



INFORMATION ASSURANCE AWARENESS BRIEFING



INFORMATION ASSURANCE

References

- AR 25-2, Information Assurance, 24 Oct 2007 Rapid Action Revision 23 Mar 2009
- Data-At-Rest Protection (DAR) Better Business Practice (BBP), 12 Oct 2006
- AR 380-5, Department of the Army Information Security Program, 29 Sep 2000



Information Assurance –

The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users.

Army Information Assurance “Program” –

A unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by Army Information Systems.

So Why Are We Concerned With Vulnerabilities and Violations?

- They can be eliminated if we use good computer security practices
- Remember to practice and comply with what you have learned in the annual Information Assurance training, Acceptable Use Policy, and Internet Use Policy

ON CYBER PATROL



INFORMATION ASSURANCE ISSUES



Hardware Issues

- **Portable Devices**

- **Universal Serial Bus (USB)**

USB Storage Devices such as memory sticks are currently forbidden for use in a Government System

- **Camera Phones**

- **Wireless Network Devices**

- **Laptops**

- **Notebooks**

- **Personal Devices connected to the network**

- **Cameras**

- **Phones**

- **Personal Digital Assistants (PDA)**



Portable Devices

While USB and other portable devices improve productivity they are currently **FORBIDDEN**.

Thumb Drive



Casio Watch Camera



USB E-Pen



Video Devices



Audio Recorders with USB connectivity



- These devices are...

- **Plug and Play:** *Generally don't need additional software to use*
- **Small:** *Convenient to carry around*
- **Large Storage Capacity:** *Some can store more data than a CD.*
- **Easily Lost or Stolen:** *Easy to misplace or conceal*

Wireless Network Devices

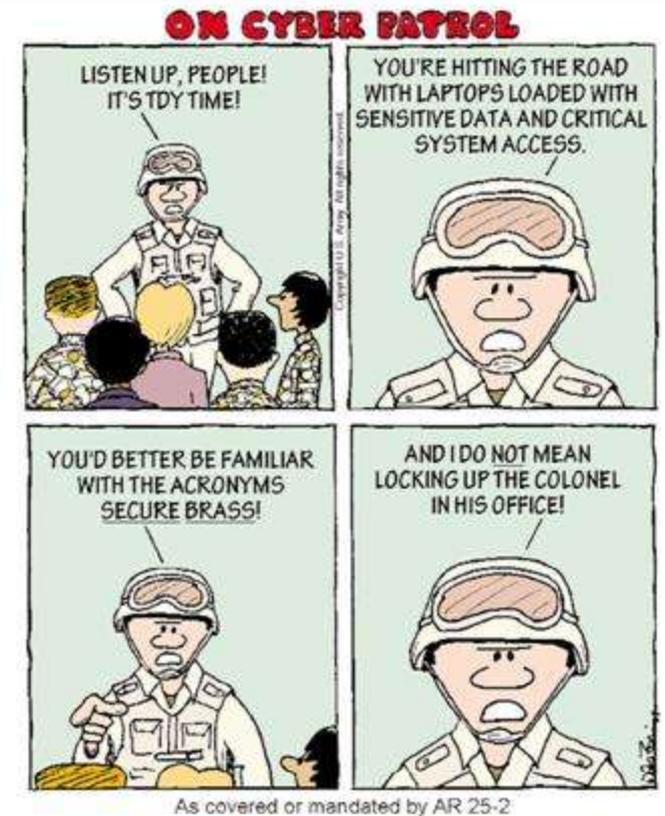
Good Laptop Security



- *While your Government Furnished Equipment (GFE) laptop is connected to the Network*
 - ***DO NOT*** use your modem and perform a dial-up connection to the internet
 - Your Wireless access ***MUST BE DISABLED***
- *Keep your laptop secure at all times while on travel.*
- *Scan all removable media, i.e., floppy disk, CDs, portable storage devices, before accessing data stored on it.*
- *If you use your laptop while on travel, have it scanned for viruses and malicious code when you return.*

