INTRODUCTION

The following FAQs are provided as an aid in understanding and interpreting the July 3, 2007 DoD Policy Memorandum “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”. The list of questions is based on experiences and questions raised during the policy’s development, after the policy was signed, and after the JTF-GNO Communication Tasking Order (CTO 08-001) was published. Individual answers are not necessarily comprehensive and the list is obviously not exhaustive. This is a living document and additional questions will be added periodically when appropriate. Additional questions and/or clarifications should be forwarded to the POCs listed on the policy memo.

TABLE OF CONTENTS

[1. Why issue the policy at this time? What's the background? 2](#_Toc193603481)

[2. What does "publicly releasable" information mean? 2](#_Toc193603482)

[3. Why do the DAR encryption products have to be FIPS 140-2 compliant? 2](#_Toc193603483)

[4. Is Microsoft’s EFS or Windows Vista DoD-approved for encrypting DAR? 3](#_Toc193603484)

[5. Why is the Trusted Platform Module (TPM) being mandated in this memo? 3](#_Toc193603485)

[6. Does the policy apply to desktop computers? 3](#_Toc193603486)

[7. Does the policy apply to cell phones or pagers? 4](#_Toc193603487)

[8. Should removable hard drives on desktop computers be encrypted? 4](#_Toc193603488)

[9. What are the encryption requirements for unclassified data transfers from SIPRNet to NIPRNet? 4](#_Toc193603489)

[10. Should removable storage media used for network or server backup be encrypted? 4](#_Toc193603490)

[11. What are the encryption requirements for various weapon systems and platforms? 5](#_Toc193603491)

[12. Should software updates, etc. that are distributed via CDs be encrypted? 5](#_Toc193603492)

[13. Why does the policy require encryption of BlackBerry’s and other PDAs when many models cannot conform to the FIPS 140-2 requirements of the memo? 5](#_Toc193603493)

[14. Have the DAR encryption products on the BPAs been tested against the HBSS? 6](#_Toc193603494)

[15. What is the Enterprise Software Initiative and why do Components have to order DAR products through it? 6](#_Toc193603495)

[16. Will DoD provide resources to support this effort? 6](#_Toc193603496)

[17. What are the reporting requirements of the policy memo? 7](#_Toc193603497)

[18. Does the policy apply to DoD contractors? 7](#_Toc193603498)

[19. Acronyms 8](#_Toc193603499)

1. Why issue the policy at this time? What's the background?

Protecting Data at Rest (DAR) has become increasingly critical given Information Technology’s trend toward utilizing highly mobile computing devices and removable storage media. Personally identifiable information (PII) or sensitive government information stored on devices such as laptops, thumb drives and PDAs is often unaccounted for and unprotected, and can pose a problem if these devices are compromised, lost, or stolen. Numerous US Government and industry laptops and removable storage media that contained PII have been lost or stolen over the last couple of years. This has generated negative media attention and potentially exposed sensitive information which has prompted a review of policies and procedures. Three policies that address protecting PII are the June 23, 2006 OMB Memorandum 06-16, *Protection of Sensitive Agency Information,* May 22, 2007 OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* and the August 18, 2006 DoD Memorandum, *Guidance on Protecting Personally Identifiable Information*. Since DoD was concerned not only with the loss of PII, but with all unclassified data contained on mobile devices, DoD decided to go a step further and issue the July 3, 2007 memorandum. It mandates encryption not only for PII records, but for all non-publicly released unclassified information that is contained on mobile computing devices and removable storage media.

[Back to Questions](#_INTRODUCTION)

1. What does "publicly releasable" information mean?

Publicly releasable information is official DoD information that has been reviewed and approved for public release by the information owner in accordance with DoD Directive 5230.9 “Clearance of DoD Information for Public Release”, April 9, 1996, certified current as of November 9, 2003. All unclassified DoD information is treated and protected as sensitive until it is reviewed and approved for release.

