



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MEDICAL DEPARTMENT
2050 WORTH ROAD
FORT SAM HOUSTON, TX 78234-6000

OTSG/MEDCOM Policy Memo 04-008

MCIM

18 Jun 04

Expires 18 Jun 06

MEMORANDUM FOR

Commanders, U.S. Army Medical Command Major Subordinate Commands
Director, DoD Executive Agencies Directorate, Office of The Surgeon General,
5109 Leesburg Pike, Falls Church, VA 22041-0054
Directors, OTSG/MEDCOM

SUBJECT: Transmission of Protected Health Information (PHI) Via Electronic-Mail (E-mail)

1. References:

a. Message, DCIO/G6, 022019Z Sep 03, subject: UCLAS ALARACT 114/2003 Army Public Key Infrastructure (PKI) Usage Guidance for Encryption and Digital Signing of E-Mail Messages, Enclosure 1.

b. Memorandum, Office of The Surgeon General, DASG-IMD, 11 June 2002, subject: Transmission of Patient Identifiable Medical Data Via Electronic Mail (E-mail), Enclosure 2.

c. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Health Insurance Reform: Security Standards (45 CFR Parts 160, 162, and 164), Federal Register, Vol. 68, No. 34, 20 February 2003.

d. Memorandum, Office of the Secretary of the Army, NEST-EST-A, 10 September 2003, subject: Update to Common Access Card (CAC)/Public Key Infrastructure (PKI) Implementation, Enclosure 3.

2. Purpose: This memorandum rescinds reference 1b, due to changes in the Department of Defense (DoD) and Department of Army (DA) guidance for encryption of e-mail and prescribes policies for securing e-mail that contains PHI.

3. Proponent: The proponent for this policy is the Chief Information Officer (CIO).

MCIM

SUBJECT: Transmission of Protected Health Information (PHI) Via Electronic Mail (E-mail)

4. Responsibilities:

a. This policy is applicable to all OTSG or all MEDCOM staff that are required to transmit PHI using e-mail.

b. All staff transmitting PHI using e-mail will follow the policies and procedures stated below.

c. These policies do not apply to PHI transmitted over the Military Health System (MHS) Virtual Private Network (VPN)(this data is automatically encrypted by the network), transmissions to commercial accounts or doctor to patient communications. Transmissions to commercial accounts will be over VPN or other protected means. Doctor to patient communications will be through TRICARE Online, when this is available.

5. Policy:

a. Effective immediately, all e-mail to and from an “.amedd.army.mil” account will be encrypted, if it contains PHI. The use of encrypted e-mails to transmit PHI is consistent with the HIPAA Security Rule standards and DoD and DA guidance for the transmission of sensitive information.

b. The DA requires that e-mails containing PHI be encrypted using the Common Access Card (CAC) and DoD public key (PK) certificates. Additional guidance for sending, receiving, and retaining encrypted e-mails is at Enclosure 1.

6. Procedures:

a. The CACs and card readers are available locally. Personnel needing CAC readers installed should contact their Director of Information Management or Information Technology staff. Priority for distribution of the CAC and installation of the card readers should be given to personnel who routinely transmit e-mails containing PHI.

b. In addition to the encryption requirement, a confidentiality notice should be inserted on e-mails containing PHI. A copy of the confidentiality notice is at Enclosure 4.

MCIM

SUBJECT: Transmission of Protected Health Information (PHI) Via Electronic Mail (E-mail)

c. Our points of contact are Ms. Sandra Parker, Office of the Assistant Chief of Staff for Information Management (OACSIM), (210) 221-7918, for PKI policy issues; Mr. Ross Roberts, OACSIM, (210) 221-7869, for HIPAA Security issues; and Mr. Larry Simmons, Contractor, U.S. Army Medical Information Technology Center, (210) 637-2308, for PKI technical assistance.

FOR THE COMMANDER:

4 Encls
as



KENNETH L. FARMER, JR.
Major General
Chief of Staff

AAUZELX RUEADWD6617 2452030-UUUU--RUEACOE.

