



ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION
INTEGRATION

SEP 02 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Secure Mobile Environment (SME) Portable Electronic Device (PED)
Implementation Guidance

The SME PED provides the DoD with a new capability that allows wireless NIPRNET and SIPRNET access, to include email and web browsing, in one device. It also provides the user secure and non-secure voice capabilities.

The SME PED has undergone both operational and security testing on DoD networks and is now approved for DoD wide implementation. This memorandum and attachments provide the initial guidance to implement the SME PED in the DoD. It applies to all DoD Components. The ASD(NII)/DoD CIO will coordinate a follow-on DoD Instruction once the SME PED capability fully matures.

The point of contact for this guidance is Mr. Danny Price, who can be reached via email at danny.price@osd.mil or telephone number 703-607-0269.


Cheryl J. Roby
Acting

Attachments:
As stated

cc:
Chief Information Officers of the Military Departments

FOR OFFICIAL USE ONLY ATTACHMENT



IMPLEMENTATION PLAN

1.0 Purpose

1.1 The purpose of this attachment is to provide guidance to DoD Components for the implementation of the Secure Mobile Environment (SME) Portable Electronic Device (PED) and to designate roles and responsibilities required for the successful operation of the SME PED across the enterprise. For the purposes of this memorandum and its attachments, DoD Components refer to the Office of the Secretary of Defense, Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commands, Defense Agencies, and Field Operating Activities.

1.2 This Guidance does not supersede any existing Public Law, Federal or DoD policy, or Executive Order including regulations, requirements, and/or policies not limited to the protection of national security systems or, handling of classified information per DoD 5200.01 (Reference (a)), and SIPRNET policy.

2.0 Background

2.1 The Director, National Security Agency (NSA) embarked upon an aggressive program to build a mobile device capable of sending and receiving both unclassified and classified information. The SME PED is a wireless handheld device designed to provide users with voice (UNCLASSIFIED to TOP SECRET (TS) Sensitive Compartmented Information (SCI)) and data communications (UNCLASSIFIED to SECRET). For classified operations, SME PED utilizes the NSA's Secure Communications Interoperability Protocol (SCIP) for secure voice and High Assurance Internet Protocol Encryptor (HAIPE) for secure data.

2.2 There are planned to be two authorized SME PED platforms, the General Dynamics (GD) Sectera Edge™ and the L-3 Guardian™ (which will collectively be referred to as the SME PED for the remainder of this document). These devices have similar features but differ somewhat in operation and user interface. The SME PED uses existing commercial wireless carriers to obtain access to cellular networks and it has the ability to connect to deployable military cellular systems. All data traffic that passes through a cellular carrier network in order to access the Defense Information Systems Network (DISN) through a Multi-Carrier Entry Point (MCEP) is encrypted. Non-DoD Federal Agencies will be allowed to use the SME PED MCEP through a Memoranda of Agreement (MOA) with the Defense Information Systems Agency (DISA).

3.0 Concept of Employment

3.1 The SME PED is intended for personnel who have a bona-fide requirement to process classified information outside of their normal workplace or who otherwise require the capability to process classified information in a mobile environment in order to accomplish their mission. Components are encouraged to issue SME PEDs based on this guidance. Components shall develop the user criteria and a review process necessary to validate requirements consistent with this concept. The following personnel are recommended SME PED users:

3.1.1 High-level officials and other personnel supporting activities that require the capability to process classified information outside of their normal workplace in order to effectively accomplish their mission.

3.1.2 High-level officials and their designated support staff who currently maintain a secure communications capability in their quarters in order to effectively accomplish their duties (e.g., Secure Terminal Equipment (STE), Defense Red Switch Network (DRSN) or Voice Over Secure Internet Protocol (VOSIP), SIPRNET, etc.).

3.1.3 Deployed personnel who are supporting combat, humanitarian, or civil authorities operations who require a mobile capability to process classified information.

3.1.4 Officials required by law to maintain communications capabilities 24x7 (e.g., Combatant Commanders).

3.1.5 Personnel who are geographically separated from their parent unit and require the capability to electronically process classified information, but do not warrant or have the capability to stand up a SIPRNET enclave locally (e.g., a detachment commander who may not need SIPRNET on a daily basis, but may need the capability to process classified information on an occasional basis), or for designated personnel operating in an approved classified telework situation.

3.2 The SME PED is intended for worldwide use. International service providers are available for secure voice and data. SME PED users must negotiate an international service provider subscription in order to use SME PED internationally. SME PED users must subscribe to a wireless network service plan that offers: Voice service (for non-secure voice calls); circuit switched data service (for secure voice calls); and a packet data service (for non-secure and secure data applications such as email and web browsing).

3.2.1 Since SME PEDs are designed for users that require high availability of voice and data communications, it is highly recommended that users also subscribe to wireless priority service (WPS) which greatly increases the call completion rate during congestion or in the event of an emergency. This service is only available to the unclassified voice phone number.

3.3 The SME PED is an extension of the user's classified and unclassified desktop when supported by a MCEP. A single classified and unclassified SME PED server can support multiple email enclaves via trusted relationships; each Component may implement the SME PED server(s) configured in an enterprise fashion, or by using various locally provided servers to meet mission requirements.

3.3.1 ASD(NII)/DoD CIO and DISA established an Integrated Process Team (IPT) to evaluate the viability of implementing a SME PED Enterprise solution. It was concluded that individual Components/Services were already consolidating their email services in an effort to be more efficient. Continued consolidation is encouraged where appropriate.