Laptop Road Warrior

- Be a safe and secure Road Warrior! Rules of the Road: **SECURE - BRASS**
- **Save**, encrypt and secure your information
- **Ensure**, against public display of content: Shoulder Surfing
- **Control**, the laptop at all times: Lock and Leave
- **Use**, operating system end point security protections
- **Report**, the loss of any information or system
- **Eliminate**, unauthorized software
- **Baseline**, and update the system before deployment
- **Restrict**, user authentication and permissions
- **Automatically**, quarantine reconnecting systems
- **Scan**, and remediate reconnected systems
- **Save**, and backup user data



Get your copy of the Road Warrior Brochure
<https://www.us.army.mil/suite/page/190357>

Personal Devices



Prohibited Activities:

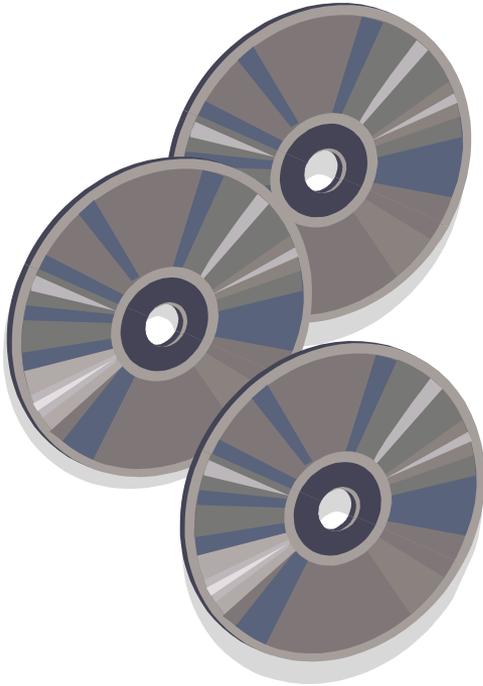
The installation and use of personal owned hardware, software (shareware or freeware), and/or computer peripherals such as modems to government owned workstations.

Connecting personal owned computers and/or electronic devices to government network ports.

Equipment may be confiscated and made U.S. Government Property

Our systems are being scanned daily. These devices, when detected, will result in a SECURITY VIOLATION

Prohibited



- **Peer-To-Peer (P2P)**
- **Illegal/Unlicensed Software**
- **Unapproved Software/Tools**
- **Download of Unapproved Plug-ins and Add-ons**

Contact your Local DOIM or call 119 for information and approval for loading authorized software.

Peer-To-Peer (P2P)

So what is P2P?

- P2P file sharing is technology that allow users to share files from their computer.
 - By default P2P software shares all documents and media files on your computer.
-
- ✓ P2P poses a serious threat to the security and integrity of our networks
 - ✓ One form of P2P is Instant Messaging (Chat)
 - ✓ The only authorized Instant Messaging on Army Networks is through AKO.
 - ✓ Currently over 100 different P2P programs released (Grokster, LimeWire, Gnutella, BitTorrent, etc...)
 - ✓ Malicious Code (Viruses, Spyware, Backdoors & other Malware)
 - P2P programs often create a backdoor or back channel that can be manipulated by someone else.

The installation and use of P2P on Army Networks will result in a SECURITY VIOLATION

Illegal and/or Unapproved Software

Certain activities are never authorized on Army networks. These activities include any personal use of government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software; gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

Extract from AR 25-2

4–5. Minimum Information Assurance Requirements

By logging into the network your activities are subject to MONITORING

Download of Software Tools

Download of Plug-ins and Add-ons

Do Not!

Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user configurable or unauthorized software (for example, instant messaging, peer-to-peer applications).

