks conducted 32 mobile training teams, training 720 students on how to be an OPSEC program manager; performed 37 OPSEC surveys to identify exploitable vulnerabilities and recommended fixes to mitigate them; provided 7 program management consultations to assist the development of command OPSEC programs; assisted in 9 information operations planning efforts; and provided support to 11 joint exercises.

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
Phone: (210) 977-3839 DSN 969-3839
http//www.facebook.com/JIOWC.OPSEC.Support

Director – Mark Springer, CAPT, USN
Deputy Director – Gail McLeod, DAFC, IA-04
Managing Editors – Gary Gardner, Contractor and
Dave Swartwood, Contractor

Raising a Purple Dragon: Evolution of OPSEC Support to the Joint Community: Continued from page 1

The ability to provide this level of support, of course, has grown immensely in the past seven years. Although the JIOWC has provided limited OPSEC support, as a core capability of Information Operations for years, the foundation of the current JIOWC/OS was born out of the renewed awareness of the need to protect critical unclassified information brought out of the tragic events of September 11, 2001, and verified by documents such as the Manchester Document. In 2004, as a result of the intelligence findings of these events, and based on a 2002 Program Decision Memorandum, the JIOWC (then the Joint Information Operations Center) participated in the Defense Planning Guidance (DPG) FY 04 OPSEC Working Group, which directed ASD (C3I), in conjunction with the Combined Joint Chiefs of Staff, to improve OPSEC practices throughout DOD. Resulting from this decision process was the formation of an OPSEC Support Element (OSE) for the joint community, which became the JIOWC's Joint OPSEC Support Element (JOSE), under USSTRATCOM.

The JOSE, working closely with the Interagency OPSEC Support Staff (IOSS), the US government lead for OPSEC, and the Services, quickly attacked its new mission and leaned forward to support the war fighter's OPSEC needs while studying, developing, and adopting the best possible techniques, tactics and procedures to improve the joint community's OPSEC posture. Within the first year, the JOSE was providing fulltime forward deployed OPSEC planners to support the fight in Iraq, where OPSEC inputs helped increase mission effectiveness and reduce losses. By taking the approach it is more important to "teach a man to fish…" the JOSE was providing training and surveying forces about to deploy, as well as assisting standing Joint headquarters to build and improve their OPSEC programs.

While building and creating dynamic OPSEC programs became the initial focus of the JOSE, the world continued to evolve and so did the JOSE, including a name change to the Joint OPSEC Support Center (JOSC) in 2006 as a JIOWC Center. Continuing its effort to improve the OPSEC posture, the JOSC looked for avenues to attack OPSEC vulnerabilities based on the real world environment. Initiatives included working with Allies and Coalition partner nations to take OPSEC into the combined world. Countries that have benefited from these JOSE OPSEC initiatives include the United Kingdom, Korea, Japan, Canada, and Columbia.

Another area where the JOSE proved the value of OPSEC was in the Cyber world. Working closely with USSTRATCOM in their UCP role as Cyber guardians, the JOSE brought another avenue of approach to defend against Cyber vulnerabilities. In addition to the "high tech" technical side such as firewall, software patches, etc., the JOSE took the basic "low tech" approach, applying OPSEC principles to the Cyber arena, resulting in a DOD-wide USSTRATCOM FRAGO on how to protect critical Information in 2008.

The JOSE, again working closely with the IOSS, and the Service OSEs, has had great success in building up the core OPSEC backbone among the Joint commands. Where in the beginning, OPSEC might have been a program "in a binder on a shelf", managed as a collateral duty, joint commands have evolved to where the OPSEC Program Manager is now, in many cases, a full time position, and a key part of Information Operations planning, improving the IO capabilities of those commands. Where once the JOSE may have stepped in to provide OPSEC planning to the commands during a crisis or real world event--the commands are now better prepared to help themselves as a result of the OPSEC training, mentoring, and assistance we and others have provided over the years. Of course the JIOWC/OS always is available to assist if needed.