3.3.2 The near-term implementation approach is designed for Components to establish NIPRNET and SIPRNET SME PED enclave servers to interact with the organizations' Microsoft Exchange Servers. To provide more efficient use of assets, it is recommended that organizations with common implementation criteria (e.g., same geographic location, same Component, shared network assets, shared domain, shared directory forests, or enterprise email solutions) consider fielding consolidated SME PED servers, where technically feasible.

3.3.3 As DoD continues to evaluate new and efficient ways to implement email at the enterprise level, it is expected that the SME PED will follow and adopt new architectures.

4.0 Requirements Determination

4.1 To adequately reflect customer requirements, the Joint Staff J6, working with Components, has determined initial SME PED requirements. If necessary, ASD(NII)/DoD CIO in coordination with the Director, NSA and DoD Components will prioritize initial fielding.

4.2 As the SME PED is deployed to users, it is important for leadership to understand how the devices are being fielded and used operationally. Joint Staff J6, Director, DISA, and Director, NSA shall work with user organizations to develop lessons learned pertaining to use and deployment to determine additional features required to enhance capabilities and to improve employment concepts.

5.0 Product Development Responsibilities

5.1 Director, NSA shall be responsible for the initial SME PED development, providing product improvements/enhancements (in conjunction with the vendors), and providing acquisition contracts for SME PEDs, servers, accessories, and training.

6.0 Network Responsibilities

6.1 Director, DISA, in coordination with DoD Components, is responsible for defining the SME PED architecture for the DoD. The SME PED architecture consists of the following major elements: the DoD MCEP(s), the Enterprise Computing Node/Defense Enterprise Computing Centers (DECC) aggregation point(s), Component enclave servers, SME PEDs, and non-DoD Federal Agencies that implement SME PEDs and servers. Director, DISA shall identify all critical points in the network and ensure redundancy while Components shall be responsible for enclave architectures.

6.2 Director, DISA shall have overall responsibility for the implementation, operations, and maintenance of the MCEP(s). Since the SME PED accesses the DISN via commercial wireless services, the MCEP is required to aggregate and route SME PED traffic. The MCEP is designed to support automated failover for wireless handsets and enclave connection. All hardware in the MCEP shall be fully redundant (e.g., Access Point Name (APN) circuits, Multi Protocol Router (MPR), Admin Server(s), etc).

6.2.1 The MCEP is currently housed in a commercial facility. Director, DISA shall evaluate options to establish a redundant MCEP at a government facility or use commercially managed services to provide redundancy in accordance with DoD Policy.

6.3 Data services for DoD customers shall be provided to access the SIPRNET and NIPRNET. The connection to these networks shall be supported via an aggregation point at an Enterprise Computing Node/DECC connected to a MCEP.

6.4 DoD Components shall configure and operate SME PED servers in accordance with the DISA SME PED Security Technical Implementation Guide (STIG) (Reference (m)), which is explained in Para 11.0. DISA shall ensure that all DoD Components and other SME PED user organizations have configured SME PED servers using the guidance in the DISA SME PED STIG prior to being given access to SME PED infrastructure.

6.5 Each non-DoD Federal Agency shall coordinate directly with Director, DISA to establish a MOA for the required services.

7.0 Procurement Procedures

7.1 The SME PED may be procured through established NSA Indefinite Delivery/Indefinite Quantity (IDIQ) contracts. Components shall MIPR funds to NSA who will in turn procure the devices on behalf of the requesting organization. Ancillaries and accessories also may be procured via NSA contracts. Users may purchase products directly from vendors but such purchases shall be done in coordination with NSA. The vendor must inform NSA of the user's COMSEC account and NSA shall verify it. Each device has a warranty of 1 or 2 years depending on the device purchased; additional warranties can be purchased if desired. Warranty information and procedures for troubleshooting the SME PED will be provided by the vendors upon purchase.

7.2 Organizations shall procure enclave software, and where necessary hardware, for the SME PED servers that allow the transfer of data from the SIPRNET and NIPRNET enclaves to the SME PED. These servers may be acquired via the NSA contract or directly from a vendor.

7.3 Organizations shall purchase airtime from a designated commercial carrier to enable the wireless communications functions of the SME PED. Activation of the SME PED on a wireless carrier network may be acquired via the NSA contract or via established customer methods. To utilize the full capabilities of the SME PED, it must be provisioned with the following cellular carrier services: circuit switched voice (for clear voice); circuit switched data (for secure voice); and packet switched data (for unclassified and classified data traffic). Before purchasing cellular services, Components should consult with their commercial carrier of choice to determine if the commercial network supports services required by the SME PED and to ensure that the services will be offered where the users intend to operate the SME PED.

7.4 Director, NSA is responsible for providing current SME PED and SME PED server pricing data as well as software updates to the DoD Components, and other Federal agencies, as

appropriate. Additional procurement information and software updates can be found at www.securephone.net.

8.0 Training

8.1 Training is critical to the successful and secure operation of each version of the SME PED. Each command shall be responsible for preparing its own training plan and materials. This SME PED Implementation Plan and Security and Operating Guidelines, SME PED user manuals, NSA Operational Security Doctrine for the SME PED (Reference (k)), Sensa email documentation, MCEP related server software manuals, the SME PED STIG, and local security procedures should form the basis of the training plan. User training should focus on the secure operation of the devices, COMSEC operational procedures, security incident reporting, Classified Message Incident (CMI)/data spill, device handling procedures, and information handling procedures. Additional device training on each version of the SME PED, systems management training for enclave servers, and installation support for the SME PED servers can be obtained at the Component's expense through the NSA IDIQ contract. Paragraphs 8.1.1 and 8.1.2 outline minimum areas that shall be contained in training plans.