Extract from AR 25-2

3-3. Information Assurance Support Personnel

INFORMATION ISSUES



- **Metadata (Hidden Data)**
- **Personally Identifiable Information (PII)**
- **Mishandling of Classified Data**
- **Mislabeling Classified Media**



- **Social Engineering**
- **File Transfer Protocol (FTP)**
- **Unauthorized Remote Access**
- **Data-At-Rest**

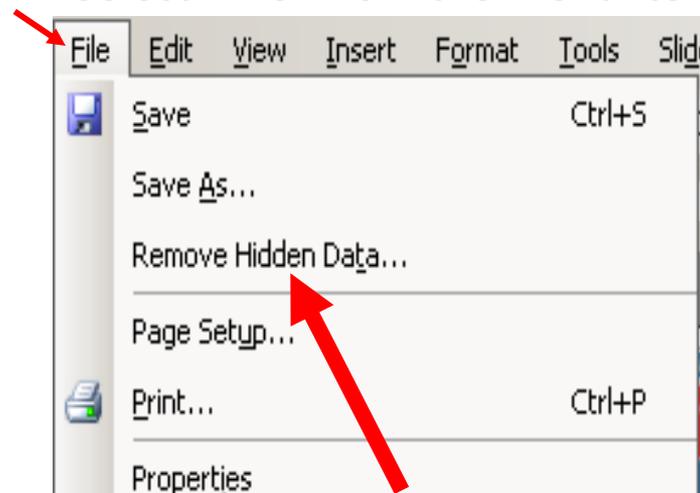


Metadata (Hidden Data)

Hidden Data is...

- Previously Deleted Text and Microsoft Metadata
- Embedded objects and Embedded Links
 - File Padding (intentional hiding)
 - Font Specific – white text, hidden text/cells/slides & tiny, tiny text
- Previously deleted data
 - Not just left behind by fast saves
 - Regular saves can also leave deleted text inside the file
 - *First line on document becomes metadata (e.g. title)*
 - *Deleted text inside an embedded object*

Select "File" from the Menu Items



**Remove Hidden Data Tool -
found in MS Word, Excel
Power Point**

Note: You might want to remove this hidden information before you share the document with other people. This hidden information can reveal details about your organization or about the document itself that you might not want to share publicly.

Personally Identifiable Information (PII)

What is PII?

Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, criminal history, employment history and information which can be used to distinguish or trace an individual's identity; such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to an individual.

This type of information in the wrong hands can result in Identity Theft!

Do not process official business on personally owned computers or on personal storage devices.

Mishandling of Classified Data

Mislabeling Classified Media

AR 380-5 is clear.
It is the users
responsibility to
properly control,
handle, mark, and
transport
Information.

1. Computer disc must reflect the highest level of classification contained on the disc
2. Standard labels should be used for all levels of classification.
 - a. The SF labels prescribed for removable storage media may be used for the marking of classified CDs and their cases
 - b. Classification must be conspicuously marked on the CD case and the CD itself



- **Do Not** send classified information across an unclassified network.
- **Do not** process or store classified information on an unclassified computer or device.

INFORMATION ISSUES

- **Social Engineering**

- The process by which an individual or group of individuals is deceived or confused into divulging information or performing an action for an attacker.
- One form of Social Engineering is called **“Phishing”**.

- **File Transfer Protocol (FTP)**

- IAMs and developers will transition high-risk services such as, but not limited to, ftp or telnet to secure technologies and services such as secure ftp (sftp) and secure shell (ssh)

Extract from AR 25-2, 4–6. Software Controls

- **Unauthorized Remote Access**

- Share personal accounts and passwords or permit the use of remote access capabilities by any individual.

Extract from AR 25-2, Prohibited Activities

Data-At-Rest

A. **“Data at Rest is Data at Risk”**. Laptops, portable notebooks, tablet-PCs, external media, and similar systems; commonly referred to as mobile computing devices (MCD); are highly susceptible to theft and loss. These devices are identified as high-risk when authorized for use in remote computing scenarios.

