DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

JUL 0 3 2007

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
EXECUTIVE DIRECTOR, DOD CYBER CRIME CENTER

SUBJECT: Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

References: (a) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006
(c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
(d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006

References (a) through (c) require encryption of various categories of sensitive DoD data at rest under certain circumstances. Reference (d) provides recommendations on means to protect sensitive unclassified information on portable computing devices used within DoD and advises that the suggestions are expected to become policy requirements in the near future. This memorandum establishes additional DoD policy for

the protection of sensitive unclassified information on mobile computing devices and removable storage media. It applies to all DoD Components and their supporting commercial contactors that process sensitive DoD information.

It is DoD policy that:

(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.

(2) Priority shall be given to satisfying the requirements of reference (c) and to encrypting DoD information on mobile computing devices used by senior officials (e.g., flag officers and senior executives) and other individuals who travel frequently, particularly to areas outside of the continental United States where loss, theft, or exploitation of the devices is more likely or the consequence of the loss would be more severe.

(3) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c).

(4) In anticipation of emerging encryption product capabilities, as well as requirements for device authentication, DoD Components shall ensure all new computer assets (e.g., server, desktop, laptop, and PDA) procured to support the DoD enterprise include a Trusted Platform Module (TPM) version 1.2 or higher where such technology is available. Written justification must be provided to the responsible Designated Approving Authority if assets are procured without TPM technology in cases where it is available.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI). The ESI establishes DoD-wide Enterprise Software Agreements / Blanket Purchase Agreements that substantially reduce the cost of common-use, commercial off-the-shelf software. Information on encryption products that meet the requirements of this policy may be found in Attachment 2. Other implementation details may be found at http://www.esi.mil and at http://iase.disa.mil

This policy is effective immediately. DoD Components will report the status of their implementation efforts to this office no later than December 31, 2007. The DoD CIO points of contact are David Hollis (703) 602-9982, david.hollis@osd.mil and David Tuteral (703) 604-0503, david.tuteral.ctr@osd.mil of the Defense-wide Information Assurance Program Office.

John G. Grimes

Attachments:
1. Definitions
2. Press Release

cc:
Chief Information Officers of the DoD Components

DEFINITIONS JUL 0 3 2007

Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media Memorandum

Data at Rest: Refers to all data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media, etc.) while excluding data that is traversing a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Laptop Computers: Also known as notebook computers, are small mobile personal computers light enough to carry comfortably. Laptops can be battery-operated and often have a thin liquid crystal display (LCD) screen. Some models can mate with a docking station to perform as a full-sized desktop system.

Personal Digital Assistants (PDAs): Also known as palmtops, hand-held computers, and pocket computers, are any small hand-held device that provides computing and data storage abilities. Examples of PDAs include, but are not limited to, BlackBerrys, Treos, Palm Pilots, and Smartphones.

Removable Storage Media: Refers to cartridge and disc-based removable and portable storage media devices that can be used to easily move data between computers. Examples of removable storage media include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives and other flash memory cards/drives that contain non-volatile memory.

Trusted Platform Module (TPM): The TPM is a microcontroller that stores keys, passwords and digital certificates. It typically is affixed to the motherboard of computers. It potentially can be used in any computing device that requires these functions. The nature of this hardware chip ensures that the information stored there is made more secure from external software attack and physical theft. The TPM standard is a product of the Trusted Computing Group consortium. For more information on the TPM specification and architecture, refer to www.trustedcomputinggroup.org/groups/tpm.

Sensitive Unclassified Information: Information that is not classified but restricted from public disclosure. For full definition, refer to DoDD 8500.1, "Information Assurance," October 24, 2002.

Press Release

U.S. General Services Administration

June 18, 2007
GSA #10359

Contact: Jon Anderson, (202) 501-1231
jon.anderson@gsa.gov

Data at Rest (DAR) Encryption Awardees Announced

WASHINGTON - The Office of Management and Budget, U.S. Department of Defense and U.S. General Services Administration awarded 10 contracts today for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices. These BPAs could result in contract values exceeding $79 million.

Awardees are MTM Technologies Inc.; Rocky Mountain Ram LLC; Carahsoft Technology Corp.; Spectrum Systems Inc.; SafeNet Inc.; Hi Tech Services Inc.; Autonomic Resources LLC; GovBuys Inc.; Intelligent Decisions Inc. and Merlin International.

Products are Mobile Armor LLC's *Data Armor;* Safeboot NV's *Safeboot Device Encryption;* Information Security Corp.'s *Secret Agent;* SafeNet Inc.'s *SafeNet ProtectDrive;* Encryption Solutions Inc.'s *SkyLOCK At-Rest;* SPYRUS Inc.'s *Talisman/DS Data Security Suite;* WinMagic Inc.'s *SecureDoc;* CREDANT Technologies Inc.'s *CREDANTMobile Guardian* and GuardianEdge Technologies' *GuardianEdge.*

The encryption of data-at-rest (DAR) information is now possible through these BPAs, which were successfully competed using DoD's Enterprise Software Initiative (ESI) and GSA's government-wide SmartBUY (Software Managed and Acquired on the Right Terms) programs.