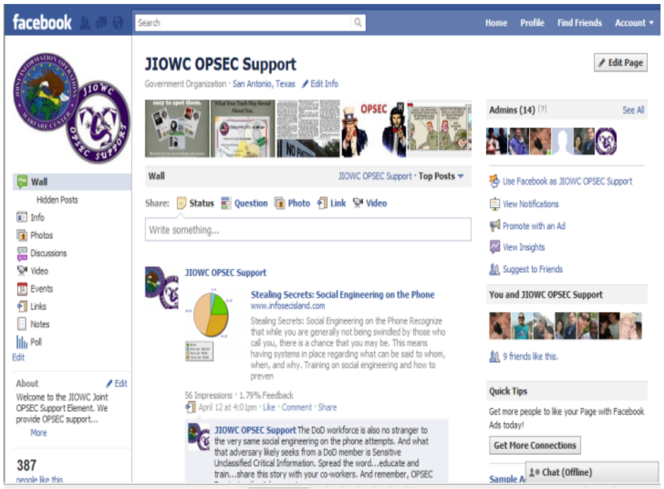
Although the joint community has had great growth in the application of OPSEC, the current JIOWC/OS directorate's work is not complete. Evolving again, the JIOWC/OS will be moving under the Joint Staff and continuing to use the name Joint OPSEC Support Element (JOSE). Under this name, the JOSE will continue to provide the same services as directed in DOD 5202.05 to support the joint war fighter as a JIOWC directorate.

Continued on page 3

Raising a Purple Dragon: Evolution of OPSEC Support to the Joint Community: *Continued from page 2*

Although OPSEC practices across DOD have increased, so has the OPSEC threat from our adversaries. The growth, ease of use, and speed of Social Media has created new vulnerabilities that our adversaries will exploit. Whether it is another WikiLeaks situation or a well intentioned but unaware Facebook posting, critical unclassified information can be lost to the enemy in the click of a mouse. The JIOWC JOSE is leaning forward, with the OPSEC community, to develop solutions to prevent the enemy from being able to collect information and use it to act against us.

Looking towards the future, while continuing to improve OPSEC programs, the JOSE strives to evolve towards "operationalizing" OPSEC to make it a mission effectiveness multiplier. By integrating OPSEC into planning for operations, and incorporating its principles and actual application into Joint exercises based on real world lessons learned from the OPSEC survey process – we have the right formula for making this an operational success.



About

Welcome to the JIOWC Joint OPSEC Support Element. We provide OPSEC support...

More

387 people like this

JIOWC OPSEC Support

Stealing Secrets: Social Engineering on the Phone
www.infosecisland.com

Stealing Secrets: Social Engineering on the Phone Recognize that while you are generally not being swindled by those who call you, there is a chance that you may be. This means having systems in place regarding what can be said to whom, when, and why. Training on social engineering and how to preven

56 Impressions · 1.79% Feedback
April 12 at 4:01pm · Like · Comment · Share

JIOWC OPSEC Support The DoD workforce is also no stranger to the very same social engineering on the phone attempts. And what that adversary likely seeks from a DoD member is Sensitive Unclassified Critical Information. Spread the word...educate and train...share this story with your co-workers. And remember, OPSEC

Get more people to like your Page with Facebook Ads today!

Visit the JOSE at: http//www.facebook.com/JIOWC.OPSEC.Support

Another city...another survey....

By: Phillip Pierce

Another city…another survey….another assessment….another planning conference…. What town are we in again? You know, when I signed on for this job, I was told the OPSEC team would put you on the road as much as a professional sports team. Let's do the math: You're basically away from the house for ten days to two weeks per month. Yeah, I would say that's a proper comparison. We save lives though, and last I checked the Boston Red Sox don't go to Afghanistan like some of my fellow OPSECers have already done (too many names to mention). Anyway I'm looking forward to doing this assessment at this Combatant Command (COCOM). I like the nightlife in this city.

Continued on page 8

Your Facebook Profile… That You Didn't Create!

By: Dave Swartwood

Does your organization have a Facebook page? How about you personally? Maybe your unit Commander or Director uses one. No? Are you absolutely sure? What if one exists that you did not create or authorize?

While many individuals and organizations have decided to embrace social networking sites such as Facebook, many have opted not to establish an online presence using these sites. The decision to not create a Facebook account is often based on many factors; security implications, not enough time or other resources, unfamiliar with how to create or maintain an account, or sometimes it is as simple as not seeing the benefits of using Facebook. If you do or don't, hopefully your decision has been carefully made by the right individual or sections within your organization (i.e., OPSEC Manager, security, public affairs, leadership, etc).