ZNR UUUUU

P 031859Z SEP 03

FM PTC EMAIL SYSTEM WASH DC

INFO RUEACOE/DA EMAIL CUSTOMER//CEHECIM/COE//

P 022019Z SEP 03 ZEL

FM DA WASHINGTON DC//DCIO/G6//

TO ALARACT

BT

UNCLAS ALARACT 114/2003 SECTION 1 OF 2

SUBJECT: UNCLAS ALARACT 114/2003 ARMY PUBLIC KEY INFRASTRUCTURE (PKI) USAGE

GUIDANCE FOR ENCRYPTION AND DIGITAL

SIGNING OF E-MAIL MESSAGES

OTHERORG

UNCLASSIFIED//

ALARACT 114/2003

THE CHIEF INFORMATION OFFICER/G-6 RELEASES THE FOLLOWING MESSAGE EFFECTIVE IMMEDIATELY:

SUBJECT: ARMY PUBLIC KEY INFRASTRUCTURE (PKI) USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES

REFERENCES

- A. MESSAGE, HQDA, SAIS-ZA, 031830Z MAY 02, SUBJECT: UNCLAS ALARACT 0048/2002, ARMY PUBLIC KEY INFRASTRUCTURE (PKI) USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES.
- B. AR 25-1, ARMY INFORMATION MANAGEMENT, 31 MAY 02.

PAGE 02 RUEADWD6617 UNCLAS

C. MEMORANDUM, ASD(C3I), SUBJECT: DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI), 12 AUG 00.

D. MEMORANDUM, ASD(C3I), SUBJECT: PUBLIC KEY INFRASTRUCTURE (PKI) POLICY UPDATE, 21 MAY 02.

E. UNITED STATES CODE, TITLE 5, PART I, CHAPTER 5, SUBCHAPTER II, SUB SECTION 552A, THE PRIVACY ACT OF 1974, 27 SEP 75.

F. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, "STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION" [45 CFR PARTS 160 AND 164], FEDERAL REGISTER, VOL. 65, NO. 250, 28 DEC 00.

G. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA), SUBJECT: RECORDS MANAGEMENT GUIDANCE FOR AGENCIES IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES, 18 OCT 00.

H. NARA BULLETIN 2003-04, AVAILABILITY OF ELECTRONIC RECORDS MANAGEMENT GUIDANCE FOR PUBLIC KEY INFRASTRUCTURE (PKI)-RELATED ADMINISTRATIVE RECORDS, 27 MAR 03.

1. PURPOSE AND SCOPE. THIS MESSAGE SUPERCEDES REFERENCE A AND PROVIDES UPDATED ARMY GUIDANCE FOR THE USE OF BOTH HARDWARE BASED AND SOFTWARE BASED DOD PUBLIC KEY CERTIFICATES TO DIGITALLY SIGN AND/OR ENCRYPT E-MAIL MESSAGES IN ACCORDANCE

PAGE 03 RUEADWD6617 UNCLAS

WITH (IAW) REFERENCES B, C, AND D.

2. USING DIGITAL SIGNATURES.

A. SENDING DIGITALLY SIGNED E-MAILS. AS A GENERAL RULE IN THE ARMY, A PKI

Encl

DIGITAL SIGNATURE SHOULD BE USED WHENEVER E-MAIL IS CONSIDERED OFFICIAL BUSINESS AND/OR CONTAINS SENSITIVE INFORMATION IAW REFERENCES E OR F. THE DIGITAL SIGNATURE PROVIDES ASSURANCES THAT THE INTEGRITY OF THE MESSAGE HAS REMAINED INTACT IN TRANSIT, AND PROVIDES FOR THE NON-REPUDIATION OF THE MESSAGE THAT THE SENDER CANNOT LATER DENY HAVING ORIGINATED THE E-MAIL.

B. RECEIVING DIGITALLY SIGNED E-MAILS. PRIOR TO OPENING AN INCOMING PKI DIGITALLY SIGNED E-MAIL, ARMY E-MAIL USERS SHOULD ASSESS THE ATTACHED DIGITAL SIGNATURE'S LEVEL OF ASSURANCE. E-MAILS SIGNED USING REVOKED CERTIFICATES SHOULD BE TREATED AS NOT HAVING ORIGINATED FROM THE INDICATED SENDER. VALID PKI DIGITAL SIGNATURES ORIGINATING OUTSIDE DOD DOMAINS MUST BE GENERATED BY AN APPROVED DOD PKI CERTIFICATE SOURCE (E.G., EXTERNAL CERTIFICATE AUTHORITY). E-MAILS THAT ARE DIGITALLY SIGNED BY UNAPPROVED SOURCES SHOULD ONLY BE OPENED, READ, AND ACTED UPON WITH CAUTION.