DoD ESI and the U.S. Air Force's 754th Electronic Systems Group at Maxwell-Gunter Air Force Base, Ala., will provide acquisition and contract support for the awards and administer the contracts throughout their five-year contract lives. GSA's SmartBUY program will provide all acquisition support for civilian agencies, including state and local governments.

"Today's SmartBUY announcement demonstrates that we remain vigilant in our efforts to strengthen security and improve our efforts to safeguard sensitive and personal information across the board," said Karen Evans. "The government is accountable to America's citizens for the privacy and protection of their sensitive information, while at the same time, improving services within the government. This agreement is critical to all levels of government—Federal, state, and local. The DoD-GSA team solved a major data encryption issue and allows our state and local governments to share in the solution while saving substantial taxpayer dollars at all levels. This is a milestone that will help build public trust as we continue to improve security within our Information Technology systems government-wide." It was Evans' OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, in June 2006 that was a key impetus for federal action resulting in the agreements.

Protecting data-at-rest has become increasingly critical in today's IT environment of highly mobile data and decreasing device size. Personal identity information 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. In addition to saving taxpayer dollars, this enhances DAR information security and requires vendors to meet stringent technical and information assurance requirements.

Two months after OMB issued its memo, the DoD Data-at-Rest Tiger Team (DARTT) was developed to address technical requirements. The goal was to award multiple BPAs by mid-2007. Eventually, the DARTT evolved into an interagency team comprised of 20 DoD components, 18 federal agencies and NATO.

"This highly successful interagency team defined and agreed upon data-at-rest requirements, which enabled the government to establish these critically important BPAs," said David Wennergren, DoD's deputy chief information officer. "It is truly historic in that agencies from across all levels of the government came together to solve a problem and develop an acquisition solution to meet all federal and local government DAR security requirements in an incredibly short time-frame."

The DARTT conducted an extensive threat/risk analysis and market survey prior to submitting recommendations to DoD military department chief information officers in October 2006. In November 2006, DARTT began the current acquisition process in conjunction with the DoD ESI. GSA SmartBUY and federal agencies joined the DARTT in December 2006 and NATO joined in January 2007, with state and local governments joining in March 2007.

"These first-ever BPAs for data-at-rest encryption are also the first available for state and local government purchases," said Jim Williams, GSA's Federal Acquisition Service Commissioner. "The DOD-GSA team has leveraged the incredible buying power of the federal government to help state and local governments with their DAR solutions."

State and local governments are participating under GSA's Cooperative Purchasing Program, which allows them to purchase IT products and services from both GSA's Multiple Award Schedule 70 and Consolidated Schedules that have IT special item numbers. Possible because Section 211 of the E-Government Act of 2002 amended the Federal Property and Administrative Services Act, cooperative purchasing is the means by which state and local governments have this first-time opportunity to join federal customers in purchasing encryption products fully compliant with FIPS 140-2. This federal standard defines national interoperability and security requirements for these governments electing to achieve this level for their networks.

"Protecting sensitive and private information, such as social security numbers and financial information, is an ongoing responsibility that New York State and its agencies are focused on each day," said Governor Eliot Spitzer. "By working with the federal government to protect this important information we have the ability to add another layer of protection, to New York's cyber security program, in an extremely cost-effective way."

Three categories of software and hardware encryption products are available under the BPAs - full disk encryption (FDE), file encryption (FES), and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements, and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than prices each vendor has available on GSA schedules, with cost avoidance to the government estimated at up to $73 million over the life of the BPAs. Additionally discounts on volume pricing range up to 85% for volume pricing, and volume pricing is based on tiers for 10,000, 33,000, and 100,000 users.

Additional information will be available on http://www.esi.mil and http://www.gsa.gov/smartbuy.

###

Attachment 2

Founded in 1949, GSA serves as a centralized procurement and property management agency for the federal government. GSA manages more than one-fourth of the government's total procurement dollars and influences the management of $500 billion in federal assets, including 8,600 government-owned or leased buildings and 205,000 vehicles. GSA helps preserve our past and define our future, as a steward of more than 420 historic properties, and as manager of USA.gov, the official portal to federal government information and services. GSA's mission to provide superior workplaces, expert technology solutions, acquisition services, purchasing and e-travel solutions and management policies, at best value, allows federal agencies to focus on their core missions.

Did You Know? FAS annual business volume of $46 billion accounts for more than one-seventh of the entire federal procurement budget. FAS manages acquisition programs that include information technology, telecommunications, furniture, tools, office products and supply items, and all travel, motor vehicles and credit card services.