Places where Data-At-Rest is stored



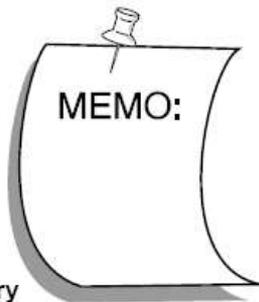
USB Drives



Laptops



Printers with memory



Printed Documents



CDs or Floppy Disks



Backup Tapes



Fax Machines



Handheld Devices



Computer Hard Drives



WEB Pages

INTERNET ISSUES



- **Unofficial Advertising**
- **Gambling**
- **Soliciting**
- **Unauthorized Commerce**
- **Sexual Oriented Material**
- **Threatening E-Mails**
- **Chain Letters**
- **Uploading to Unapproved Commercial Web Sites**



- **Unofficial Advertising**
 - **Gambling**
 - **Soliciting**
- **Unauthorized Commerce**



Prohibited Activities:

The use of communications systems for unlawful activities, in support of “for profit” activities, personal financial gain, personal use inconsistent with Army policy, or uses that violate other DOD policies or public laws are prohibited. This may include, but is not limited to, violation of intellectual property, gambling, and terrorist activities.

This type of activity can result in PUNITIVE ACTIONS

- **Sexual Oriented Material**

Prohibited Activities:

Intentionally sending, storing, or propagating sexually explicit, communications.

Anyone becoming aware of instances of child pornography or other illegal activity MUST report such activity to the Provost Marshal for investigation. This includes if you find it by accident during course of normal duties. Do not inform the individual.

Extract from AR 25-2, Prohibited Activities

- **Threatening E-Mails**
- **Chain Letters**

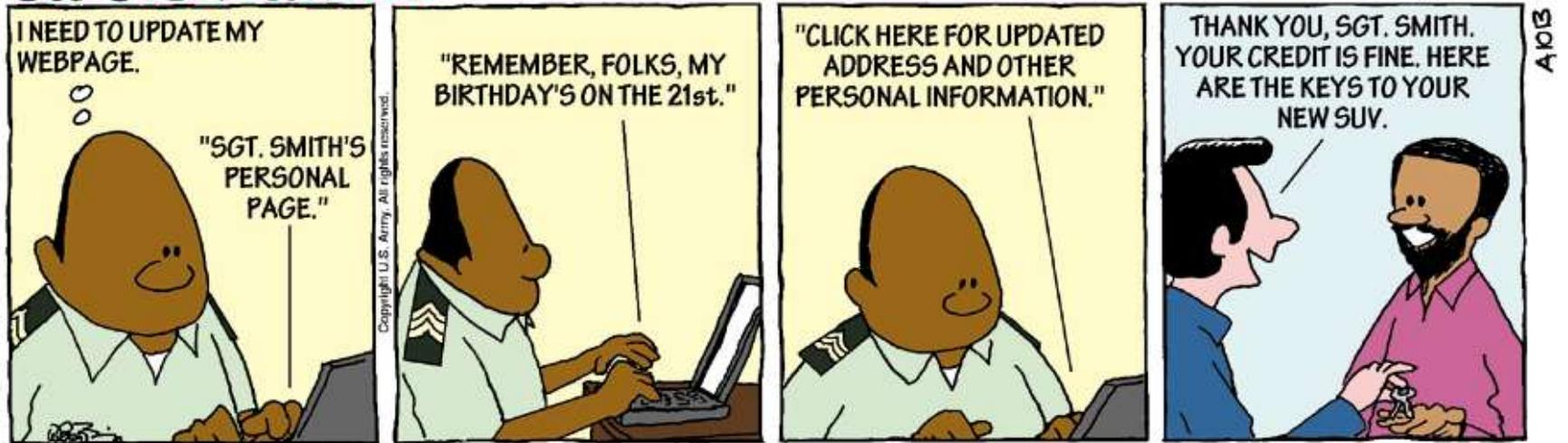
Prohibited Activities:

Intentionally send, store, threatening, harassing, political, chain letters, or unofficial public activity (that is, spam) communications. (Law Enforcement/Counter Intel investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.)

Extract from AR 25-2, Prohibited Activities

Uploading to Unapproved Commercial Web Sites

ON CYBER PATROL



As covered or mandated by AR 25-2

The Lights Are On, but Nobody's Home

- Your family's whereabouts are a military secret. Well, not really. However, treating them like they are can help keep you and you loved ones safe from the people who are constantly searching the internet looking for information that would allow them to take advantage of an empty house.
- Military personnel are drilled on the need for operational security (OPSEC) and keep information about unit strength, deployments and missions to themselves. Unfortunately, the popularity of social networking often outweighs OPSEC concerns in our private lives. Personal travel information that can be exploited by bad guys can now be found with very little effort.
- Look how much information is in this simple social network posting. "The family is head off to Florida tomorrow. Looking forward to a solid week of R&R. Our neighbors, Jim and Lucy, are joining us. Found a kennel for Sparky. Thanks again, Fred for agreeing to drop by on Wednesday to check on things. See ya Sunday!"

