The Purple Dragon

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

From the Dragon's Mouth

Comments from the Chief, JIOWC OPSEC Support Division

Donald P. Taylor, Jr
COL, USA

No Change in OPSEC Support

On 1 October 2011, the Joint Information Operations Warfare Center (JIOWC) was realigned from U.S. Strategic Command to Joint Staff, Director for Operations (J-3), as a Chairman's Controlled Activity.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5125.01, *Charter of the Joint Information Operations Warfare Center*, 1 Sep 2011, outlines the Joint Staff's proponency for Information Operations, to include the individual capability of OPSEC. To execute the Joint IO mission, the CJCSI further designated the JIOWC to support the Joint Staff in this effort. So what does this mean to you whom the JIOWC has supported with OPSEC in the past? The answer is twofold.

First, the JIOWC continues the Joint OPSEC Support Element (JOSE) mission to support Combatant Commands and Joint Forces Commanders with planning, exercise support, program development, training and surveys.

Second**,** the request for support (RFS) process has changed. Send your RFS directly to the JOSE via SIPRNET (OS_STAFF@jiowc. smil.mil) or via NIPRNET (jiowc.jose@us.af.mil). If your organization is subordinate to a Combatant Command, route the RFS through the Command OPSEC Program Manager. Service organizations please contact your Service OPSEC Support Element or staff proponent. For more information about the RFS process, visit our SIPRNET website at http://www.intelink-sgov/sites/jiowc/Divisions/OS/default.aspx or send an email.

As we enter this new era of fiscal constraints, the JOSE will work with our customers to maximize support but we need your help in forecasting requirements. Please get your RFS' in early.

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) 977-5192 DSN 969-5192
http://www.facebook.com/JIOWC.OPSEC.Support

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

Social Networking Sites and OPSEC

Social Networking Sites (SNS) are a great way to stay connected with family and friends, collaborate and network. However, SNS sites can also provide adversaries with sensitive information they need to disrupt your mission or to do harm to yourself, coworkers or even your family. Here are some tips to help practice good OPSEC on SNS sites:

- Know your organization's Critical Information List to know what not to post
- Educate family members on the risks of SNS
- Be suspicious! People are not always who they say they are
- Verify "real" friends
- Lock down your profile/make it private
- Review information and photos before posting to include metadata
- Be aware of what your family and friends are posting to ensure you're not giving sensitive information directly to the "bad guy". Remember, data aggregated from different sources could reveal sensitive information when pieced together
- Incorporate protecting OPSEC sensitive information into SNS awareness and training

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

Adversary's Corner

(As a new feature in our Purple Dragon newsletters, we turn to our adversaries to provide their thoughts and opinions on American OPSEC.)

Thank You!

Greetings American military partners. I just wanted to take this opportunity to send a quick "THANK YOU" for all of your assistance these past few months. Without you, my associates and I would have been unable to successfully obtain the required information on your new technology – months before it is deployed! With your help, we have been able to acquire enough sensitive information to develop our own countermeasures and tactics to defeat America's newest weapon system.

Throwing your sensitive papers and notes in the trash, discussing the sensitive capabilities at restaurants, and on social networking sites…you've made our job so much easier. You have become a great asset to our successful collection operations. You may have asked yourself why I have referred to you as "my American military partners." Well, it's simple: If you continue to ignore your own OPSEC and traditional security measures… you are an active and helpful "partner" to our terrorist organization. And for that, we thank you!

