Data-At-Rest (DAR)

“Protection of PII and SI”

(**Please read all notes included with the slides**)

Data-At-Rest is Data-At-Risk!
NOTES

• Welcome to the this Data-At-Rest (DAR) Training. Please read all notes included with every slide.
• **PURPOSE:** The purpose of this training is to provide you information on the new Data-At-Rest policy and program

• **OBJECTIVES:** At the end of this briefing, you will learn:

  – Why the DAR Program is important
  – Understand the DAR Policy
  – How to encrypt PII and SI by using the "Encrypt" Folder
  – What to do when preparing for travel
  – Requirements while traveling
  – What to do when returning from travel
NOTES

• Here is the purpose and the objectives of this training.
Agenda

- Purpose
- History
- Definitions
- User Responsibilities
- How to Use the "Encrypt" Folder
- Why important
- Preparing for travel
- While traveling
- Returning from travel
- Protecting Personally Identifiable Information Video
- DAR Policy References
NOTES

• This is the Agenda.
• To increase awareness and educate users on the new policy requirements for Data-At-Rest, including the protection of Sensitive Information (SI) and Personally Identifiable Information (PII)

• Instruct users how to use the "Encrypt" Folder on the desktop
NOTES

• The purpose of the program is to increase awareness and educate users on the new requirements for the handling of DAR devices, and the protections of SI and PII and to instruct users how to use the (……..)on the users desktop.

• “Fort …… is just one incident away from being another Army Statistic.”
• ALARMED by the new information security threats and the loss of PII and SI

• Army policy, standards, and guidance have existed since 2003 and relied on voluntary management enforcement

• Data-At-Rest is Data-At-Risk!
NOTES

• Alarmed by new information-security threats and the subsequent loss of personally identifiable information (PII) and sensitive information (SI), the U.S. Army and XXXX are updating their policies to add more security measures on the use and safeguarding of digital media, cell phones, personal digital assistants, portable pen scanners and other devices. These tighter restrictions come as experts sound the alarm on the dangers presented by the small, portable, yet powerful items, which are increasingly used to steal sensitive information.

• These devices are found every day in soldiers’ pockets, and yet all present a frightening security risk. But no matter how handy these devices are, they can also serve as a tremendous source of data leakage. Through this medium classified information is being passed on to sources who don’t have a need to know or to our enemies.

• Policies have been in existence since 2003 and relied on voluntary compliance, management and enforcement. Since this is not working, the Army is now directing the immediate implementation of DAR remediation procedures.

• Just remember, Data-At-Rest is Data-At-Risk!
Definition

• Personally Identifiable Information (PII)

• Sensitive Information (SI)

• Data-At-Rest (DAR) Devices
  • Mobile Computing Device (MCD)
  • Data Storage Device (DSD) / Removable Media

• Government Facility

• The DAR Policy is punitive in nature IAW AR 25-2.
NOTES

• Here are some key definitions you need to know to be successful in today’s environment.

• Personally Identifiable Information (PII) - PII is defined as any information about an Individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

• Sensitive Information (SI) – SI is defined as any information of interested to the U.S. Government, DoD, and the Army that is sensitive in nature and requires protection. Examples of this include, but not limited to: Privacy Act, For Official Use Only, HIPAA, information requiring special handling, Draft publications, Plans or lessons learned, Operations, plans and training data, Logistics/maintenance data and the list goes on.

• Basically anything that is not releasable to the general public requires protection. Your outlook PST or personal folder must be protected as it mostly contains sensitive information and often personally identifiable information.

• DAR Devices include mobile computing devices such as notebook computers, PDAs, Blackberries. Etc. This also includes Data Storage Devices (DSD) or Removable Media which include thumb drives, removable hard drives, Compact disks, floppy disks, etc.