ON CYBER PATROL

As covered or mandated by AR 25-2



- If I'm a bad guy who knows where you live, I'm going to be backing a truck up to your house on Thursday knowing I don't have to worry about you, Sparky, Fred or the neighbors. I might as well pay Jim and Lucy's house a visit as well.
- It's one thing to mention your travel plans to a few close friends or office mates. It's entirely another thing to post it on the internet. Doing that is the same as putting a notice on the grocery store bulletin board or taking out an ad in the local paper. If only one bad guy picks up on the free intel, your personal property is suddenly at risk. The bad guy is probably annoyed that the information is so public, because he knows he's going to have plenty of competition in the race to steal your new HD flat screen TV

Here are a few social networking tips for talking about travel and vacations:

- Talk about vacations after they happen. Share pictures and stories after you have returned.
- Don't post details like flight info or exactly where you are staying.
- Guard travel information about family members and friends as well.
- Keep postings about personal activities limited to a small group of immediate family and friends. Don't share this info freely.
- Enjoy your travels, but keep your upcoming plans to yourself. If you can hold onto your stories and pictures until you return, then you will likely come home to your HD flat screen TV sitting just where you left it.

Policy Violations REMINDER

NO!

These types of activities can result in a
SECURITY VIOLATION
and lead to
PUNATIVE ACTIONS

Unauthorized Downloads

Personal Devices

Peer-to-Peer

Chain Letters

Mishandling Classified Materials

Illegal Activities

File Transfer Protocol (FTP)

Sexually Oriented Material

Threatening E-Mails

Unapproved Software

Unofficial Advertising

Gambling

Soliciting

If it isn't for official business don't do it

Prevention Is The Cure

- Be a strong link in the security chain!
- Keep passwords safe! Adhere to password standards. **DO NOT SHARE!**
- Watch what you upload and download from the INTERNET or where you 'travel' on the WEB.
- Adhere to email standards.
- Separate classified from unclassified information. Use classification guidance when regarding classified information. Label your diskettes!
- Keep track of your removable media. Store them when not in use.
- Watch your file transmissions! Make sure the files you transfer or the email you send is appropriate for the sensitivity of that network!
- Keep your files and access to the network safe!
- Report anomalies, i.e. requests for information from unknown sources (foreign countries), destroyed, infected or corrupted files, missing computer hardware, etc.
- Traveling with a government computer? Keep track of it!
- When in doubt - encrypt it.
- **Secure our Perimeter! Secure our Information! Secure our Warfighters!**



IA Home **Login** Courses MTT Locations Resources Contact

INFORMATION ASSURANCE TRAINING CENTER
US ARMY SIGNAL CENTER FORT GORDON, GA

Be a strong link in the security chain!