8.1.1 Handheld device operations training (specific to either the General Dynamics or L-3 device) shall include instructions on how to: Authenticate with the device; zeroize keys; erase user data; operate the keyboard and function keys; operate secure and non-secure voice; operate secure and non-secure e-mail; conduct secure and non-secure web browsing; conduct secure wireless access to the SIPRNET and NIPRNET; operate personal organizer functions (calendar, contacts, tasks, alarms and notes); conduct desktop synchronization; change passwords; use of SCIF Mode (where authorized); how to store data in the devices secure vault to enable data at rest protection; and sign and encrypt emails.

8.1.2 User security training shall be provided to each actual user by local commands and must be completed, concurrent with issuance of the SME PED. Areas that shall be covered include: how to operate the device in a security conscious manner; physical security requirements for SME PED; procedures for reporting a lost or stolen device; discussion of requirement not to install or remove applications without the approval of the Information Assurance Officer and the Terminal Administrator; email auto-signature configuration requirements; types of email that must be digitally signed and/or encrypted (per C/S/A policies); what constitutes a security incident and related reporting procedures CMI/data spillage); INFOSEC and OPSEC information handling procedures (including use cases on when it is not appropriate to initiate or receive classified telephone calls or send or receive classified emails); required procedures described in Component or local site SME PED CONOPS; requirements to use DoD-approved CAC PKI certificates, prior to provisioning on SME PED; and proper password storage and usage.

8.2 Components should appoint and train Terminal Administrators who shall be responsible for SME PED configuration, user and security training, control and use requirements, and administration of SME PEDs. Comprehensive Terminal Administrator training can be purchased through the NSA IDIQ contract.

8.2.1 Training for Terminal Administrators shall include but is not limited to: procedures for provisioning SME PEDs (specific to either the General Dynamics or L-3 device); preparation and maintenance of the user agreement; requirement that users must complete required training before being issued a SME PED; requirement that all DoD SME PEDs be configured to operate with the users DoD-approved CAC PKI certificates; required procedures described in Component's or local site's SME PED CONOPS (Reference (1)); procedures for reporting security incidents, including a CMI; provisions in the DISA SME PED CONOPS and DISN procedures related to provisioning and issuing a SME PED; procedures for safeguarding passwords; and procedures for re-provisioning DoD-approved CAC PKI certificates on SME PEDs when user's certificates expire.

8.3 Apriva Sensa is currently the secure email client that supports the Windows CE-based SME PED while accessing either NIPRNET or SIPRNET email via the Non-Type 1 and Type 1 operational modes of the SME PED. It is recommended that each local command appoint a Sensa Server System Administrator or assign additional duties to existing IT support personnel. Personnel chosen to perform this function shall be familiar with the following: DISA SME PED STIG; procedures for hardening the Sensa server operating system via the applicable operating system STIG and Gold Disk; procedures for setting up secure server administrative accounts; procedures for setting up user accounts on the server and providing DISA new account information (per DISA CONOPS and DISN procedures); procedures for disabling user accounts when a SME PED has been reported lost or stolen; procedures for notifying DISA when a SME PED has been reported lost or stolen (to prevent access to the MCEP from the lost or stolen device); required procedures described in Component or local site SME PED CONOPS; and required procedures when a user reports a security incident (including a CMI).

8.4 Where authorized by the Facilities Security Manager, DoD facilities with SCIFs should also provide training to SCIF security staff on how to check that a SME PED is in the SCIF mode.

9.0 User Support

9.1 For device support, the user will contact their local Helpdesk, Terminal, or System Administrator. The local maintenance support staff will follow established trouble support procedures for resolution of the user's problem. If further assistance is required, it is recommended that the Terminal/System Administrator contact DISA DISN Customer Call Center (DCCC) at 1-800-554-DISN (3476). Director, DISA shall maintain 24x7 monitoring of the MCEP(s) to ensure continuous operations of the SME PED network and will be informed of other network issues as well as most device issues. Additionally, troubleshooting instructions for the devices will be available through vendor user guides and documents, and if necessary, the Terminal Administrator can call the device help desk number. The General Dynamics help desk numbers are 877-230-0236, DSN 644-1139 and commercial 410-850-4893. The L-3 help desk number is 1-800-339-6197.

10.0 Accreditation

10.1 NSA shall certify both SME PEDs to process classified information. NSA certified the General Dynamics Sectera Edge SME PED for Secret data communications and Top Secret

voice communications in Dec 2007. NSA is projecting certification of the L-3 device for Secret data and Top Secret voice communications late in calendar year 2009.

10.2 NSA will work with the SME PED vendors to obtain wireless carrier certifications to allow the SME PEDs to operate on the carriers' wireless networks. Director, DISA will be responsible for accreditation of the MCEP(s) and the MCEP(s) interface in the Enterprise Computing Node/DECC.

10.3 The DISN Flag Panel is responsible for assessing the enterprise security risk of operating of the SME PED and will authorize its connection to the DISN in accordance DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process, dated November 28, 2007 (Reference (g)).

10.4 Each enclave is responsible for its own certification and accreditation for both SIPRNET and NIPRNET. Each enclave shall conduct a DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation or update existing accreditation and connection package to support SME PED per DoDI 8510.01.

10.5 The addition of a server to the local SIPRNET enclave requires that the system administrator prepare and submit an update to the site accreditation package. The process for submission of the accreditation package to the DISA Classified Connection Approval Office (CCAO) is available at SCAO@disa.mil, DSN 381-1455/comm 703-882-1455.