If you have chosen to not create a Facebook account, does that mean you, or your organization, does not have one?

Continued on page 6

7 Habits of Highly Effective OPSEC Program Managers

By: Gail McLeod

Just as there are common habits that lead to personal and professional success, as defined in Stephen R. Covey's book, *The 7 Habits of Highly Effective People®*, I believe there are 7 habits that if actively practiced by an OPSEC program manager, will lead to a successful OPSEC program. These 7 habits are:

1. Work the Program.

Become familiar with applicable OPSEC policy and guidance that applies to you and your organization and implement it. Learn the requirements for a sound OPSEC program, as described in OPSE 2500, and then execute actions within your organization to meet those requirements. If you haven't taken OPSE 2500, take it now and learn it well enough to teach it. Visit the Interagency OPSEC Support Staff (IOSS) web site and register for OPSE 2500 or other OPSEC courses at: https://www.iad.gov/ioss/index.cfm.

2. Be Proactive.

Seek out opportunities to improve education and awareness in your organization. You need to remind people why they need to practice good OPSEC now – don't wait until someone posts critical information on the internet to teach people what NOT to do. Being reactive in the world of OPSEC just doesn't work – you can't put the cat back in the bag -- we all must be proactive in order to protect plans, missions and lives.

3. Think Creatively.

People remember things and events that are interesting, funny, unusual, and sometimes just plain odd. Capitalize on that and initiate something that will create a common OPSEC interest in your unit – perhaps, an OPSEC mascot that shows up at Commanders' Calls and special events to extol the OPSEC message. Maybe a monthly one-page newsletter that highlights current OPSEC issues and offers solutions to common vulnerabilities. You know your organization and should be looking for creative ways to best inject OPSEC into its "way of life."

4. Practice what you preach.

Don't just talk OPSEC, practice it; and if you see others practicing good OPSEC, praise them in public (maybe via a Commander's Call or that newsletter you are now publishing.) Institutionalize OPSEC within your unit; include it in all aspects of planning; make it a part of your culture. The more you "practice" the OPSEC 5-part process, the more proficient you'll become at applying it.

5. Get Involved.

Make sure your constituents know who you are. Be visible; be in front; lead the charge. When you hear about new projects or operations that are kicking off, ensure that OPSEC is incorporated. Make sure that if there is an OPSEC question in your unit, people know who they can go to for advice, answers and support---YOU!

6. Be a Role Model for Others.

You need to be a role model for your Working Group members and your coordinators. If you are not doing it right, neither will they. Make sure that they see you in action and they have access to the policy, procedures, and tools they need to do their job. This is your opportunity to mentor others and create a strong pool of OPSEC advocates within your organization and location.

7. Engage Yourself and the Community.

Don't be an island unto yourself. Share what you know; and learn what you don't. Strive to be an OPSEC subject matter expert (either as a generalist or niche specialist) and share that expertise within the OPSEC community. Hone your skills by becoming certified as an adjunct faculty for the OPSE 2500 and/or joining a professional OPSEC association. If you have an OPSEC specialty or area of interest, brief it at various OPSEC venues or submit it to our newsletter for publication. Correspond and interact with other OPSEC professionals to include the IOSS, the Joint OPSEC Support Element (us!) and the service OSEs. Get added to OPSEC e-mail distribution lists and seek out opportunities to interact with the community; attend the annual National OPSEC conference coming up May 16th – weather permitting! Embrace your craft!

The bottom line is that great OPSEC programs don't just happen; people--specifically OPSEC program manager people--make them happen. Hopefully, by focusing on and applying some of these 7 habits, you will be able to improve your OPSEC program, making a difference in your organization by effectively protecting your plans, mission, and lives!

UPCOMING Joint OPSEC Support Element (JOSE) Hosted

OPSEC TRAINING

OPSEC Analysis and Program Management Course (OPSE 2500)

The focus of this course is on the basic skills and knowledge needed to conduct an OPSEC risk analysis (apply the five parts) 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 own organizations and activities;
(2) Identify sources of information and support materials for OPSEC practitioners;
(3) Conduct an OPSEC analysis of a program, activity or operation;
(4) Market an OPSEC program;
(5) Write 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-1300) or equivalent

Upcoming Course Dates & Locations:

6-10 Jun 2011, Huntsville, AL

6-10 Jun 2011, Miami, FL

14-17 Jun 2011, Ramstein, Germany

20-24 Jun 2011, Peterson AFB, CO

11-15 Jul 2011, San Antonio, TX

18-22 Jul 2011, Elmendorf AFB, AK

8-12 Aug 2011, Grafenwoehr, Germany

9-12 Aug 2011, Yokota AB, Japan

16-19 Aug 2011, Misawa AB, Japan

22-26 Aug 2011, San Antonio, TX

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

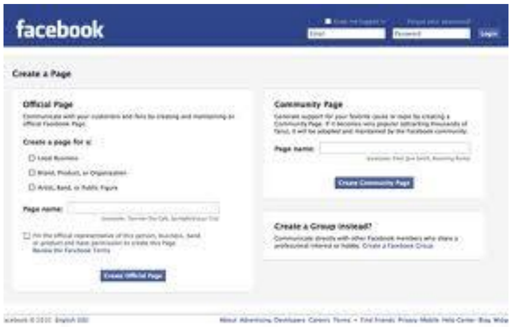
Facebook Profile: Continued from page 3

Increasingly, the answer may surprise you. In April 2010, Facebook released their Community Pages feature. Per Facebook Community Page developer Alex Wi on his Facebook Blog, “Community Pages are a new type of Facebook Page dedicated to a topic or experience that is owned collectively by the community connected to it. Just like official Pages for businesses, organizations and public figures, Community Pages let you connect with others who share similar interests and experiences.” Facebook’s Help Center further describes Community Pages as allowing people to …“learn more about a topic or an experience—whether it's cooking or learning a new language—and see what your friends and others in the Facebook community are saying about this topic.” Per Facebook, “our long-term goal is to make them the best collection of shared knowledge on a topic. We're starting by showing Wikipedia information, but we're also looking for people who are passionate about any of these topics to sign up to contribute to the Page.” As of April 2010, Facebook has generated over 6.5 million Community Pages – many auto-generated by information originally posted to the Wikipedia website.

“Open source research is a favorite method of obtaining your critical information and the amount of sensitive DoD information posted online is disturbing.”

What does this Wikipedia-Facebook relationship mean to you and your Command? During several recent OPSEC surveys conducted by the Joint OPSEC Support Element (JOSE), we’ve discovered the answer is simple: you may have a Facebook profile whether you want one or not. If you don’t control your profile, then who does, and what are they posting?

In recent months, our OPSEC surveys have identified multiple individual and organization Facebook accounts created as Community Pages. These pages have included detailed information, (including personal family details) concerning General Officers and critical mission information of DoD units. These pages are linked back to the original Wikipedia posting and can be created by anyone with a desire to share such information, whether accurate or not. For those unfamiliar with Wikipedia, individuals from around the globe can create, read, and edit topics of their choosing. If you have never searched Wikipedia for information on your organization, yourself, or your assigned personnel, you’re missing a significant opportunity to learn what information exists for possible adversaries to gain and exploit. According to Wikipedia, over 17 million articles written in dozens of languages currently exist on their website. If a topic doesn’t exist on Wikipedia or Facebook Community Pages, users are encouraged to create one and share it with the global community.



So again, I ask you; do you or your organization have a Facebook profile? I think it’s safe to assume your adversaries know the answer. Open source research is a favorite method of obtaining your critical information and the amount of sensitive DoD information posted online is disturbing. Under-estimating someone’s desire to become an “expert” on your organization and create one of these pages is a serious vulnerability to your OPSEC program. Maybe the information they share is sensitive, maybe even classified. How about if it’s simply false and spreads untrue and damaging information about your unit or leadership?

Whether or not you’ve embraced the social networking revolution yourself as an individual or a DoD entity, you need to be aware of what information exists in open sources. I am not advocating every organization create a Facebook or other SNS profile, but it is important to understand that if you don’t, someone else may… and you may not like what they have to say.

