2007 Computer End User Training
1 June 2007
2007 Information Assurance
Security Awareness Briefing

AMRDEC Information Assurance
AMRDEC IA Team
256-876-0954

usarmy.redstone.rdecom-amrdec.list.ags-support@mail.mil
• This Presentation is UNCLASSIFIED

• What is Information Assurance
• General Security Guidance
• Protecting Information
• Reporting Violations
• What can you do?
Are You the Problem or the Solution?

WHAT PART OF THE COMPUTER SEEMS TO BE CAUSED THE SECURITY PROBLEM?
THE NUT AT THE KEYBOARD!
Information Assurance is:

“What information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation ... providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

as defined by the CNSSI 4009, “National Information Systems Security Glossary,” dated May 2003
What is Information Assurance?

- **AVAILABILITY**: Making sure the computer and the information is there when we need it.

- **INTEGRITY**: Making sure the information we use, transmit, process, or store has not been corrupted or adversely manipulated.

- **AUTHENTICATION**: Making sure we know who is using our computers and accessing our data.

- **CONFIDENTIALITY**: Making sure the information is protected from disclosure.

- **NONREPUDIATION**: Making sure the information is ‘tagged’ so when we send it – we know it got there, and the recipient knows who sent it.
So, Why Are You Here?

- DOD and Army policy requires annual information assurance awareness training.
- Need to emphasize important security tasks and acceptable user practices.
Your Mission

• Recognize your computing responsibilities.
• Accept responsibility for protecting government information.
• Recognize the challenges and threats that can harm our National Security.
Do You Know What “OK” Means?

- When you login, you acknowledge that the information system you are using is for “Official Government Use Only”.
- The server and all of its information are subject to inspection.
- Your actions are subject to continuous audit.
Protect your identity (User Id) by using strong passwords. The following applies:

- User generated passwords must be 14 characters or longer.
- Must contain three of the four character types: uppercase, lowercase, numbers, and special characters.
- Passwords will be changed at least every 60 days.
• Always log off of the Wiki, Jira, or Perforce when leaving your computer unattended!

You are responsible for the data on your system at all times!
AMRDEC prohibits the use of this server for:
- Chain letters.
- Private commercial activities.
- Accessing pornographic or gambling sites.
- Participating in online auction activity.
- Political Activity.
- Illegal fraudulent or malicious activities.
- Any use which reflects adversely on AMRDEC or any other DOD element.

Virus Protection:
- Avoid attaching media from other computing environments. If unavoidable, at the least, ensure virus scan is performed on the media before utilizing data.
- Ensure your workstation runs a daily virus scan.
Types of Information

• Information can be stored on:
  - Printers with Memory
  - Printed Documents
  - CDs or Floppy Disks
  - Backup Tapes
  - Handheld Devices
  - Computer Hard Drives
  - Web Pages
  - Fax Machines

DOD treats all media as documents.
What is Spillage?

• It is a form of System Contamination.

• It is the unintentional improper storage, transmission or processing of CLASSIFIED information on an UNCLASSIFIED system or via a communications path.

• Most common occurrence is transmission via email or embedded in Power Point Presentations or other non-redacted files.
Why is This Happening?

• Users are not reading Email completely.
• Electronic media is not being marked properly.
• File names or subject headers do not reveal content sensitivity of information.
• Rules for “data aggregation” / derivatively classifying are not well understood.
• Individuals are unaware of classification guides / guidance.
• Improper storage, cleansing, transmission, processing of classified information.
• All AMRDEC personnel are PERSONALLY responsible for protecting sensitive and classified information.

Bottom Line: THESE INCIDENTS MUST STOP!
• The Army Game Studio servers are not accredited for Classified processing!

DO NOT STORE ANY CLASSIFIED DATA ON THE AGS SERVERS!
Security Incident:
• An attempt to exploit a national security system; may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service.
  – Security incidents include:
    • penetration of computer systems.
    • exploitation of vulnerabilities.
    • introduction of computer viruses or other forms of malicious code.

If an incident occurs:
• Gather all pertinent information:
  – time, details, person(s) involved, actions taken, etc.
• Report it to your IASO, SA, IAM and the AMRDEC Help Desk.
• Site administrators should notify LCIRT (lcirt-r@redstone.army.mil).
• If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.

Report ALL Suspicious Activity!!
• Report suspicious persons or circumstances immediately to your Supervisor, IASO, the Information Assurance Team, or the AMRDEC Security and Intelligence Division.

• Be alert for:
  – surveillance attempts.
  – suspicious persons or activities.
  – individuals using unauthorized recording devices.
To Improve our Security Program

• Be a strong link in the security chain!
• Adhere to password standards.
• Keep passwords safe!
• Do not share your username or password with anyone!
• Separate government work from personal activities.
• Separate classified from unclassified information. Use classification guidance when regrading 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!

• Report anomalies. Requests for information from unknown sources (foreign countries), destroyed, infected or corrupted files, missing computer hardware, etc. Report this to your IASO and to the Help Desk.
• **Strictly** follow Army and AMRDEC security guidance. If you don’t know - ask!

• Contact your Information Assurance Security Officer (IASO), Information Assurance Manager (IAM) or the Information Assurance Team at usarmy.redstone.rdecom-amrdec.mbx.sed-ia@mail.mil / 313-2777 for assistance.

Pay Attention to Detail.
Be Alert.
Be Aware!

*Security is your responsibility!*
AMRDEC Training:
https://intranet.amrdec.army.mil/Training

Fort Gordon Information Assurance (IA) Training:
https://ia.gordon.army.mil/ia_courses.htm

AMRDEC IA Training links and information:

AMRDEC IA Frequently Asked Questions:
AGS SED Information Assurance Team
256-876-0954
usarmy.redstone.rdecom-amrdec.list.ags-support@mail.mil