10.6 Due to the SME PED's reliance on commercial cellular networks, whose technologies, systems, and services are not under direct DoD control, the SME PED system shall be certified and accredited as meeting only basic availability requirements. SME PED shall be operated with a mission assurance level at which the consequences of loss of availability shall be tolerated without an impact on the overall mission effectiveness, per DoDI 8500.2 (Reference (e)).

11.0 Security Technical Implementation Guide (STIG) Development

11.1 Director, DISA shall be responsible for developing an enterprise-wide STIG that provides guidance for each type of SME PED and the enclave SME PED servers. The SME PED STIG checklist shall provide: both required and optional security configuration settings for each SME PED architecture component; specific security-related user training requirements; SME PED provisioning; and system operations requirements. The SME PED STIG, which is FOUO, is available via the DISA Information Assurance Support Environment website at <https://powhatan.iie.disa.mil/stigs/net-sec-guides/>.

12.0 Interagency Agreements

12.1 Director, DISA shall be responsible for establishing and coordinating Interagency MOAs with non-DoD Federal agencies that operate SME PEDs and servers. Each Interagency MOA shall address at a minimum: service to be provided; organization responsibilities; cost/funds;

and system security measures/requirements. Each MOA shall be reviewed annually and updated as required.

SECURITY AND OPERATING GUIDELINES

1.0 Introduction

1.1 The security operational guidelines and procedures outlined in this attachment apply to the Secure Mobile Environment (SME) Personal Electronic Device (PED) handset operation, network infrastructure, and email gateway servers.

1.2 The SME PED offers cellular voice, web browsing, and two-way email messaging support for both unclassified and classified operations. SME PED offers cellular voice services that can be unclassified or classified up to the TOP SECRET Sensitive Compartmented Information (SCI) level and data services that can be unclassified or classified up to SECRET.

1.3 SME PED offers two fully independent operational modes for data (standard applications include web browsing, two-way email messaging, etc.). One operational mode is for unclassified data operations that support the processing of information up to For Official Use Only (FOUO) sensitivity level, and the other operational mode supports classified data operations up to the SECRET level. The SME PED has an integrated DoD Common Access Card (CAC)/Public Key Infrastructure (PKI) reader that can be used for email activities (i.e., encrypting, decrypting, and signing S/MIME email messages), encryption/decryption of protected data-at-rest, and client authentication to secure web sites while operating in the unclassified mode. SME PED offers data-at-rest protection in order to ensure that information stored on the device cannot be accessed unless the device is enabled (i.e. the device is unlocked and the user is signed in). SME PED uses Federal Information Processing Standard (FIPS) 140-2 validated encryption for data-at-rest in the unclassified operational mode. The SME PED also uses NSA-approved Type 1 encryption for data-at-rest in the classified operational mode.

1.4 Users should refer to DoDD 8100.02, DoDD 8500.01E, and DODI 8500.2 (References (b, d, and e)) regarding the security requirements for commercial wireless devices, systems, and technologies, and refer to DoDI 5200.01 (Reference (a)) which describes the handling, safeguarding and dissemination of classified and FOUO information).

2.0 Applicability

2.1 The following provisions apply to all DoD employees, contractor personnel, consultants, and all other personnel performing classified and unclassified work involving SME PED operation, administration, or maintenance for the DoD.

2.2 All users shall be required to complete user training and to sign a user agreement prior to, or upon issuance, of a SME PED. A sample copy of the SME PED user agreement is included in the SME PED Security Technical Implementation Guide (STIG) (reference (m)) and can be found at <https://powhatan.iie.disa.mil/stigs/net-sec-guides/>.

SME PED user organizations are encouraged to adapt the sample user agreement to meet their local requirements.

3.0 Classification and Marking

3.1 (FOUO) The SME PED is an unclassified Controlled Cryptographic Item (CCI) when unkeyed. It is also an unclassified CCI when keyed as long as the secure function of the device is disabled (i.e., secure side user password is not entered). However, once the secure function of the device is enabled and password entered, the SME PED is classified and must be handled at the highest level of the key activated on the device.

3.2 (FOUO) Processing classified information at a level higher than the key contained on the SME PED is prohibited and constitutes a security violation that could lead to the compromise of classified information. Please note: there are two crypto keys in the SME PED, one for voice and one for data. Depending on your organization, the level of crypto key may be different for each.

3.3 (FOUO) For security and Operational Security (OPSEC) considerations, SME PEDs shall not be marked with a classification level. Local commands will keep track of devices by using the device's unique serial numbers for accountability purposes.

4.0 General Guidance

4.1 Only cleared, trained, and authorized personnel shall operate SME PEDs. Personnel must possess a security clearance which authorizes access to information at a classification that is equal to or higher than the information being accessed via SME PED, and shall sign a user agreement provided by their local command indicating that they understand the SME PED handling and security requirements, as specified in both the user agreement and this document.

4.2 (FOUO) Admin and User passwords/PINs shall comply with DoD guidelines for strong passwords/pins suitable for the protection of SCI. Admin and User passwords/PINs shall not be written, stored, or otherwise affixed to the SME PED and must be protected at the same level of classification as the information processed on the SME PED. User passwords shall be changed every 60 days, at a minimum. The same password shall not be used for the different domains on the device.

4.3 (FOUO) The Terminal Administrator shall configure the device so a user has at most four consecutive attempts to successfully log into the device, after which the user account will be automatically disabled. To reactivate the device, the SME PED must be returned to the cognizant Terminal Administrator for user account restoration.

4.4 (FOUO) Components shall ensure DoD-approved CAC/PKI certificates are used to authenticate with the Apriva Sensa secure email client while accessing NIPRNET email via the Non-Type 1 operational mode of the SME PED.