Social Media Security Considerations:

- Use Common Sense
- Don't divulge classified, For Official Use Only (FOUO), or sensitive materials, photos or videos
- Always Think OPSEC
- Be aware of the image you present when posting. Remember, once posted, you can't retract
- Limit usage of social media to personal use only, do not write about work issues, always assume that everyone in the world is able to see what you write
- Keep anti-virus software updated, run it regularly
- Be cautious of how much Personally Identifiable Information (PII) you disclose (employment organization and location, home address, home and business email addresses, birth date, family members and pet names, phone numbers, social security numbers, photos, your schedule or routines, vacations, TDYs, day trips, and shopping places)
- Don't assume you are in a trusted environment
- Review your social media platforms' privacy settings, understand what information is collected and shared (pay attention to the site's privacy policies and terms) Default privacy settings are not private (set on high security)
- Avoid online games or quizzes that require you to provide personal information
- Adhere to secure password guidelines (don't use same password for multiple social media sites and definitely not ones used at work)
- Exhibit caution in downloading third party applications
- Log off when you are finished
- Keep up with latest social media scams
- Google/Bing your name and check what information on you is online
- Deactivate location-based (Geotags) including Smartphone
- Do not log on to social media from public computers (internet cafes)
- Always be skeptical and wary if someone asks to be your friend on social media
- Do not automatically trust that posts are from who they claim they are from…

Another City: Continued from page 3

Another city…another survey…Now I don’t want to sound too pessimistic but I gotta tell ya…some of the places we’ve visited are lacking some serious OPSEC discipline. Some units had no Critical Information Lists (CILs); some didn’t even know what a CIL is. Some of the most seasoned warriors couldn’t even tell me some of the publications that lead you to a better OPSEC understanding. Most of these warriors, God bless ‘em, are spot on with putting bullets on the target, but many of them didn’t seem to place enough emphasis on OPSEC. Many of the places I visited said they haven’t had a living breathing human being give OPSEC training in over five years. Instead, everybody received the cold, impersonal power point presentation. Now, for all you power point rangers, I’m not saying that power point is a bad thing. If used properly, it can greatly enhance your OPSEC program. However, it shouldn’t **dominate** your program.

“Some units had no Critical Information Lists (CILs); some didn’t even know what a CIL is.”

Another city…another survey…I digress; anyway, the OPSEC team arrived at 1300. As everybody headed to the rental, the usual cracks and putdowns, indicative of a good team, started to fly. Once we arrived, we instantly met the OPSEC point of contact who immediately took us on a tour of the headquarters building. Once inside, I noticed immediately that this might be a different trip. Every room we went to you constantly heard the crisp sound of “Phones up….Phones down”. At first I thought the troops were doing this for show…but then I thought nobody else does it for show when we arrive. In fact they don’t do it for **real** whenever we arrive for a survey.

Another city…another survey…It wasn’t for show. This unit was for real. During the OPSEC surveys, 90% of the troops we talked to had a strong understanding of OPSEC and how to apply it. All personnel received an OPSEC briefing EVERY SIX MONTHS. Not a power point brief, mind you, but a lively, energetic OPSEC professional briefing at commander’s call. Most of the personnel even **knew** what the Purple Dragon stood for. Each J unit had an energetic point of contact. Garbage cans were virtually empty…why? Because trash was shredded. As I sat down to talk to the troops, each and every one of them knew who the OPSEC Program Manager was. Not only did they know him, but they were able to point to their critical information list **posted at every desk**. After the last interview, I walked the hallways of the headquarters in disbelief. “Can a headquarters element be this good at OPSEC?” I thought. The answer hit me like a slap in the face as I walked by dozens of original OPSEC posters strategically posted for all to see. I stood there absolutely stunned by the recent string of events when I heard a voice from up above “Pierce…get back to work…I need a note taker for the commander’s interview”. It was CDR Durdin. Never was one for small talk.

It was another city…but it was **not** just another survey. It didn’t take long to see why. As we interviewed the head honcho of the headquarters, he was actually disappointed that only 90% of his troops had a strong understanding of OPSEC. He was concerned about the remaining 10%. This Colonel sat at every OPSEC team meeting. This Colonel sent his program manager to various OPSEC schools to make her a well rounded OPSEC professional. This Colonel understood “Mission and People first” but in order to take care of both, you have to instill a strong OPSEC culture within your organization. He understood that the strength of the program has to start with the leadership. We said our goodbye’s and passed on our praises. As we walked away, CDR Durdin patted me on the shoulder. “Is this a sign of kindness from the man?” I thought. He looked at me and said “Change in the game plan…you’re replacing Mike in the next survey…pack your bags now Pierce.”

Thank you Commander may I have another…another city….another survey.