Signed,
Your Terrorist Partner

HOW TO RECOVER
YOUR OLD E-MAIL ENCRYPTION KEYS

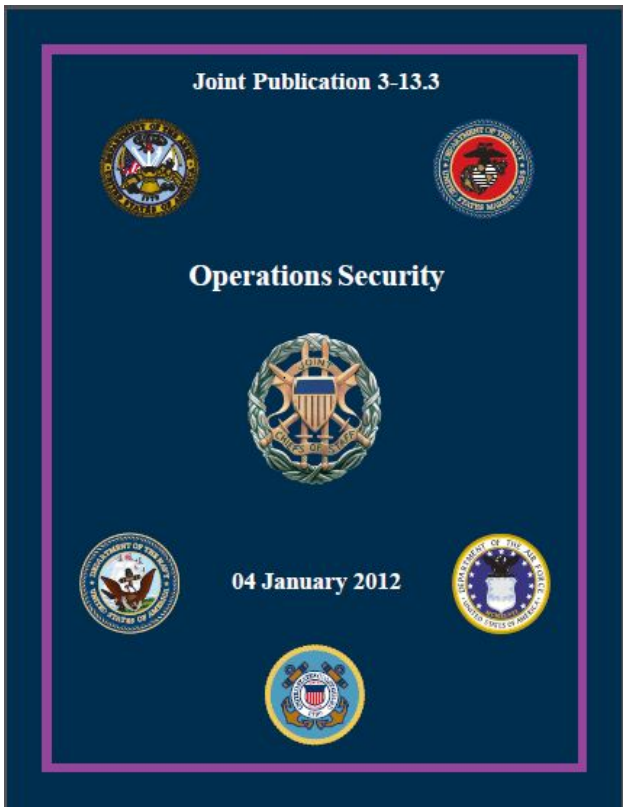
Encrypted e-mails received can only be opened with your private encryption key. When your CAC is replaced, previously encrypted e-mails can no longer be accessed. Previously encrypted e-mail can only be opened using the previous CAC encryption certificates.

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

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

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

New Joint Pub 3-13.3, Operations Security



New Joint Publication 3-13.3., Operations Security has hit the street and can be found at https://jdeis.js.mil/jdeis/new_pubs/jp3_13_3.pdf. The following are some of the changes:

• Restructured document format, removing key sections from appendixes and placing them within appropriate chapters.

• Added figure providing examples of critical information during threat analysis in the operations security (OPSEC) process.

• Increased the components of OPSEC risk assessment to three by adding a second step in which the commander and staff estimate the impact on operations associated with implementing each possible OPSEC countermeasure.

• Added section on joint and interagency planning during OPSEC planning.

• Added a section on intergovernmental and nongovernmental organization considerations during OPSEC planning.

• Redefined the terminology for OPSEC assessments: Changed the OPSEC command assessment to an OPSEC assessment and OPSEC formal assessment to an OPSEC survey.

• Stated the requirement for an OPSEC assessment to be conducted annually, while an OPSEC survey will be conducted every three years.

• Added additional OPSEC countermeasures: physical attack and electronic warfare as an operational and logistic measure, awareness of OPSEC vulnerabilities presented by online social networking, and shredding of documents as administrative measures.

• Added a new appendix, "Sample Operations Plan."

• Updated references and acronyms.

Factors that must be considered when performing OPSEC planning:

• OPSEC planning guidance should be provided as part of the commander's planning guidance.

• OPSEC is an operations function, not a security function.

• OPSEC should be integrated into the IO cell.

• OPSEC planning should focus on identifying and protecting critical information.

OPSEC Publications

✓ Joint Pub 3-13.3, Operations Security, 4 Jan 12
✓ CJCSI 3213.01C, Joint Operations Security, 17 Jul 08 *
✓ DoDD 5205.02, Operations Security, 6 Mar 06 *
✓ DoDM 5205.02, DoD Operations Security Program Manual, 3 Nov 08
✓ AR 530-1, Operations Security, 19 Apr 07 (USA)
✓ MCO 3070.2, Marine Corps Operations Security Program, 18 May 07 (USMC)
✓ OPNAVINST 3432.1A, Operations Security, 4 Aug 11 (USN)
✓ AFI 10-701, Operations Security, 8 Jun 11 (USAF)

** Note: Currently being reviewed and updated*

Operations Security (OPSEC)
Observations and Recommendations

Below are some common findings noted during OPSEC assessments and surveys:

OPSEC awareness training generic, not localized

- Training found to be generic and not localized
- Training did not incorporate CIL understanding or applicable countermeasures
- Command written OPSEC guidance was not incorporated into initial, annual or periodic OPSEC awareness training
- Threat not addressed in training materials

Recommendations

- Incorporate local OPSEC awareness training into overall training program
- Train workforce on how to and what to protect locally
- Incorporate higher headquarters and organization's written OPSEC guidance into *awareness* tra*ining material*

Personnel unaware of the organization or higher headquarters Critical Information List (CIL)

- CIL not created
- CIL not easily accessible
- CIL training not included in the initial, annual, or periodic OPSEC awareness training

Recommendations

- Develop means for personnel to reference CIL e.g. desk card, intranet, "OPSEC" share drive, desktop shortcut icon, and/or screen saver.
- Train personnel how to apply the CIL to their day-to-day operations and protect information at their level

OPSEC training did not include contractors nor was it tailored for duty positions requiring additional training