4.5 Only NSA may authorize upgrades to the SME PED's operating system, firmware, and encryption software. The SME PED Terminal Administrator shall approve, in advance, all other SME PED software upgrades including third-party software. SME PED software, features and functions can be upgraded via local installation by downloading software from www.securephone.net and using the appropriate software update cable.

4.6 Only applications that have been approved, tested, and digitally signed by the vendor and/or the Terminal Administrator, as stated in paragraph 5.11 of this attachment, can be installed on the SME PED.

4.7 (FOUO) Voice (SCIP) and Data (HAIPE) keys are loaded into the SME PED. SCIP offers the flexibility to talk to four different communities of interest (COI): U.S. National; Combined Communications-Electronic Board ((CCEB), aka, 2nd Parties); NATO Nations; and Coalition Partners. Users and Terminal Administrators should determine ahead of time what communities of interest with which the user will need to interact.

4.8 (FOUO) Appropriately keyed SME PEDs are approved to protect information up to the maximum level of keying material loaded into the device for both secure voice and secure data applications. For secure voice applications, the maximum security level is TOP SECRET SCI. For secure data applications the maximum security level is SECRET. Users shall be explicitly informed of this difference in authorized security level during their initial training and cautioned not to exceed the authorized classification level for all applications.

4.9 (FOUO) Initial keying of SME PEDs shall be performed by an approved COMSEC Custodian.

4.10 (FOUO) Users may re-key SME PEDs over-the-air by placing a call to the Central Facility re-key number. The re-key number is 1-800-218-3238. SME PED re-key is required whenever the key is expired (keys have a one-year crypto period) or as directed by the Central Facility. The SME PED shall allow the electronic re-keying of both SCIP and HAIPE keys. Prior to key expiration users should allow adequate time to re-key the device as the classified operational mode is rendered inoperable whenever keys are expired. Terminal Administrators and users should refer to the vendor specific user manual for more details on how to re-key devices.

5.0 Control and Use Requirements

5.1 (FOUO) The SME PED is a Controlled Cryptographic Item, accountable within the COMSEC Material Control System (CMCS) or other approved CCI tracking systems. Loss, theft, unauthorized use, or tampering must be immediately reported to the Electronic Key Management System Manager/COMSEC custodian, the cognizant Information Security Officer, and the Terminal Administrator, who will further notify the

NSA Information Assurance Insecurities Branch at DSN 244-6811 or commercial 410-854-6811.

5.2 SME PED users shall periodically verify the physical integrity of the SME PED and check for evidence of tampering. Evidence of tampering may include: notification to Admin/User in the device's Trusted Display that the device has been tampered; lifted edges or blemishes on the manufacturer's label under the battery; pry marks on the edges of the device's housing; abnormal behavior of the device; and/or other signs of entry (these may be subtle).

5.3 When transporting SME PEDs which are unkeyed and/or do not have the password entered, they shall be treated as a high dollar value item and protected from loss, theft, unauthorized use, and tampering.

5.4 (FOUO) Newly acquired SME PEDs shall be shipped by the vendor only by authorized modes of transportation as set forth in NSA Central Security Service (NSA-CSS) Policy Manual No. 3-16, dated 5 August 2005 (Reference (j)). SME PEDs must be zeroized by the vendor in accordance with User Manual instructions before initially shipping. SME PEDs may be shipped by the COMSEC Custodian or the Terminal Administrator to the end user only when approved by the Designated Approving Authority (DAA). The SME PEDs shall be treated as a high dollar value item and if ever shipped shall be protected from loss, theft, unauthorized use, and tampering.

5.5 Once the secure function of the device is enabled and password entered, the SME PED is classified and must be handled at the highest level of the key activated on the device.

5.6 (FOUO) Where authorized by local security policy, SME PEDs are allowed in SCIFs when in SCIF mode. DIA will soon release a more specific policy on this topic. SCIF mode has been certified by NSA to disable all transducers, microphones, and Radio Frequency (RF) transmitters thus mitigating the threat to information being transmitted, stored, or processed in a secure facility that would otherwise be created by the SME PED's presence. Specific settings for SCIF Mode operation can be found in the STIG.

5.7 It is the user's responsibility to ensure that sufficient privacy is available to allow the SME PED to be used in classified mode with minimal risk of compromise to classified information. Unless mission requirements dictate otherwise, users shall not discuss, use email, or otherwise process classified or sensitive information outside of a secure area. When using the SME PED outside of a classified area, users shall seclude themselves from the general population when operating the device. When critical mission requirements dictate use in an area of general population, constant vigilance shall be maintained to ensure awareness of surroundings during use (e.g., be aware of the proximity of unauthorized personnel who may be able to overhear conversation or have the ability to view the text screen). Ensuring the protection of classified information is paramount to the operator. The awareness of the operational surroundings includes the operator's cognizance of an adversary's unique capabilities of voice amplification, video

capabilities, and even the use of lip reading. Traditional espionage tradecraft concerns, such as the bugging of hotel rooms, airplanes or meetings rooms shall also be considered. The SME PED was designed to be a mobile device and to meet level 3 requirements of NTISSAM TEMPEST 1/92, "Compromising Emanations Laboratory Test Requirements, Electromagnetics" (Reference (r)) and thus should not be used in environments where more stringent TEMPEST levels are required. Individual countermeasures should include refraining from classified discussions in areas where uncleared individuals are present or where the area is subject to technical attack/bugging. Users shall make every attempt to protect classified information by minimizing the amount of classified information discussed, restricting comments to yes/no answers, and/or covering the mouth.