[Back to Questions](#_INTRODUCTION)

1. Why do the DAR encryption products have to be FIPS 140-2 compliant?

This policy was developed based upon previous DoD and OMB DAR encryption policies that specify a requirement for FIPS 140-2 cryptography. To clarify what FIPS 140-2 compliant means, it is a cryptographic module validated by NIST to meet NIST FIPS 140-2 requirements or the module has been approved by NSA. Encryption products that are FIPS 140-2 compliant afford DoD a higher level of assurance for encryption and authentication. This validation involves more stringent requirements and testing for modules to prevent compromise and enhance mitigation of threats.

[Back to Questions](#_INTRODUCTION)

1. Is Microsoft’s EFS or Windows Vista DoD-approved for encrypting DAR?

At this time, Microsoft’s Encrypting File System (EFS) and Windows Vista BitLocker are not FIPS 140-2 validated, therefore they should not be used to encrypt unclassified data (not publicly releasable) on DoD mobile computing devices or removable storage media. Several DoD Components have used EFS as a stop-gap measure until the DARTT procurement process was completed, which represented an acceptable use of EFS. OMB and DoD now require FIPS 140-2 compliant encryption products, therefore Components using EFS will have to migrate to approved encryption products. If EFS or Vista BitLocker receive FIPS 140-2 validation, they will become an approved solution for encrypting DoD unclassified DAR. Other products that contain approved NSA cryptographic modules can also be used to encrypt DoD DAR. According to the 21 March 2007 DAR Encryption Acquisition Memo (signed by the Deputy DoD CIO), DAR encryption that is bundled into a larger, inclusive technology (such as BitLocker in Vista OS or Seagate encrypted hard drives in Dell laptops) can be purchased outside of the DARTT Blanket Purchase Agreements. It is an OMB and DoD requirement that all encryption products meet NIST FIPS 140-2 requirements or have an NSA Approval Letter for use in US Government networks.

[Back to Questions](#_INTRODUCTION)

1. Why is the Trusted Platform Module (TPM) being mandated in this memo?

The TPM paragraph was inserted into this memo to ensure all new DoD computer assets have this module since there are many future software products that will use the security features of the TPM. Supporting TPM is a desirable requirement at this time since many DoD components want to leverage its capabilities in the future for the protection of DAR on mobile computing devices. Legacy systems will not be required to be retrofitted with TPM. Based upon Service inputs, TPM is already being mandated by some Services, it’s readily available on the commercial market, and in most cases is standard on new computer equipment.

[Back to Questions](#_INTRODUCTION)

1. Does the policy apply to desktop computers?

The policy applies to desktop computers to the extent they are used to encrypt non-publicly released unclassified information on removable storage media. If a user downloads non-publicly released unclassified information from a desktop computer to removable storage media (such as a USB thumb drive, CD, DVD, etc.) and the removable storage media does not contain approved automatic encryption capabilities, then encryption software must be installed on that desktop computer. This will allow users to encrypt data that is transferred to removable storage media generated from that desktop computer. If the desktop computer is configured or locked down so it does not allow data downloads to removable storage media, then the desktop does not require encryption software.

[Back to Questions](#_INTRODUCTION)

1. Does the policy apply to cell phones or pagers?

The policy applies to cell phones or pagers only when these devices are used as Personal Digital Assistants (PDAs) or Smartphones and store unclassified DoD data that has not been approved for public release.

[Back to Questions](#_INTRODUCTION)

1. Should removable hard drives on desktop computers be encrypted?

Removable hard drives used in desktop computers that are used to transport unclassified DoD data at rest that has not been approved for public release from one desktop to another off-site desktop, must be encrypted. For removable hard drives that stay in-house, it’s a good practice to encrypt these hard drives, but they are not a target of the policy memo.

[Back to Questions](#_INTRODUCTION)

1. What are the encryption requirements for unclassified data transfers from SIPRNet to NIPRNet?

First, you must exercise approved trusted downloading procedures for release of unclassified information from SIPRNet. If removable storage media is used to transport the data from a SIPRNet system to a NIPRNet system and the removable storage media contains only unclassified DoD data that has not been approved for public release then the DAR shall be encrypted, regardless if the removable media stays within a protected facility or not. Removable storage media like floppies, CDs, and thumb drives are too easy to lose, misplace, and steal; and they are easily taken off-site. This policy does not address encryption requirements for classified DAR.