Recommendations

- Monitor and track OPSEC training for all personnel who work with or have knowledge of sensitive and critical information that requires additional protection (Civilians, Contractors, Military, Reservists)
- Provide tailored OPSEC training for specific duty positions i.e. Anti-terrorism/Force Protection Officer, Public Affairs Officer, Information Manager, Web Master

OPSEC policies not developed, current, enforced, or disseminated

- Nonexistent or continually in "draft"
- Outdated or no periodic review
- Not assessed to ensure compliance
- Not enforced
- Countermeasures not addressed to protect critical information

Recommendations

- Create, review, and update OPSEC guidance
- Leader's must emphasize; all personnel must enforce
- Get the "Word" out (Note: OPSEC guidance in a plan, directive, instruction or any publication does no good if no one is aware of it.)

OPSEC not integrated into key functions (Anti-terrorism, Contracting, Critical Infrastructure)

Purple Dragon 4

Recommendations

- Ensure OPSEC plan is incorporated into AT plan

UPCOMING

Purple Dragon 5

JOINT OPSEC SUPPORT ELEMENT

OPSEC TRAINING

OPSEC Analysis and Program Management Course (OPSE 2500)

The focus of this course is 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 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) 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

Th rity Av

Upcoming Course Dates & Locations:

12-15 MAR 2012, OFFUTT AFB OMAHA, NE

19-22 MAR 2012, CAMP FOSTER, OKINAWA, JAPAN

26-29 MAR 2012, SAN ANTONIO, TX

10-13 APR 2012, REDSTONE ARSENAL, AL

15-18 APR 2012, MANAMA, BAHRAIN

16-19 APR 2012, USAG YONGSAN, SOUTH KOREA

1-4 MAY 2012, CAMP ARIFJAN, KUWAIT

14-17 MAY 2012 HEIDELBERG, GERMANY

11-14 JUNE 2012 CAMP SMITH, HAWAII

18-21 JUNE 2012 CJTF-HOA DJIBOUTI, AFRICA

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

If you're going to get a handle and work to reduce OPSEC disclosures, everyone in the organization must (a) understand the threat, (b) know what sensitive unclassified information

must be protected, (c) be vigilant and protect sensitive information and (d) apply OPSEC countermeasures to safeguard sensitive information.

OPSEC within an organization is only as strong as its weakest link and senior leader involvement in the program is key. An organization's OPSEC policy must apply to everybody. It does no good to educate only the military and DoD civilians and not include contractors who also handle sensitive information.

OPSEC training is for everyone, from the Commanding General to the lowest enlisted and it should include ways to reach family members. It must include all contractors and partner nations that have access to sensitive critical information. (Note: 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.

OPSEC Program Managers must focus on localizing OPSEC training for their organization and geographical area. 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 generic OPSEC awareness 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. Issue OPSEC advisories when new threats and vulnerabilities are announced and talk about appropriate countermeasures to mitigate these threats. Consider the following venues:

- ✓ Commander Calls
- ✓ Staff Meetings
- ✓ E-mail

- ✓ Your organization's intranet
- ✓ Posters
- ✓ Videos

OPSEC awareness training can reinforce command policy to protect sensitive unclassified 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 unclassified information within your organization.

Purple Dragon 7

OPSEC Fun & Games

By: Mike Goss

OPSEC Logic Problem: Critical Information

Four military members all compromised a different piece of critical information, each via a different vulnerability. Using the clues provided, can you identify each members Rank, Last Name, Vulnerability, and Critical Information compromised.

Clues:

1. The Major was not the untrained person who compromised deployment dates.

2. Jones, who is not a Staff Sergeant, took photos of his unit in the field.

3. Smith received training.

4. Lieutenant Thomas threw away something important, but not the VIP itinerary.

5. The Airman sent an unclassified E-mail, but it did not contain unit photos.

	Smith	Jones	Johnson	Thomas	Trash	Unclass Email	Lack of Training	Social Media	Alert Roster	Deployment Dates	Unit Photos	VIP Itinerary
Airman												
Staff Sergeant												
Lieutenant												
Major												
Alert Roster												
Deployment Dates												
Unit Photos												
VIP Itinerary												
Trash												
Unclass Email												
Lack of Training												
Social Media												

Rank	Name	Vulnerability	Critical Information

How to play: All the information you need to solve the problem is in the clues. When you eliminate a choice, place an X in the box. When you are sure of a choice, place a dot in the box. When you identify a correct response, you can eliminate all others from that choice. For example, below we have identified that A is 2. Therefore, 1, 3, and 4 cannot be A; likewise, B, C, and D cannot be 2.