5.7.1 In accordance with the guidelines above users should consider the following when deciding to use or not to use the SME PED for classified voice and data operations.

5.7.1.1 Use the SME PED when sensitive or mission critical information must be processed, transmitted, or relayed.

5.7.1.2 Use the SME PED when you are in a private location isolated from the public.

5.7.1.3 Use the SME PED in a mission environment only if you can isolate yourself from those without a need-to-know.

5.7.1.4 Use the SME PED, when traveling overseas, in a US facility whenever possible.

5.7.1.5 Do not use the SME PED when you have access to a secure land line or a SIPRNET terminal.

5.7.1.6 Do not use the SME PED outside of a secure area unless you have determined that it is critical to the mission and all other alternatives have been considered.

5.7.1.7 Do not use the SME PED in an open public location or place of business (i.e. grocery store, etc.). Ensure the area is isolated or move to a more secure location.

5.7.1.8 Do not use the SME PED in a taxi, or a rental vehicle or location that may have a wireless remote phone (e.g. On-Star) or listening capability.

5.7.1.9 Do not use the SME PED while taking public transportation (e.g. bus, subway, train).

5.7.1.10 Do not use a SME PED while in an OCONUS residence or hotel that may be insecure.

5.7.1.11 Do not prepare physical notes from classified SME PED conversations, emails, etc., unless there is approved secure government storage available and the notes can be

properly safeguarded (appropriate cover sheets, double wrapping/pouches, and continual personal surveillance and control) until delivered to the storage facility.

5.8 Users shall verify that SME PEDs are operating at the appropriate classification level while in the secure mode, prior to using it for classified voice conversations or classified e-mail, classified web browsing, or creating/viewing classified documents. This is done by observing the trusted display, which displays in real time the mode in which the device is currently operating.

5.9 Users shall not exceed the classification level indicated on the SME PED trusted display. Because different SME PEDs/telephones/terminals may have different maximum classification level settings, the display may indicate a level lower than the maximum classification of the key loaded on the SME PED (for example, if a SME PED with a TOP SECRET key terminal calls a STE/secure terminal with a SECRET key, "SECRET" will be displayed on both terminals as the maximum authorized level of information to be discussed during the call). Therefore, users shall observe the display for each call and limit discussion contents to the classification level presented on the display.

5.10 Contractor activities that own and operate a DoD approved SIPRNET or NIPRNET enclaves are not permitted to install SME PED servers in their enclave. DoD contractors requiring the use of a SME PED to perform authorized duties shall do so through the use of SME PED servers located at an agreed upon DoD enclave.

5.11 Component and DAA's shall be responsible for approval and configuration management of applications installed on the SME PED and shall provide a list of authorized applications to Terminal Administrators. Applications that are not part of the baseline (factory) SME PED configuration shall be tested to ensure they will operate properly in the SME PED environment. These applications must also be digitally signed with the appropriate digital signature in order to be executed by the SME PED; consult with the specific vendor's device user manuals for additional details. Requirements found in DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)" (Reference (h)) apply to any new application installed on the SME PED. Applications that are approved for installation onto the SME PED shall be included as part of the Component's certification and accreditation of the SME PED, per DoDI 8510.01 (Reference (g)).

5.12 The SME PED is considered a mobile extension of the user's local environment. Security and COMSEC policies that pertain to the user organization shall also pertain to the SME PED. As such, access to authorized information and networks allowed to be transferred between DoD Component organizations and foreign nationals or non DoD personnel will be extended to the SME PED in compliance with current operating procedures.

5.13 (FOUO) Antivirus and firewall applications must be NSA approved and Joint Task Force-Global Network Operations (JTF-GNO) authorized for operation on the SME PED

and shall use the latest security updates, patches, and definition files. Upon this issuance, only one antivirus solution is approved for use on the General Dynamics SME PED; a firewall is included as part of the Apriva Sensa software suite. Anti-virus software can be purchased via the NSA IDIQ contract. NSA, in conjunction with the SME PED vendors, will work to find and approve more antivirus solutions. Authorized antivirus and firewall applications that are approved for installation onto the SME PED, shall be included as part of the Component's certification and accreditation of the SME PED, per DoDI 8510.01 (Reference (g)). Component and local DAA's shall be responsible for approval, configuration management updating and maintenance of antivirus and firewall applications on SME PEDs.

5.14 Data stored on the device shall be properly protected based on Data at Rest (DAR) procedures in DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (Reference (p)). It is the SME PED user's responsibility to ensure that DAR is properly encrypted. Users must be aware that DAR encryption is manual with some applications in the unclassified operational mode. Thus, users may have to manually move files to DAR encrypted folders. The Terminal Administrator shall verify that DAR protection is compliant with the STIG, during all security audits. This will provide a mechanism for the Terminal Administrator to validate and ensure that users are appropriately protecting all stored files.

5.15 Terminal Administrators that enable SME PED Desktop synchronization via Universal Serial Bus (USB) shall ensure that users disable SME PED wireless capabilities prior to performing wired Desktop synchronization, by enabling the SCIF mode.

6.0 Administrative Requirements

6.1 If the SME PED is malfunctioning, its appearance has changed, or it has been out of the user's control and the user suspects it may have been compromised, it shall not be used for classified operations or introduced inside areas where classified discussions are held, and it shall be returned immediately to the Terminal Administrator for evaluation.

6.2 The Terminal Administrator shall program the SME PED to automatically lock the screen after periods of inactivity per STIG direction.