• Government Facility is the office area where the device is normally located. So if I want to take the laptop out of my office and move it to another building across base, this applies. These rules come into play not when you go to another installation, or another country, but as soon as you remove the device from the facility where it is normally used and secured. For Official Use Only
Responsibilities

Users:

• Identify and maintain accountability for all government MCDs/DSDs in your possession
• Ensure all devices are properly marked
• Secure all devices from theft and pilferage
• Encrypt all sensitive data on devices in their possession
• Use the "Encrypt" Folder in your Documents Folder for encryption of all sensitive data
• Use only government approved/owned devices
• Complete the Common User Training CBT and sign the Acceptable Use Policy (AUP)
• Ensure system is scanned upon returning
• Report any loss of information
NOTES

• The users are the most important, but also the weakest link in this process. As mentioned earlier compliance has been voluntary, but in a couple of slide you will see what has happened when did not properly protect the data they were charged with protecting.

• The user must identify and maintain accountability for all government devices in their possession. They must be marked and secured to prevent theft and pilferage.

• Encrypt all sensitive data on the devices in their possession, and when you are traveling it is a good idea to encrypt all data. Use the (…) on the desktop.

• Users are prohibited from using personal devices on government computers. They are only authorized to use government approved and owned.

• Obtain written authorization prior to removing a device, create and submit a security plan to the approval authority and report any incident immediately IAW the NEC incident reporting policy and procedures.
Using the “Encrypt” Folder

Use the "Encrypt" Folder on your desktop to encrypt all sensitive data and Personally Identifiable Information (PII) by one of two options:

1. Copy all those files in the "Encrypt" Folder and then delete them from where you copied them, after you have verified that all those files are in that folder

2. Or you can drag and drop them into the "Encrypt" Folder

** Choose whatever option you are most comfortable with doing. If you are unsure of the instructions please contact your Unit or Garrison IA personnel**
NOTES

• Encrypt all sensitive and personally data on devices in their possession
• Use the (……..) on your desktop to encrypt all sensitive data and Personally Identifiable Information (PII) by copying all those files in the (……..)and then deleting them from where you copied them from after you have verified that all those files are in that folder.
• Or you can drag and drop them into the (……..)whatever you are most comfortable with doing. If you are unsure of the instructions please contact your unit or garrison IA personnel
American investigators have paid thousands of dollars to buy back the stolen drives, according to shopkeepers outside the major military base here.

By Paul Watson, Los Angeles Times | April 15, 2006

Stolen military data for sale in Afghanistan
Despite crackdown, computer drives found with names of alleged spies
NOTES

• a. The Los Angeles times broke this story on 15 Apr 06, on how thumb drives, hard drives and other storage media were making their way off Bagram Airfield and ending up in the shops of the Bazaar; many apparently stolen, but not all.

• b. The reporters found that many of these devices contained sensitive information on them. American investigators spent days in the bazaar paying the shop keepers for them in an attempt to keep sensitive information from getting into the hands of the Taliban and to determine the real damage that these devices and the information on them had caused or would potentially cause.

• c. Despite crackdowns computer drives continue to be found with sensitive information, including names of alleged spies. Just outside the main gate of the huge U.S. military base in Bagram, Afghanistan, shopkeepers at the bazaar peddle a range of goods, including computer drives with sensitive and even secret information, stolen from the base. At this very bazaar, an Associated Press reporter purchased a handful of memory sticks in order to protect information.
One flash memory drive, sold for $40, holds the names, photos and phone numbers of people described as Afghan spies working for the military. Other thumb drives have been found to contain:

- Social Security numbers listed next to the names of hundreds of Soldiers
- Names of senior Afghan ministers whom US intelligence agencies believe to be drug smugglers
- List of 12 provincial officials the US reportedly wants removed from office

One shopkeeper said, “They were all stolen from offices inside the base by the Afghans working there,” he said. “I get them all the time.”

“Convenience Kills”
NOTES

a. The bullets are extracts from a number of the news reports that resulted from the LA Times story and highlight that every device improperly handled can cause serious unintended consequences for the army

b. Though unable to discuss the actual results of the damage done, suffice it say that it was not trivial. Even the information listed here could cause problems, for example.

(1) Pictures of Afghan spies. I am sure if the Taliban were to get this one, the Taliban would try to kill every one of them. Plus, now it’s going to be harder to recruit new spies if they think we can’t be trusted to protect their identity.