	1	2	3	4
A	x	.	x	x
B		x		
C		x		
D		x		

The Joint OPSEC Support Element is now on YouTube!

http://www.youtube.com/user/JointOPSECSupport

Come check us out and let us know what you think!

Answers are located on page 11

Tips to Prevent OPSEC Disclosures Today

Family members play a vital role in protecting sensitive information: Our family members know 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 unclassified 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? Computer systems hold the information--servers, desktops, laptops, and external hard drives. For starters, you have mobile devices, mobile phones, and personal digital assistants. After this come other gadgets such as digital cameras and perhaps USB storage devices. 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. The actual answer is more than you thought. 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. I know the information is unclassified, but everyone does not need access to all your critical information from the web or internal network. Remove access where it makes no sense, and reduce the risk.

Identify when and how the 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? Laptops, mobile phones, thumb drives and CDs. These devices must be protected and 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 is 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. Be trained and help train the masses.

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. Place cross-cut document shredders near photo copiers and outside of meeting rooms. If using a third-party shredder, ask: Do they shred on site? 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 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.

Improve Your OPSEC Posture With Encryption Wizard

By: Aaron DeVaughn, DAFC, IA-04
Joint OPSEC Support Element

Recently, I came across an encryption tool called Encryption Wizard (EW) that is free (and approved for use on NIPRNet and SIPRNet) and can be used to protect critical information. It can significantly increase an organization's OPSEC posture at little to no cost by protecting sensitive unclassified information in transit (E-mail, FTP, or shared web folders) or at rest on a removable storage device. The program was created by the Software Protection Initiative (ATSPI) Technology Office located at Wright-Patterson Air Force Base, Dayton Ohio.

The software can be installed without installation or elevated privileges, and runs on Windows, Mac, Linux, Solaris, and other computers with Sun Java. The tool uses a simple drag-n-drop interface and offers 128-bit AES encryption, SHA-256 hashing, searchable metadata, archives, compression, secure deleting, and PKI/CAC/PIV support. Encryption Wizard is GOTS - Government invented, owned, and supported software and comes in two, fully-compatible and interoperable editions, "EW-Public" and "EW-Govt." Anyone can download EW-Public at *http://www.spi.dod.mil/ewizard.htm* and use it for free. EW-Gov is designed for US Federal Government (and contractor) computers and is accredited by the Army and Air Force for use on NIPRNet and SIPRNet.

Figure 1: Choose a Key Type

Fast, Easy-to-Use

To encrypt files or directories, simply drag them into the Encryption Wizard window, press encrypt, and enter a passphrase and/or use a PKI certificate. The software can also create encrypted (and optionally compressed) archives of files and directories.

Free Public Version

Download from spi.dod.mil.

Free FIPS Version

This restricted version uses a FIPS 140-2 validated encryption module from RSA® for use by the federal government and its contractors. Encrypted files are compatible with the public version. Escrow keys can be embedded for use in your enterprise. To obtain the FIPS version or customize for your enterprise, contact the Software Protection Initiative.

Cryptographically Strong

Encryption Wizard protects data on your network, while stored on media, and during transmission across the Internet using a FIPS 140-2 validated module. 128-bit AES encryption, SHA-256 hashes, and RSA digital signatures meet DoD requirements for transmitting and storing critical unclassified information.

Enterprise Ready

Encryption Wizard aims to protect data wherever stored and however transmitted between dissimilar networks, platforms, and operating systems for a broad range of users. Listed on the Air Force Enterprise Products List, Encryption Wizard complements Data-at-Rest products for defense-in-depth and granular control. Optional command line interface permits scripting of data protection. Installation packages available for common enterprise software distribution systems.

Encryption Wizard Use Cases

Encryption Wizard was initially developed by ATSPI as a way to send sensitive contractual information between the Government and their Small Business Innovative Research contractors. From this, two fully compatible and interoperable editions were built for both public and government use. Since then, many others have adopted Encryption Wizard as a way to send and store their sensitive information.

The Air National Guard uses Encryption Wizard for emailing EPRs, orders, alert rosters and such to/from people's home email accounts. As some have said, "when the Guard is home they're away and when deployed they're just farther away." Encryption Wizard helps keep airmen closer to their home unit.

The DoD lead in Acquisition Intelligence (AFMC/IS) uses EW-Govt on both NIPRNet and SIPRNet as an additional means of enforcing Need-to-Know policy.