6.3 Where the device allows, it is recommended the Terminal Administrator program the SME PED to lock the screen and have the user key-in their PIN for every 30 minutes of continuous use. Local decisions may be made to increase or decrease the setting however, the setting shall not exceed 90 minutes.

6.4 The Terminal Administrator should periodically review audit information and shall conduct a hands-on/visual inventory of SME PEDs in accordance with STIG instructions. Users shall also reaffirm their user agreement as well during the periodic inventory/inspection.

6.5 The Terminal Administrator shall ensure the real time clock is set accurately.

6.6 The Terminal Administrator shall configure the appropriate maximum-security level for both the secure voice and e-mail connections.

6.7 The Terminal Administrator may request that users return the SME PED for any reason. Common reasons for requesting the return may include the need to: Perform SME PED maintenance; conduct software uploads; modify SME PED security parameters; or perform other duties per applicable local security policy and procedures.

7.0 User Responsibilities

7.1 SME PED users shall comply with the guidance in this document and local user agreements. A sample user agreement can be found with the DISA SME PED STIG at <https://powhatan.iie.disa.mil/stigs/net-sec-guides/>. Local commands are encouraged to modify the sample user agreement to best meet their local requirements.

7.2 SME PED users shall be personally responsible for ensuring the proper protection of classified information under their custody and control, per reference (a). SME PED users shall ensure that classified information is not compromised or released to unauthorized individuals by properly handling the SME PED and knowing their environments.

7.3 All personnel issued a SME PED shall sign a local user agreement outlining usage parameters and security restrictions associated with use of a SME PED, concurrent with training and issuance of the SME PED.

7.4 Users shall return the SME PED to the Terminal Administrator upon request.

7.5 Users shall consistently verify the physical integrity of the SME PED and check for evidence of tampering as stipulated in paragraph 5.2 of this attachment. Evidence of tampering shall be immediately reported to the Terminal Administrator and the NSA Information Assurance Insecurities Branch at 410-854-6811.

7.6 The SME PED shall not be left unattended while the user is logged into either the classified or unclassified modes.

7.7 Users shall not perform actions that could promote the release of classified or sensitive information by the device, applications or data storage mechanisms inherent to the SME PED.

7.8 The SME PED contains no user replaceable parts, except the battery, RF Module, and Subscriber Identity Module (SIM) card. Any attempt to open a SME PED, other than to access these user accessible components, automatically voids the warranty and shall be

regarded as a COMSEC incident. Excluding designed user replaceable items (battery, RF SIM card) all defective SME PEDs shall be returned to the Terminal Administrator for repair and/or replacement. User destruction of a defective SME PED is not authorized under non-hostile conditions. Forward all SME PEDs to NSA for destruction upon final disposition in accordance with CNSS No. 4004.1, Annex B (Reference (o)).

7.9 When it becomes necessary to prevent information on the device from being compromised by hostile or other unauthorized persons, the SME PED should be zeroized (or otherwise rendered unusable by the erasure of keying information), in accordance with SME PED user manual instructions. SME PED zeroization actions shall be reported as quickly as possible to the Terminal Administrator and COMSEC Account Manager.

7.10 Upon departing the issuing organization, the SME PED shall be returned to the Terminal Administrator.

8.0 Reportable COMSEC Incidents and Security Violations

8.1 (FOUO) COMSEC incidents, to include evidence of tampering with a keyed or unkeyed SME PED, unauthorized access to a keyed or unkeyed SME PED, or loss or theft of a keyed or unkeyed SME PED shall be immediately reported to the Terminal Administrator and COMSEC custodian who will notify the NSA Information Assurance Insecurities Branch at 410-854-6811.

8.2 (FOUO) Should a SME PED be reported lost, in addition to reporting the loss as a COMSEC incident, the Terminal Administrator must immediately remove the SME PED account from the local SME PED enclave Servers, contact the commercial wireless carrier to deactivate service to the device, and notify the DISA DISN Customer Call Center (DCCC) at 1-800-554-DISN (3476). The DCCC will open a trouble ticket and contact the MCEP to have the device terminated at the MCEP. The DCCC is a 24x7 center/function.

8.3 Any potential or actual compromise of classified information shall be reported immediately to the local security officer and investigated in accordance with guidance provided in Reference (a).

9.0. COMSEC Requirements

9.1 (FOUO) SME PED units will be accounted for in the COMSEC Material Control System as an Accounting Legend Code (ALC) 1 item, as appropriate.

9.2 (FOUO) SME PED end user COMSEC training will be provided and documented along with completion of a risk assessment certificate before issuing SME PEDs to end users.

REFERENCES

- (a) DoD Instruction 5200.01, Information Security Program and Protection of Sensitive Compartmented Information, dated October 9, 2008
- (b) DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), dated April 14, 2004
- (c) ASD(NII) Memorandum, Use of Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG), dated June 2, 2006
- (d) DoD Directive 8500.01E, Information Assurance (IA), dated October 24, 2002
- (e) DoD Instruction 8500.2, Information Assurance (IA) Implementation, dated February 6, 2003
- (f) DoD Directive 8520.1, Protection of Sensitive Compartmented Information (SCI), dated December 20, 2001
- (g) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated November 28, 2007
- (h) DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM), dated August 13, 2004
- (i) Federal Information Processing Standard (FIPS) Publication 140-2, dated December 3, 2002
- (j) NSA Central Security Service (NSA-CSS) Policy Manual No. 3-16, Control of Communications Security (COMSEC) Material, dated August 5, 2005.
- (k) Operational Security Doctrine for the Secure Mobile Environment (SME) Portable Electronic Device (PED), DOC-006-07, dated December 2007
- (l) DISA SME PED Data Services Concept of Operations, dated February 19, 2008
- (m) DISA Wireless STIG, Secure Mobile Environment – Portable Electronic Device (SME PED) Checklist, V1R1.1, dated Jul 24, 2008.
- (n) DISA SME PED IP Address Assignment Tactics, Techniques and Procedures, dated September 24, 2008
- (o) CNSS No 4004.1 Annex B, Destruction and Emergency Protection Procedures for COMSEC and Classified Material, dated August 2006, with Amended Annex B dated January 9, 2008