(2) Social Security numbers are troubling. The loss of data by Military personnel particularly Social Security numbers has jeopardized the security of many Soldiers and created a new criminal enterprise. “I-Jacking”, the highjacking of personal information, is a new criminal enterprise that is a spin-off of personal information theft and has life long (extended) potential for victims.
   • SS Numbers do not change and you can be a victim of lifelong credit fraud - - which could be used by the terrorists to fund their operations
   • Terrorists can track SS numbers to your door step years after you retire from Military service

(3) The suspected drug smugglers could go underground making more difficult to catch them.

(4) The provincial officials, if they knew they were going to be fired could cause problems in their area by stirring up the local population against the US and coalition forces.

“Convenience Kills”. This is so true as the information we have on our systems, on these mobile devices is just as deadly, if not more, than an IED or other improvised weapon used by our enemy.

For Official Use Only
Identity Theft

• Michelle Brown, a victim of identity fraud from January 1998 - July 1999
  – Impersonator procured good and services worth over $50,000
  – Impersonator engaged in escalated level of crimes including drug trafficking
  – Damaged credit, erroneous arrest record, a warrant for arrest, and a prison record

• USA
  – 2003 to 2006 decreased total number of victims but an increase total value to US $56.6 billion in 2006
  – Average fraud, per person rose from $5,249 in 2003 to $6,383 in 2006

• Australia – Between $800 Million and $3.3 Billion in 2001

• United Kingdom – 2006 $3 Billion
NOTES

• Most of us have heard about the VA notebook that was stolen from an employee's residence containing 2.2 million U.S. military personal data. This was nearly 80% of the active-duty force.

• You might have heard about the contractor working at Camp Pendleton who lost a notebook computer containing the personal data for 2,400 marines.

• Here is what can happen when identity theft occurs. The most widely publicized account was a 29-year-old lady named Michelle Brown. For over a year and a half from January 1998 through July 1999, one individual impersonated her procuring over $50,000 in goods and services. This not only damaged her credit, but resulted in her name being associated with crimes that she could never have imagined, including drug trafficking. These crimes resulted in an erroneous arrest record, a warrant out for her arrest and eventually a prison record when the impersonator was booked under her name as an inmate in the Chicago Federal Prison.

• The US has seen a decrease in the total number of identity theft victims, but has seen an increase in the total value resulting from identity theft. In 2006 the US reports $56.6 Billion loss associated with identity theft. This is not limited to just the US. Australia reported between $800M and 3B in 2001 and the UK $3B loss.
Lost, Stolen or Compromised PII

• Organization involved: US Army Recruiting Command
• Date of incident: February 17, 2007

• Brief description:
  – A Brigadier General’s laptop was stolen from his hotel room
  – The PII data was not encrypted
  – The PII was in emails stored in exchange offline file on the laptop
  – PII is NCO Evaluation Report and Military Police Blotter Reports
  – Also, 300 Army recruiting prospects, some minors

• Describe actions taken:
  – Local police immediately notified
  – SJA responsible for notifying individuals whose information was compromised
  – NEC investigated what emails might have been on the laptop
NOTES

• Here is an incident that recently happened within the U.S. Army and it does not only happen to sergeants and captains. This can happen to anyone of any rank. Most users don’t realize that if they process evaluations, pay documents, 4187, and so on that are sent through your email, then you have PII on your system.

• Here is a General Officer who was TDY staying in a hotel room in a major city in the US. His notebook was not secured within the room and the data was not encrypted. The laptop contained an exchange offline file that is commonly used by most everyone, or also called a PST. This file had common emails associated with doing day to day business. This includes the emailing of performance evaluations, blotter reports, and information on 300 recruiting prospects of which some were minors.

• The laptop was stolen and the individual immediately reported the incident and a number of organizations became quickly involved. Two of interest are the DOIM and the SJA.