PAGE 04 RUEADWD6617 UNCLAS

C. RETAINING DIGITALLY SIGNED E-MAIL. AGENCIES MUST ACCOMMODATE THE PRESERVATION NEEDS IF A DIGITALLY SIGNED RECORD REQUIRES TEMPORARY OR PERMANENT PRESERVATION IAW REFERENCE G. THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) REQUIRES THAT AN AGENCY CHOOSE AN APPROACH THAT IS PRACTICAL AND FITS BUSINESS NEEDS AND RISK ASSESSMENT. AS THE FUNCTIONAL PROponent FOR RECORDS MANAGEMENT, THE OFFICE OF THE DEPUTY CHIEF OF STAFF/G-1 (ODCS/G-1) ARMY RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY HAS DETERMINED THE MINIMUM STANDARDS FOR PRESERVATION OF DIGITALLY SIGNED E-MAIL. ADDITIONAL INFORMATION REGARDING MINIMUM REQUIREMENTS MAY BE FOUND IN REFERENCES G AND H, AND AT THE US ARMY RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WEBSITE: [HTTPS://WWW.ARIMS.ARMY.MIL](https://www.arims.army.mil).

3. ENCRYPTION OF E-MAILS.

A. SENDING ENCRYPTED E-MAILS. DATA IS ENCRYPTED TO ENSURE CONFIDENTIALITY. HOWEVER, DATA CONFIDENTIALITY RESULTS WHEN ONLY THE INTENDED RECIPIENT CAN DECRYPT ENCRYPTED INFORMATION. IAW REFERENCE C, ALL DOD E-MAIL THAT REQUIRES ENCRYPTION MUST USE, AT A MINIMUM, DOD CLASS 3 ENCRYPTION CERTIFICATES. ENCRYPTION USES A GREATER AMOUNT OF BANDWIDTH THAN DIGITAL

PAGE 05 RUEADWD6617 UNCLAS

SIGNATURE. THEREFORE, ENCRYPTED E-MAILS SHOULD BE THE EXCEPTION, NOT THE RULE AND SHOULD ONLY BE USED TO SEND (1) SENSITIVE INFORMATION; (2) INFORMATION PROTECTED BY THE PRIVACY ACT OF 1974 (REFERENCE E); (3) INFORMATION PROTECTED UNDER REFERENCE F, THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA).

B. RECEIVING ENCRYPTED E-MAILS. WHEN AN ENCRYPTED E-MAIL IS RECEIVED WITHIN A DOD DOMAIN, RECIPIENTS MUST TAKE APPROPRIATE MEASURES TO PROTECT THE ENCRYPTED INFORMATION. IF A MESSAGE HAS BEEN ENCRYPTED, THE IMPLICATION IS THAT IT CONTAINS SENSITIVE INFORMATION THAT NEEDED TO BE PROTECTED DURING TRANSMISSION. ONCE IT HAS BEEN RECEIVED, THE NEED TO PROTECT

THE INFORMATION REMAINS.

C. RETAINING ENCRYPTED E-MAIL. E-MAILS THAT ARE RECEIVED IN ENCRYPTED FORM AND CONTAIN SENSITIVE INFORMATION NEED TO BE STORED IN ENCRYPTED FORM TO ENSURE APPROPRIATE PROTECTION OF THE INFORMATION. IT SHOULD BE NOTED THAT STORAGE (AND SUBSEQUENT RETRIEVAL) OF ENCRYPTED E-MAIL TAKES ADDITIONAL TIME AND SPACE AND MAY REQUIRE IMPROVED STORAGE DEVICES. ENCRYPTED E-MAIL RECEIVED THAT DOES NOT CONTAIN SENSITIVE INFORMATION, OR

PAGE 06 RUEADWD6617 UNCLAS

INFORMATION PROTECTED BY REFERENCES E AND F, (THE PRIVACY ACT OR THE HIPAA PRIVACY RULE) SHOULD BE STORED UNENCRYPTED.