(p) DoD Chief Information Officer Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, dated July 3, 2007

(q) CNNS Policy No 17, National Information Assurance Policy on Wireless Capabilities, dated August 2005

(r) National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetics", dated December 15, 1992

GLOSSARY

Classified Message Incident (CMI): A situation that occurs when a classified message is found on an unclassified system. A Classified Message Incident (CMI) or “data spill” occurs on the SME PED when a classified email is inadvertently sent on the NIPRNet and received on a unclassified/Black PDA of the SME PED or classified email with a classification higher than the classification level of the Type 1 key is inadvertently sent on the SIPRNet and received on the Red PDA of a SME PED.

COMSEC Custodian: An individual who assumes accountability for the COMSEC equipment or material. Upon receipt of COMSEC equipment or material the individual controls its dissemination ensuring that only authorized individuals based on job requirements and a need-to-know basis are issued the COMSEC equipment or material.

Controlled Cryptographic Item (CCI): National Security Agency term for secure telecommunications or information handling equipment, associated cryptographic component, or other hardware item which performs a critical COMSEC function. Items so designated may be unclassified but are subject to special accounting controls and required markings. Part of the physical security protection given to COMSEC equipment and material is afforded by its special handling and accounting. The COMSEC Material Control System is used to distribute accountable COMSEC items such as classified and CCI equipment, keying material, and maintenance manuals.

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

Designated Approving Authority (DAA): The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

High Assurance Internet Protocol Encryptor (HAIPE): A device that provides networking, traffic protection, and management features ensuring information assurance (IA) services on an IPv4/IPv6 network.

Indefinite Delivery/Indefinite Quantity (IDIQ): A type of contract that provides for an indefinite quantity of supplies or services during a fixed period of time. The Government places delivery orders (for supplies) or task orders (for services) against a basic contract for individual requirements. The Government uses an IDIQ contract when it cannot predetermine, above a specified minimum, the precise quantities of supplies or services that the Government will require during the contract period.

Initial Operating Capability (IOC): The first attainment of the capability to effectively employ a device. In the case of the SME PED IOC was declared after security and operational testing indicated that device operated sufficiently to support stated requirements.

Multi-Carrier Entry Point (MCEP): Supports the operational deployment of the SME PED with a complex multi-network and multi-application environment. It provides the interface to multiple wireless carriers, and provides Type 1 and non Type 1 S/MIME message traffic routing in support of data services provided on the SME PED.

Secure Communications Interoperability Protocol (SCIP): The U.S. Government's standard for secure voice and data communication

Secure / Multipurpose Internet Mail Extensions (S/MIME): A standard for public key encryption and signing of e-mail encapsulated in MIME.

Security Technical Implementation Guide (STIG): Standardized security implementation guidance outlining the configuration standards for DOD IA and IA-enabled devices/systems. STIGs are developed by DISA and mandated for use within the DoD. STIGs provide specific security settings and suggested optional settings to minimize the security risks associated with computer hardware, software, or applications that are widely used within the DoD.

Terminal Administrator (TA): The individual responsible for the configuration of the SME PED security features and terminal capabilities, upgrading terminal software, establishing and restoring User Accounts, and inspecting of the terminal's physical integrity. The TA secure password allows the TA to access a SME PED's TA functionality. Using the TA functionality, the TA may disable any of the following applications on the SME PED: clear voice, secure voice, clear data, or secure data.

Type 1: Classified voice or data information.

Non-Type 1: Sensitive but unclassified voice or data information.

ACRONYMS

ALC	Accounting Legend Code
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
CAC	Common Access Card
CCAO	Classified Connection Approval Office
CCEB	Combined Communications-Electronics Board
CCI	Controlled Cryptographic Item
CMCS	COMSEC Material Control System
CMI	Classified Message Incident
COMSEC	Communications Security
CONOPS	Concept of Operations
DAA	Designated Approving Authority
DAR	Data at Rest
DCCC	DISN Customer Call Center
DECC	Defense Enterprise Computing Center
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	Department of Defense Chief Information Officer
DRSN	Defense Red Switch Network
DSAWG	Defense IA/Security Accreditation Working Group
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FSO	Facility Security Officer
GD	General Dynamics
HA�PE	High Assurance Internet Protocol Encryptor
IA	Information Assurance
IDIQ	Indefinite Delivery/Indefinite Quantity
IOC	Initial Operational Capability
IPT	Integrated Process Team
JTF-GNO	Joint Task Force-Global Network Operations
MCEP	Multi Carrier Entry Point
MIPR	Military Interdepartmental Purchase Request
MOA	Memorandum of Agreement
NSA	National Security Agency
NSA-CSS	NSA Central Security Service
OPSEC	Operational Security
PKI	Public Key Infrastructure
RF	Radio Frequency
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIP	Secure Communications Interoperability Protocol
SIM	Subscriber Identity Module
SME PED	Secure Mobile Environment Portable Electronic Device
STE	Secure Terminal Equipment

STIG
VOSIP

Secure Technical Implementation Guide
Voice Over Secure Internet Protocol