• I checked the website for this organization and the individual named in the report is no longer listed as part of the organization. We understand this General Officer was relieved of his duties and asked to retire. The data that was lost wasn’t even classified. What do we do when someone losses classified or causes a spillage?

• No one can be above this. Everyone has to comply for the program to work. Don’t be the next statistic for the Army, and if you are a supervisor, don’t let your subordinate become that statistic. Enforce the program and make it part of day to day business.
While Traveling

- Safety and security recommendations should be followed to protect laptops and safeguard sensitive data
- Use visual deterrents
- Avoid leaving unsecured laptops unattended
- Keep laptops inconspicuous
- Back-up valuable data on a scheduled basis
- Stay informed
NOTES

• Computer loss and theft represents a huge security risk to both individuals and the government. It's absolutely imperative to safeguard computing assets because of the direct security implications as well as the liability of exposure and malicious use of the data that the computer holds. A single $1,000 laptop may hold personally identifiable information, sensitive information and years of accumulated knowledge that could cost an organization millions of dollars in exposure and lawsuits. A few simple steps can mitigate risk and prevent a devastating loss.

• Some security experts say you should think of your laptop sitting on the table as a thousand dollars in cold cash; you wouldn't turn your back on that, would you? When traveling, never take your eyes off your laptop, even if it's in that nondescript bag. One laptop theft scam involves a security screener at the airport who passes your laptop computer through the X-ray machine while another screener stops you because of some metal on your person. During the screening, your laptop goes missing.

• But don't stop your constant vigilance when you leave the airport. Never leave your laptop unattended anywhere, especially at a big conference. And, this is really just common sense, don't leave your laptop out in plain view in your hotel room; bury it under some clothes or in a backpack, out of sight. The same goes for laptops in cars. Put your machine in the trunk or at least hide it under a jacket.

• A cable lock or other locking mechanism can act as a deterrent to would-be criminals. Although they can be ripped off the plastic exterior of a laptop with a strong tug, they do force some criminals to think twice before taking the risk.

• Lock them in cupboards, laptop carts or other secure facilities when not in use. If they must be left in a vehicle, they should be covered up or locked in the trunk.

• Laptops should always be carried in inconspicuous carrying cases, such as backpacks or tote bags, instead of tell-tale laptop bags.

• Data back-up needs to happen as frequently as possible to minimize the risk to organizations in the event of theft or loss. The information or ‘knowledge’ that is stored on the computer is more valuable than the computer itself.

• Continue to educate yourself on the tools and techniques used today by cyber criminals as well as the latest scams and other security risks to company data.

For Official Use Only
While Traveling

- Safeguard your data
- Carry laptop hard drive in jacket pocket
- Keep removable media separately in a backpack or briefcase
- Encrypt the data
- Check with IA personnel for latest advances prior to travel
NOTES

• In most cases, laptop thieves simply resell your hardware on eBay to make a few bucks; the criminals never think to check out the contents of the hard drive. That can be a good thing. Within the last year, two laptops used by Wells Fargo Home Mortgage were stolen— one in April 2006 and one in November 2003. These incidents illustrate how damaging such thefts might have been. In both cases, the suspects wanted only the hardware, not realizing the treasure trove of personal data contained within. Nonetheless, Wells Fargo did the right thing by contacting all the affected individuals to let them know that their mortgage data had entered the wrong hands.

• An inexpensive tip is to remove the hard drive when the laptop isn't in use and simply carry it in your jacket pocket. That way, even if someone at the security checkpoint steals your laptop, they won't make off with any PII or SI. If you can't easily remove your hard drive, you can also keep all of your sensitive data on removable media, such as recordable DVDs, CDs, and USB storage devices, and keep these separately in a backpack or a briefcase.

• Encrypt the data using Microsoft Encrypting File System (EFS) which is your (….)(Change to what you use) on your desktop. You will copy all PII and SI files there. While encryption doesn't guarantee your data will always remain safe, it will hamper all but the most persistent criminal hacker.