[Back to Questions](#_INTRODUCTION)

1. Should removable storage media used for network or server backup be encrypted?

The policy does not mandate encryption of unclassified data on removable storage devices used to backup data on networks or servers that are stored for prescribed periods of time, whether those devices are thumb drives, CDs, hard disks, tape drives, etc. However, if individuals use removable storage media to backup their laptop or desktop’s unclassified information, then the policy to encrypt that data does apply. Encrypting backup media is a good practice and will likely be mandated sometime in the future, but it is not a target of the policy memo. Encrypting backup media requires careful thought and detailed guidelines since it introduces several management and configuration control issues especially if the media is stored for many years.

[Back to Questions](#_INTRODUCTION)

1. What are the encryption requirements for various weapon systems and platforms?

All weapon system programs and platforms with removable media should procure and use approved DAR encryption products where possible, however, their unique requirements may warrant non-standard solutions.

[Back to Questions](#_INTRODUCTION)

1. Should software updates, etc. that are distributed via CDs be encrypted?

If the removable storage media contains DoD information not releasable to the public, then yes it should be encrypted.

[Back to Questions](#_INTRODUCTION)

1. Why does the policy require encryption of BlackBerry’s and other PDAs when many models cannot conform to the FIPS 140-2 requirements of the memo?

The DARTT’s efforts are to maintain consistency with NIST, OMB, and HSPD-12 requirements for the protection of unclassified and personally identifiable information data at rest in mobile computing devices and removable storage media. DoD-issued Blackberry models and other PDA or smartphone devices may offer inherent data at rest encryption capabilities. To protect BlackBerry’s, “Content Protection” should be enabled as outlined in the DISA Wireless Checklist (STIG) to meet the DAR encryption memo. Other vendor’s data at rest encryption solutions may or may not meet FIPS 140-2 certification. Agencies should refer to the appropriate DISA Wireless Checklists for those specific products. The Department hopes to motivate vendors through this process to become compliant with FIPS 140-2 and provide solutions for mobile email devices. In addition, some products available through the DAR encryption BPAs support some PDA and smartphone devices. Note, through the year 2030, Triple DES (3DES) and the FIPS 197 AES will coexist as FIPS approved algorithms – thus allowing for gradual transition to AES. Other implementations of the DES function are no longer authorized for protection of Federal government information.

[Back to Questions](#_INTRODUCTION)

1. Have the DAR encryption products on the BPAs been tested against the HBSS?

Yes, the Air Force has tested all the DAR products against the Host Based Security System (HBSS) and they found no interoperability issues. Since testing can not cover every possible situation, there is always a chance that something may be identified once the products are fully implemented. To review the Air Force test reports, access the <https://collab.core.gov> website and refer to the Test Reports section under the SmartBUY/Data at Rest Community. The Air Force HBSS tests for each individual vendor are under Test ID #7.

[Back to Questions](#_INTRODUCTION)

1. What is the Enterprise Software Initiative and why do Components have to order DAR products through it?

The DoD Enterprise Software Initiative (ESI) DAR Encryption Enterprise Software Agreements (ESAs) are Blanket Purchase Agreements (BPAs) co-branded with GSA SmartBUY with the Air Force ESI Software Product Manager serving as the ESAs’ administrative/management leader.   ESI and SmartBUY have similar goals and objectives, but different customer bases.  ESI BPAs provide for DoD agencies, Coast Guard, Intelligence Community, NATO and FMS.  Through the partnership with GSA SmartBUY, BPAs are extended to other Federal agencies as well as state, local and tribal organizations.