INFORMATION ON DECRYPTING AND STORING UNENCRYPTED E-MAIL CAN BE FOUND AT [HTTPS://SETDWEB.SETD.ARMY.MIL/SUPPORT/ADDLRESOURCES.HTM](https://setdweb.setd.army.mil/support/addlresources.htm).

FURTHER ASSISTANCE CAN OBTAINED BY CALLING THE ARMY SET-D HELP DESK AT (866) SET-DCAC (738-3222). IN ACCORDANCE WITH REFERENCE G, AGENCIES SHOULD DEVELOP RECORDS SCHEDULES AND PROPOSED RETENTION PERIODS FOR NEW RECORDS FOR NARA TO REVIEW; HOWEVER, IF THE RECORDS ARE ALREADY SCHEDULED, THEY WOULD NOT NEED TO BE RESCHEDULED BECAUSE THEY WERE ENCRYPTED THE SAME RETENTION WOULD APPLY IN BOTH CASES. THE ODCS/G-1, RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WILL DETERMINE APPROPRIATE RECORDS RETENTION ACTIONS REGARDING ENCRYPTED E-MAILS. USERS SHOULD BE AWARE THAT IF THEIR CAC OR SOFTWARE-BASED PKI TOKEN WERE LOST, OPENING STORED/SAVED-ENCRYPTED E-MAIL WOULD NOT BE POSSIBLE WITHOUT RECOVERY OF THEIR PRIVATE KEY.

UNCLAS ALARACT 114/2003 FINAL SECTION OF 2

SUBJECT: ARMY PUBLIC KEY INFRASTRUCTURE

DESK AT (866) SET-DCAC (738-3222). IN ACCORDANCE WITH REFERENCE G, AGENCIES SHOULD DEVELOP RECORDS SCHEDULES AND PROPOSED RETENTION PERIODS FOR NEW RECORDS FOR NARA TO REVIEW; HOWEVER, IF THE RECORDS ARE ALREADY SCHEDULED, THEY WOULD NOT NEED TO BE RESCHEDULED BECAUSE THEY WERE ENCRYPTED THE SAME RETENTION WOULD APPLY IN BOTH CASES. THE ODCS/G-1, RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WILL DETERMINE APPROPRIATE RECORDS RETENTION ACTIONS REGARDING ENCRYPTED E-MAILS. USERS SHOULD BE AWARE THAT IF THEIR CAC OR SOFTWARE-BASED PKI TOKEN WERE LOST, OPENING STORED/SAVED-ENCRYPTED E-MAIL WOULD NOT BE POSSIBLE WITHOUT RECOVERY OF THEIR PRIVATE KEY.



DEPARTMENT OF THE ARMY
OFFICE OF THE SURGEON GENERAL
5109 LEECHBURG PIKE
FALLS CHURCH VA 22041-3258

REF:VTO
ATTENTION OF:

11 JUN 2002

DASG-IMD

MEMORANDUM FOR Commanders, U.S. Army MEDCOM Major Subordinate
Commands/Activities/Installations
Chiefs, Staff Offices

SUBJECT: Transmission of Patient Identifiable Medical Data via
Electronic-Mail (E-Mail)

1. There is a recognized requirement for the U.S. Army Medical Department senior leadership to receive timely patient information associated with deployments and military operations. Such data are not envisioned to be a patient medical record or abstract, but rather patient identification, cause of injury or nature of illness, severity, prognosis, planned disposition, and the like. Although, essential for the successful conduct of deployments and military operations, such medical data must nonetheless be afforded appropriate security and protections. Transfer and release of such data must also meet the requirements set forth by the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Army Regulation 40-66, paragraph 2-4a(1).

2. Secure e-mail will be used to transmit essential patient identifiable medical data outside established reporting systems and is restricted to mission or operation-essential requirements. These e-mails will be restricted to the smallest number of users feasible. Pending final guidance as to the specific requirements associated with the exclusion the Armed Forces are granted under HIPAA, the following interim guidance is provided:

a. The Department of Defense Public Key Infrastructure (PKI) certified e-mail provides the security such medical data warrants and meets current HIPAA guidance. Accordingly, patient data transfer via e-mail will be accomplished using PKI-certified transmissions exclusively.