Protecting Sensitive Emails (OPSEC)

By: Aaron DeVaughn

Be the strongest link and think Operations Security (OPSEC) when sending sensitive emails on unclassified DoD networks. Did you know encrypting e-mails is an effective OPSEC measure to protect e-mails from being read by unintended recipients? It's a known fact that business conducted on DoD networks provides opportunities for sensitive information to be read and compromised when not encrypted.

You can identify what sensitive unclassified information requires protection by reviewing your organization's and higher headquarters' OPSEC critical information lists (CIL). From an OPSEC perspective, critical information is defined as information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities, or limitations an adversary seeks in order to gain military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly resources or cause loss of life. If you have not been trained or are not aware of this important document, contact your organization's OPSEC point of contact.

Encrypting emails is not new to the DoD. The policies apply to all unclassified email sent from DoD-owned, operated or controlled systems or accounts to include desktops, laptops, and personal electronic devices such as BlackBerry devices. OPSEC surveys conducted by the Joint OPSEC Support Element found when personnel failed to encrypt emails, they usually fell into one of three categories: Individuals did not configure the computer device they were using to send encrypted emails, personnel did not know what to encrypt, and personnel did not know how to encrypt. All of these situations can be corrected by commanders and directors with the help of their OPSEC POC and IT staff:

First. Get involved and make an active effort to ensure your organization's computer devices used to send sensitive emails are properly configured to encrypt emails. In addition, ensure all personnel publish their PKI certificates to the Global Address List (GAL).

Second. Ensure personnel are trained on what to encrypt and made aware of your higher headquarters and your organization's critical information list. Remember, if personnel encrypt every e-mail message, then this can have an equally damaging effect by increasing the bandwidth across DoD networks.

In addition to being aware of your higher headquarters and organization's critical information list, also include in training and awareness, the need for personnel to encrypt:

- Controlled Unclassified Information (CUI) such as:
    - Information potentially exempt from disclosure under the Freedom of Information Act (FOIA) that is marked For Official Use Only (FOUO)
    - Personally Identifiable Information (PII) protected by the Privacy Act
    - Individual's health information that is protected under the Health Insurance Portability Accountability Act (HIPAA)
- Other Sensitive information
    - Unclassified Technical Data
    - Sensitive Acquisition Information
    - Proprietary Information
    - Drug Enforcement Agency (DEA) Sensitive Information
    - Antiterrorism/Force Protection Information

Protecting Sensitive Emails (OPSEC): Continued from page 9

Third. Personnel must be trained on how to encrypt sensitive unclassified emails. Incorporate encryption training in initial, annual and recurring OPSEC training.

"Ensure personnel are trained on what to encrypt and made aware of your higher headquarters and your organization's critical information list."

An excellent source for additional training for personnel to know how to encrypt emails can be found at: http://iase.disa.mil/eta/using_pki/launchpage (*Using PKI Certificates*).

In this information age, we must control and safeguard our sensitive and critical information to maintain our advantage over our adversaries. When we fail to protect this information, we are the weakest link in protecting our own, others, and our command's critical information. The ultimate goal of OPSEC is increased mission effectiveness. To prevent our adversaries from gaining access to critical information, you must be the strongest link and encrypt sensitive e-mails. If you would not hand your sensitive e-mails to the enemy, don't send them unencrypted. Think OPSEC!

Additional info on OPSEC and encrypting emails can be found at: http://iase.disa.mil/pki-pke/ and http://www.facebook.com /JIOWC.OPSEC.Support

Purple Dragon Call for Article

The Purple Dragon welcomes your articles regarding all aspects of OPSEC. Please submit your articles in Microsoft Word format, version 6.0 and higher, doubled-spaced in 12-point, Times New Roman font. Email unclassified submissions to: jiowc.jose@us.af.mil. All articles should be security/OPSEC screened and released by the author's parent command/agency/organization prior to submission.

"We"...Have Lost Control

By: George Allen

The premise behind this paper is to bring to light what "We" have freely given away for many years. Not out of stupidity, but due to ignorance that now has the attention of a growing minority. "We" have used a worthy process throughout life as a means to protect our daily routine, evaluate outcomes and guide decisions that impact our lives. Yet, in the wake of this 21st century, it would benefit many to go back to more similar times and retake and protect what we now offer without conscious thought.