• Check with your unit IA personnel for the latest advances or changes implemented by the organization prior to your travels.
Reporting Lost, Stolen or Compromised PII or SI

User Responsibility

a. Report immediately to your Information Assurance Security Officer (IASO) and/or local chain-of-command.
b. The Information Assurance Security Officer (IASO) and/or local chain-of-command will report it immediately to the RCERT-CONUS first, and then report it to the Fort Gordon NEC.

A Serious Incident Report (SIR) will be generated and reported per AR 190–45 under the following conditions:

(1) Access or compromise of classified, sensitive, or protected information (for example, Soldier identification information (SSN), medical condition or status, doctor-patient, or attorney-client privilege

(2) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the USACE

(3) Loss of any IS or media containing protected or classified information

See the reference page for further information
NOTES

• User responsibility

  • Report immediately to your Information Assurance Security Officer (IASO) and/or local chain-of-command.
  • The Information Assurance Security Officer (IASO) and/or local chain-of-command will report it immediately to the RCERT-CONUS first, and then report it to the Fort (…..) NEC.
  
  • A serious incident report (SIR) will be generated and reported per AR 190–45 under the following conditions—

    • (1) Access or compromise of classified, sensitive, or protected information (for example, Soldier identification information (SSN), medical condition or status, doctor-patient, or attorney-client privilege).
    • (2) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the USACE).
    • (3) Loss of any IS or media containing protected or classified information.

  • See the reference page for further information
After Return from Travel

• Inform the approving authority that you have returned with the device and that it has been properly secured

• For Personally Identifiable Information, sign the data back in with the Security Officer or Supervisor

• If the device has been off the network more than 14 days or connected to another network, you must do the following:
  – IAM or IA personnel scan the mobile computing device for vulnerabilities and review
  – IAM or IA personnel scan the mobile computing device and data storage devices for viruses, worms, and trojans
NOTES

• Upon returning from your trip there are still several things that need to be accomplished.

• You must inform the approving authority for your trip that you have returned and the device(s) have been secured back in the office. Securing does mean just placing it on the desk and locking the door. It means locking it within a cabinet, drawer, safe or using a cable lock to attach it fix device or item that is not easily moved.

• If you had signed out PII with your supervisor or security officer, you must sign it back in verifying that it has been properly secured.

• If the device has been off the network for more than 14 days or has been connected to another network, you must contact your organization IAM or IA personnel to have the device scanned to make sure it will not introduce any viruses, worms, trojans and so onto the network.

• For example, you fly to attend a 5 day conference. You connect the notebook computer to the hotel network. When you return you will have to have the device scanned prior to connecting it back to the office LAN.
Remember these three important points!

- Users are the weakest link in MCD physical security
- Proper security and configuration of DAR protection on the device will prevent or hinder access and exploitation of the information
- Report Incidents
NOTES

• So through this process we have learned that Users are the weakest link when it comes to the security of PII and SI stored on mobile devices.

• Proper security, configuration and protection of these devices will prevent or at least hinder access and exploitation of the information.

• If there is an incident, report it immediately. This news will get much worst with time.
DAR Policy References

(https://ia.gordon.army.mil/refLib.asp)

- OMB Memo on PII
- DoDI 8500.2 Information Assurance Implementation
- AR 25-1, Army Knowledge Management and Information Technology
- AR 25-2, Information Assurance, numerous paragraphs
- Data-At-Rest (DAR) Protection – Mobile Devices using EFS Implementation (v1.0) BBP https://informationassurance.us.army.mil/bbp/BBP%20DAR%20VER%201%200.pdf
- “Road Warrior” Laptop Security BBP https://informationassurance.us.army.mil/bbp/BBP_Road_Warrior_VER_1_3.pdf
- AR 25-2, Section VIII Incident and Intrusion Reporting and https://www.rcert-c.army.mil/index.html

For Official Use Only
Please see your Unit or Garrison IA personnel or contact the NEC Information Assurance Division at:
Usarmy.gordon.93-sig-bde.list fg-nec-info-assurance-div@mail.mil

Data-At-Rest is Data-At-Risk!

Click Here to validate.

Select “Fort Gordon Data at Rest validation” to validate.