Encl 2

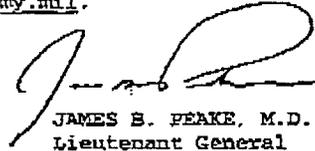
DASG-IMD

SUBJECT: Transmission of Patient Identifiable Medical Data Via Electronic-Mail (E-Mail)

D. Once received via secure, PKI-certified e-mail, patient data will be afforded the same protection and handling as that of all other medical data. The message will include a "confidentiality notice" which will address the redisclosure and destruction of disclosed information at Enclosure.

3. My point of contact is COL Barclay Butler, Assistant Chief of Staff for Information Management, DSN 761-8286 or Commercial (703) 681-8285, or email address: Barclay.Butler@otsq.amedd.army.mil.

Encl
as



JAMES B. PEAKE, M.D.
Lieutenant General
The Surgeon General

CONFIDENTIALITY NOTICE

DA policy mandates that the confidentiality of patient medical information and medical records will be protected to the fullest extent possible. Patient medical information and medical records will be released only if authorized by law and regulation. See paragraph 2-2, AR 40-66 for details.

Encl

NEST-EST-A

SUBJECT: Common Access Card (CAC)/Public Key Infrastructure (PKI) Implementation

Personnel must bind their PKI certificates to their AKO email account. It is the intent of the Chief Information Officer (CIO)/G-6 that no full-time soldier, civilian or contractor will have full access to Army networks without an AKO email account as the default reply address, a CAC issued under the AKO email address, and a CAC reader (limited access still possible on a case by case basis with userid & password and wartime exemptions will be made). Although some locations have been granted the authority to issue CACs without PKI certificates in order to facilitate mobilization, leaders at these locations are not relieved from meeting the CIO/G-6 intent.

7. The aggressive execution of this guidance is essential in securing the Army's communication infrastructure. We ask all Commanders identify this issue as an OER line item for all subordinate leaders and as a critical element of success for all civilian personnel in positions of authority.

8. DOIMs and Regional Chief Information Officers (RCIOs) must report CAC reader installation progress on a weekly basis via the Program Manager Secure Electronic Transactions-Devices (PM SET-D) website (<https://setdweb.setd.army.mil>). Help desk support is also available (Monday – Friday 0600-2100 EST) to assist the fielding effort (1-866-738-322).

9. The points of contact for this memorandum are: Ms. Susan Maks, 703-601-1933, susan.maks@us.army.mil (CIO/G6); MSG James M. Stover, 703-428-1233, james.stover@us.army.mil (DCS, G-1); and Mr. Lester Echols, 703-692-9247, lester.echols@us.army.mil (OACSIM).

JOHN M. LE MOYNE
Lieutenant General, GS
Deputy Chief of Staff G-1

PETER M. CUVIELLO
Lieutenant General, GS
Chief Information Officer/G-6

LARRY L. LOST
Major General, GS
Assistant Chief of Staff
for Installation Management

NEST-EST-A

SUBJECT: Common Access Card (CAC)/ Public Key Infrastructure (PKI)
Implementation

DISTRIBUTION:

UNDER SECRETARY OF THE ARMY

VICE CHIEF OF STAFF, ARMY

SERGEANT MAJOR OF THE ARMY

ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND
TECHNOLOGY), ATTN: SALT

ASSISTANT SECRETARY OF THE ARMY (CIVIL WORKS), ATTN: SACW

ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT AND
COMPTROLLER), ATTN: SAFM

ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS AND ENVIRONMENT),
ATTN: SAIL

ASSISTANT SECRETARY OF THE ARMY (MANPOWER AND RESERVE AFFAIRS),
ATTN: SAMR

GENERAL COUNSEL, ATTN: SAGC

ADMINISTRATIVE ASSISTANT TO THE SECRETARY OF THE ARMY, ATTN: SAAA

CHIEF INFORMATION OFFICER/G-6, ATTN: SAIS-ZA

THE INSPECTOR GENERAL, ATTN: SAIG-ZA

THE AUDITOR GENERAL, ATTN: SAAG-ZA

DEPUTY UNDER SECRETARY OF THE ARMY, ATTN: SAUS

DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS AND RESEARCH),
ATTN: SAUS-OR