DoD Components must purchase DAR encryption products to protect DoD DAR on mobile computing devices and removable storage media through the ESI because it benefits all of DoD. Exceptions would be if those encryption products were FIPS 140-2 compliant and included as an integral part of other products such as Vista BitLocker, or if the cryptographic modules are approved by NSA (with formal NSA Approval Letter). The DAR products on the ESI BPAs have gone through a full and open competition and have met technical requirements as specified by DoD Components. All awarded products are FIPS 140-2 compliant, support CAC integration, and licenses are transferable within a federal agency and include secondary use rights. Volume pricing is based on tiers for 10,000, 33,000, and 100,000 users and discounts on volume pricing range up to 85% off of GSA Schedule prices. DoD Components are strongly encouraged to combine orders to leverage volume pricing discounts.

[Back to Questions](#_INTRODUCTION)

1. Will DoD provide resources to support this effort?

DoD does not have resources to centrally fund and purchase DAR encryption products. Therefore each Component will have to budget on their own for this effort. Centralized funding will be re-evaluated for POM10 based upon the Components implementation status in FY08.

[Back to Questions](#_INTRODUCTION)

1. What are the reporting requirements of the policy memo?

The memo states “DoD Components will report the status of their implementation efforts to this office no later than December 31, 2007.” The DAR encryption implementation status and efforts by Components were collected through the JTF-GNO Communication Tasking Order (CTO) 08-001. The CTO came out the week of 7 January 2008 and it explained what data was to be reported by 31 January 2008. JTF-GNO sent out the Warning Order (WARNORD 07-047) on October 9, 2007. After analyzing the Components status results, a second JTF-GNO CTO or official advisory notice will be sent out in early CY08 updating and confirming the 25%, 50%, 75%, and 100% implementation timeline dates. At that time, Components will be directed to update the Vulnerability Management System (VMS) website at the end of each timeline period indicating percent progress.

[Back to Questions](#_INTRODUCTION)

1. Does the policy apply to DoD contractors?

Yes, the policy applies to DoD contractors. The policy covers all DoD non-publicly released unclassified information, regardless of ownership of the mobile computing device or removable storage media. According to Defense Federal Acquisition Regulation (DFAR) Supplement Part 239—Acquisition of Information Technology, subpart 239.71--Security and Privacy for Computer Systems (Revised January 10, 2008) “Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes.” This includes the July 3, 2007 DoD Policy Memorandum “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media” which addresses the need to protect DoD sensitive unclassified data regardless of the location or ownership of the transport media (mobile computing devices and removable storage media). Agencies need to ensure that contractors understand (and price into their contracts) that mobile DoD sensitive data has to be encrypted and protected under the same requirements for contractor devices as well as government.

To purchase from the DoD Data at Rest encryption Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs), which are co-branded with GSA SmartBUY, contractors need a letter from their CO/COTR stating that they are eligible to purchase off the BPAs. The letter needs to include the contract number under which they are eligible. Contractors should also refer to FAR Part 51 (Contractor Use of Government Supply Sources) and DFARS 252.251-7000 (Ordering from Government Supply Sources).

[Back to Questions](#_INTRODUCTION)

1. Acronyms

AES – Advanced Encryption Standard

BPA – Blanket Purchase Agreement

CDs – Compact Discs

COTR – Contracting officer technical representative

CTO – Communications Tasking Order

DAR – Data at Rest

DARTT – Data at Rest Tiger Team

DES – Data Encryption Standard

DFAR – Defense Federal Acquisition Regulation Supplement

DoD – Department of Defense

EFS – Encrypting File System

ESI – Enterprise Software Initiative

FAQs – Frequently Asked Questions

FAR – Federal Acquisition Regulation

FIPS – Federal Information Processing Standards

FMS – Foreign Military Sales

GSA – General Services Administration

HBSS – Host Based Security System

JTF-GNO – Joint Task Force - Global Network Operations

NIST – National Institute of Standards and Technology

NSA – National Security Agency

OMB – Office of Management and Budget

PDA – Personal Digital Assistant

PII – Personally Identifiable Information

TDEA – Triple Data Encryption Algorithm

TPM – Trusted Platform Module

[Back to Questions](#_INTRODUCTION)