Military medical groups, such a Air Force Medical Service, have used EW-Govt to protect HIPAA (private health) information.

EW-Govt complements (not replaces) commercial, full disk, transparent GSA/DoD Data-At-Rest (DAR) solutions by providing secure file sharing between multiple vendors' proprietary solutions. EW-Govt meets/exceeds 92% of the 103 applicable DAR requirements.

Many people use EW-Public at home to strongly protect their passwords lists, tax records, and other sensitive documents.

Many organizations of all types use both EW-Govt and EW-Public to share sensitive documents among themselves despite incompatible enterprise encryption solutions.

Engineers use Encryption Wizard to strongly protect and share technical documents. Analysts use Encryption Wizard to secure their findings until they are ready for release. Deployed soldiers use it within LPS-Public to share financial information with their families at home from un-trusted computers. Sailors have used it to protect and backed up personal files burned on CDs.

System Requirements

- Java Runtime Environment SE, v1.5 (or newer)
- Administrator access not required for installation

Contact Information

Software Protection Initiative
AFRL/RYT, Wright-Patterson AFB
ATSPI_outreach@wpafb.af.mil
(937) 320-9095 x150

spi.dod.mil

Logic Puzzle Answers

From Page 8

Rank	Name	Vulnerability	Critical Information
Airman	Smith	Unclass Email	VIP Itinerary
Staff Sergeant	Johnson	Lack of Training	Deployment Dates
Lieutenant	Thomas	Trash	Alert Roster
Major	Jones	Social Media	Unit Photos

Obtaining Usable Threat Information

Mr. Dave Swartwood
Joint OPSEC Support Element

"Threat is the key!" How many times have you heard this statement? If you've attended one of our Program Manager courses, I'm sure you've heard it so many times you fell asleep with it repeating in your head. Without a threat, there is no need for any security program. Of course, there is always some degree of threat in anything we do. From a robust nation-state with large resources, to the dynamic terrorist, to your local criminal element, there will likely be an adversary with both intent and capability to harm our mission or our family.

Joint Pub 3-13.3, Para 3, provides straight forward guidance on how to conduct a threat analysis. Too often we simply want someone (i.e., J2, OSI, NCIS, etc.) to hand us a simple threat report capturing all of our concerns in one package. For those who have been in the OPSEC realm for any amount of time, we know this doesn't happen. In reality, OPMs need to gather data from multiple sources and ask these questions (as outlined in JP 3-13.3):

1. Who has the intent and capability to take action against our operation?
2. What are our adversaries' goals?
3. What are our adversaries' potential courses of action?
4. What critical information does our adversary already know?
5. What are our adversaries' intelligence collection capabilities?
6. Who are our adversaries' friends that they will share information with?

During our OPSEC courses, we're often asked how to obtain usable threat information. If you are not an intelligence analyst, the world of military intelligence can seem daunting and confusing. Of course, the best answer we can give program managers is to develop a close working relationship with their intelligence directorate and the counterintelligence professionals within their organization, base or command. Working with your intel shop you can obtain existing threat summary reports or submit intelligence requests for information (RFI) specifically tailored to your OPSEC program needs.

While your relationship with your intel/counterintelligence partners can't be overstated, we've also developed a list of SIPRNet web sites that can provide you with superb intelligence products on a daily basis. If your organization uses or maintains a valuable threat resource that we haven't included, please send the JOSE an e-mail letting us know about it and we'll share it with the OPSEC community. Something else you probably heard in our OPSEC courses is your OPSEC peers are often times one of your best resources. Help us share valuable resources you've discovered to be helpful to your successful program.

List of SIPRNet Threat Links: *http://www.intelink.sgov.gov/sites/jiowc/Divisions/OS/default.aspx*

Encrypted e-mail not good as an attachment

It's a common practice to send an e-mail message to someone and include a different e-mail message as an attachment. This works fine if the attached message is unsigned and unencrypted, and even if it's digitally signed. If it's encrypted, however, the recipient will receive the following error message when trying to open the attachment: *"Your Digital ID name cannot be found by the underlying security system."* The reason is the attached message is not encrypted to the person trying to open it, so their private key cannot decrypt the message. Remember, PKI digital encryption is a writer-to-reader transaction. When a sender encrypts a message using a recipient's public key, only that recipient can decrypt the message with their corresponding private key. When an encrypted e-mail is then sent to a different recipient as an attachment, that recipient is not authorized to view it.