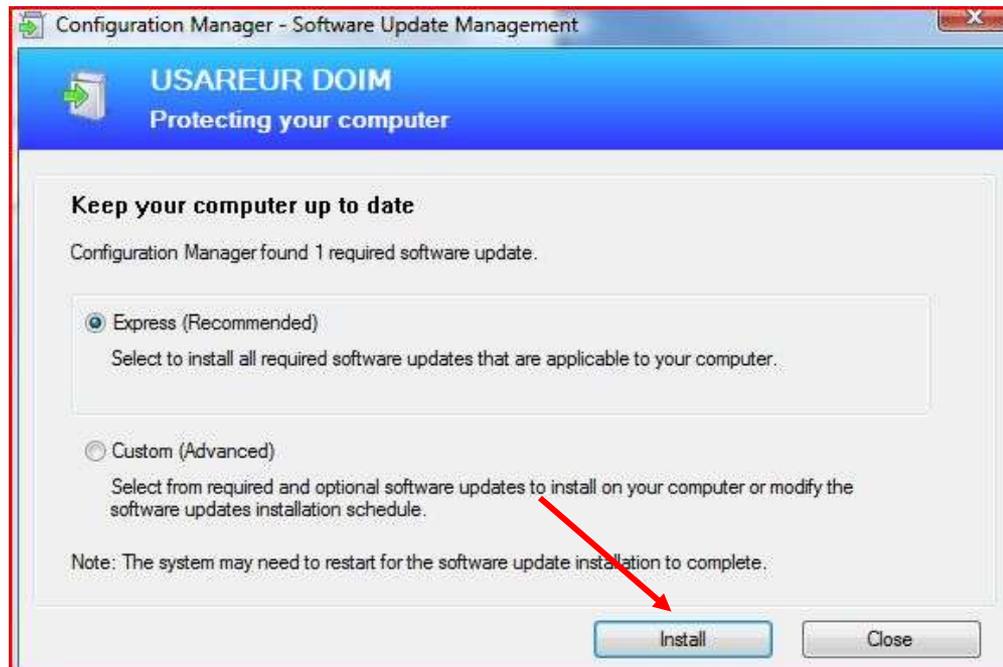
Did you know It's mandated all users with access to USAREUR networks LOGIN and take annual Information Assurance Training at :

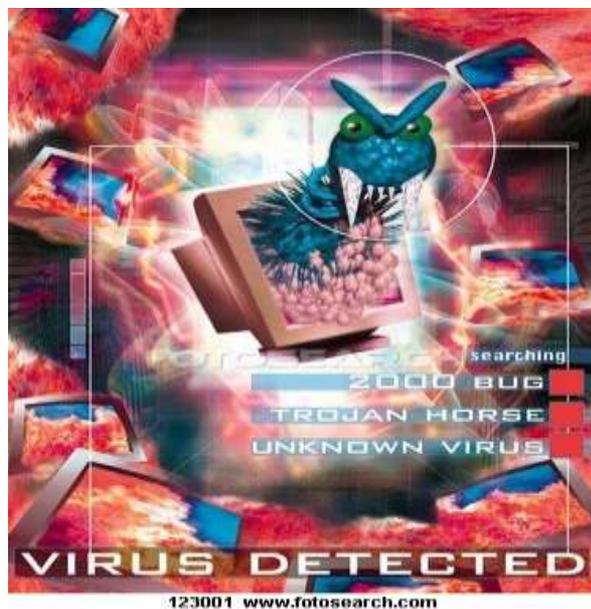
<https://ia.signal.army.mil/>

- USAREUR IAM is working to ensure your system is protected however, it's up to you to install these updates.
- If you see this icon on the bottom right hand corner of your taskbar, click on the box with the green arrow and install the updates.



NOTE: the system may require a reboot in order for the patches to take effect.





What to do if you suspect your system has a virus:

- Call the DOIM IANM section immediately and provide your name, phone and building number.
- Unplug your system from the network and leave system running and cease using your system.
- Await further instructions from IANM office.

- IANM, Mr. Benjamin Estela or Mr. Jason Hart
- DSN: 485-6210 or 7399



rws4860 www.fotosearch.com

What to do if you suspect your system has been Compromised:

- Call the DOIM IANM section immediately and provide your name, phone and building number.
- Cease using your system but leave it powered on and connected to the network.
- Await further instructions from IANM office.

- IANM, Mr. Benjamin Estela or Mr. Jason Hart
- DSN: 485-6210 or 7399



I should have remembered to leave my computer turned on!
What a sad ending to a happy vacation!!!



VIRUS ALERT!
VIRUS ALERT!
VIRUS ALERT!



DOIM scans your systems for vulnerabilities on a weekly basis. We push patches and updates daily, this process is transparent to you as a user.

Also, if your going TDY or leave **DO NOT SHUT OFF YOUR COMPUTER !** otherwise your system will become vulnerable. Ask coworkers to ensure your PC is kept on (*unless otherwise directed by the DOIM*)