CHIEF OF LEGISLATIVE LIAISON, ATTN: SALL

CHIEF OF PUBLIC AFFAIRS, ATTN: SAPA-ZA

DIRECTOR, SMALL AND DISADVANTAGED BUSINESS UTILIZATION, ATTN:
SADBU

DIRECTOR OF THE ARMY STAFF, ATTN: DACS-ZD

DEPUTY CHIEF OF STAFF, G-1, ATTN: DAPE-ZA

DEPUTY CHIEF OF STAFF, G-2, ATTN: DAM 1-ZA

DEPUTY CHIEF OF STAFF, G-3, ATTN: DAMO-ZA

DEPUTY CHIEF OF STAFF, G-4, ATTN: DALO-ZA

DEPUTY CHIEF OF STAFF, G-8, ATTN: DAPR-ZA

ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT, ATTN: DAIM-
ZA

CHIEF OF ENGINEERS, ATTN: DAEN-ZA

THE SURGEON GENERAL, ATTN: DASG-ZA

CHIEF, NATIONAL GUARD BUREAU, ATTN: NGB-ZB

CHIEF, ARMY RESERVE, ATTN: DAAR-ZA

THE JUDGE ADVOCATE GENERAL, ATTN: DAJA-ZA

CHIEF OF CHAPLAINS, ATTN: DACH-ZA

(CONT)

NEST-EST-A

SUBJECT: Common Access Card (CAC)/ Public Key Infrastructure (PKI)
Implementation

DISTRIBUTION: (CONT)

COMMANDER

U.S. ARMY EUROPE AND SEVENTH ARMY, ATTN: AEACG

EIGHTH U.S. ARMY, ATTN: EACG

U.S. ARMY FORCES COMMAND, ATTN: AFCG

U.S. ARMY TRAINING AND DOCTRINE COMMAND, ATTN: ATCG

U.S. ARMY MATERIEL COMMAND, ATTN: AMCCG

U.S. ARMY CORPS OF ENGINEERS, ATTN: CECG

U.S. ARMY SPECIAL OPERATIONS COMMAND, ATTN: AOCG

U.S. ARMY PACIFIC, ATTN: APCG

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND, ATTN: IACG

U.S. ARMY MILITARY TRAFFIC MANAGEMENT COMMAND, ATTN: MTCG

U.S. ARMY CRIMINAL INVESTIGATIVE COMMAND, ATTN: CICG-ZA

U.S. ARMY MEDICAL COMMAND, ATTN: DASG-ZA

U.S. ARMY MILITARY DISTRICT OF WASHINGTON, ATTN: ANCG

U.S. ARMY SOUTH, ATTN: SOCG

U.S. ARMY TEST AND EVALUATION COMMAND, ATTN: CSTE

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND, ATTN: SMDC-ZA

SUPERINTENDENT, U.S. MILITARY ACADEMY, ATTN: MASP

PROGRAM EXECUTIVE OFFICER

AVIATION

GROUND COMBAT AND SUPPORT SYSTEMS

COMMAND, CONTROL, COMMUNICATIONS SYSTEMS

INTELLIGENCE, ELECTRONIC WARFARE AND SENSORS

STANDARD ARMY MANAGEMENT INFORMATION SYSTEMS

TACTICAL MISSILES

AIR AND MISSILE DEFENSE

PROGRAM MANAGER

CHEMICAL DEMILITARIZATION

JOINT SIMULATION SYSTEMS

MISSILE DEFENSE AGENCY

CONFIDENTIALITY NOTICE

This document may contain information covered under the Privacy Act, 5 USC 552(a), and/or the Health Insurance Portability and Accountability Act (PL 104-191) and its various implementing regulations and must be protected in accordance with those provisions. Healthcare information is personal and sensitive and must be treated accordingly. If this correspondence contains healthcare information it is being provided to you after appropriate authorization from the patient or under circumstances that don't require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Redisclosure without additional patient consent or as permitted by law is prohibited. Unauthorized redisclosure or failure to maintain confidentiality subjects you to application of appropriate sanction. If you have received this correspondence in error, please notify the sender at once and destroy any copies you have made.

Encl 4