"We" are a culture that takes advantage of our prowess, thinking that nothing I say or do can be used against me. A nation of people that too often forget that the slightest bit of who I am, what I do, and / or who I work for – can be used against me. Not that "We" might offer such information in one setting or scribble down Personally Identifiable Information (PII) and post it on a bulletin board – No one I know would do such a thing. Yet, it happens. Not in such literal terms, but I've collected it from many people, places and organizations over the world.

Frankly, it's my job. Here at the Joint Information Operations Warfare Center (JIOWC) / Joint OPSEC Support Element (JOSE), "We" are working to bring about an awareness that many have degraded in the name of freedom…of speech, action, protection, etc; When OPSEC requires each of us to protect those valuable pieces of unclassified information that when once put together, would allow an adversary access to information "We" must control. The question remains, what has history taught us? From countless wars, used as teaching tools to remind us of what not to do; to moments of terrorist acts that "We" cannot forget…"We" are trapped in a culture that leads to complacency, which hinders our protection of

"We …Have Lost Control: Continued from page 10

information during everyday life. Not that we should be terrified in public or question our freedom of movement, just conscious of our surroundings. And vigilant in our methods of correspondence and handling of what has been entrusted to our safe keeping.

"We cannot forget… 'We' are trapped in a culture that leads to complacency, which hinders our protection of information during everyday life."

Our job as a directorate is to assist, assess, and evaluate DoD Services and Agencies around the world in how they are handling unclassified, but sensitive information. Once done, each leader will ask the question: "How do we fare against the others in our OPSEC posture?" A valid question that has yet to change our response, "Your organization has the same concerns / issues that we have observed in others." What does that response tell our leadership? "We" have lost control, more importantly, how do "We" move forward in changing a cultural attitude about protecting unclassified, but sensitive information.

The most prevalent misunderstanding encountered during our assessments or surveys is that we are here to evaluate how the organization is protecting classified information. Hence, the lack of training and awareness with respect to OPSEC. The JOSE is not an arm of the Inspector General but works to develop OPSEC Programs that will promulgate a necessary change in how "We" do handle and disseminate unclassified information. A foundational discovery in Manchester England gave us insight to a terrorist's methodology of collecting intelligence; over three quarters (80%) of intelligence gathered on a "target" is given to a terrorist via open source. Yes, "We" give it away….piece-by-piece.

It's not that information "We" continually classify according to DoD guidance and keep locked inside a Sensitive Compartmentalized Information Facility (SCIF). Since "We" protect classified so well, many are driven to tell others openly what they do, write it down in letters, make videos of sensitive operations, blog on SNS, etc; And in the end, "We" lose control. Not realizing who we are talking to and what small "piece" of the puzzle has been given away today, that when aggregated tomorrow, puts a soldier, sailor, marine or airman's life in jeopardy. The adversary is in no hurry, unlike us. "He" will wait until enough of what has been discovered openly paints an adequate picture for him / her to meet what is an undesirable outcome for us.

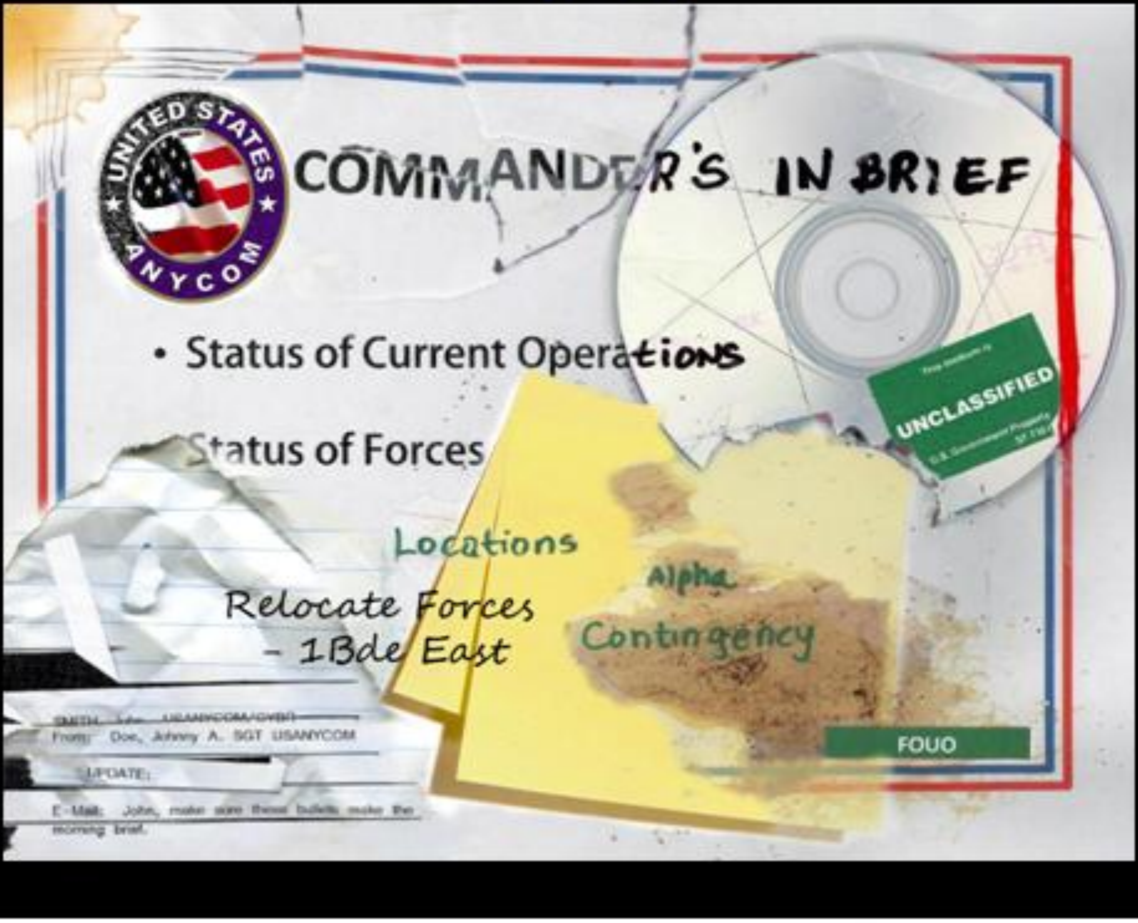
What needs to be given attention will only come from the highest levels within our services and agencies. JOSE emphasizes that OPSEC is a Commander's Program and without buy-in at that level, change is not possible. It's our job here in the OPSEC Support Directorate to take this mission we hold dear and convey its reality to responsible leadership. More than that, to continue to assess, survey and train designated Program Managers to ensure protection of unclassified information remains consistent over time. "We" know that it didn't take a day for us to lose control and it will take emphasis to change a cultural attitude.

How do we get there, from here? The technical leaps made in computer technology has offered the right hardware / software to combat an adversary's ability to extract information communicated via computer networks. "We" lose our advantage when failing to encrypt unclassified information that has been deem critical to the organization. Additionally, the simplicity of changing outdated telephone receivers to push-to-talk ones or practicing "phone-up" alert prior to answering calls…will enhance protective measures. "We" would not experience any further incidents that would lead to the highest levels in DoD mandating the lockdown of computer ports throughout the force. "We" can change our OPSEC posture at the lowest levels and begin to reshape cultural attitudes from the bottom – up.

Our mission to save lives has long been viewed as an additional duty. Here in the JOSE…OPSEC IS HOT! And what we do to point out what has been "lost" opens the eyes of Commanders at the end of the day. We have taken strip-shredded trash, put it together and are able to tell them the who, what, where, when and how of their last trip. If that's what it takes to protect those in the foxholes, our efforts will not be in vain.

What JOSE is mandated to educate and teach across DoD is that "We" are our own worst enemy. Now that we have seen the enemy, let us change the way he / she approaches how we protect unclassified, but sensitive information.

YOU WOULD BE SURPRISED WHAT YOUR TRASH REVEALS ABOUT YOU.



IMPROPERLY DISPOSING OF TRASH TO INCLUDE DIGITAL MEDIA, STRIP SHREDDING, POST-IT® AND HANDWRITTEN NOTES MAY GIVE ADVERSARIES DIRECT INSIGHT INTO YOUR OPERATIONS.

JOINT OPSEC SUPPORT ELEMENT (JOSE)
jiowc.jose@us.af.mil
JOINT INFORMATION OPERATIONS
WARFARE CENTER
http://www.facebook.com/JIOWC.OPSEC.Support
DSN: 312-969-5650 Comm: (210) 977-5650