P 262121Z FEB 09
FM PTC WASHINGTON DC//ALARACT//
TO ALARACT
ZEN/RMY/OU=ORGANIZATIONS/OU=ADDRESS LISTS/CN=AL ALARACT(UC)
BT
UNCLAS

QQQQ
********* THIS IS A COMBINED MESSAGE *********
SUBJ: ALARACT 050/2009 PERSONALLY IDENTIFIABLE INFORMATION (PII) INCI
DENT REPORTING AND NOTIFICATION PROCEDURES
UNCLASSIFIED//
THIS MESSAGE HAS BEEN SENT BY THE PENTAGON TELECOMMUNICATIONS CENTER
 ON BEHALF OF DA WASHINGTON DC//CIO-G6//
SUBJ: PERSONALLY IDENTIFIABLE INFORMATION (PII) INCIDENT REPORTING
 AND NOTIFICATION PROCEDURES.
REF A. DEPARTMENT OF DEFENSE MEMORANDUM, 21 SEP 07, SUBJECT:
 SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY
 IDENTIFIABLE INFORMATION (PII).
1. THE ARMY CONTINUES TO IMPLEMENT POLICIES AND PRACTICES TO
 SAFEGUARD THE PII OF ITS PERSONNEL AND THEIR FAMILIES. PART OF THIS
 PROCESS IS TO PROPERLY REPORT THE SUSPECTED OR ACTUAL LOSS OF THIS
 INFORMATION AND TO NOTIFY THOSE IMPACTED SO THEY CAN PROPERLY
 SAFEGUARD AGAINST IDENTITY THEFT.
2. PII IS ANY INFORMATION ABOUT AN INDIVIDUAL WHICH CAN BE USED TO
 DISTINGUISH OR TRACE AN INDIVIDUAL'S IDENTITY SUCH AS NAME, SOCIAL
 SECURITY NUMBER, DATE AND PLACE OF BIRTH, MOTHER'S MAIDEN NAME, AND
 BIOMETRIC RECORDS. THIS INFORMATION CAN BE IN HARD COPY (PAPER COPY
 FILES) OR ELECTRONIC FORMAT, STORED ON PERSONAL COMPUTERS, LAPTOPS,
 AND PERSONAL ELECTRONIC DEVICES SUCH AS BLACKBERRIES AND FOUND
 WITHIN DATABASES. THIS INCLUDES BUT IS NOT LIMITED TO, EDUCATION
 RECORDS, FINANCIAL TRANSACTIONS, MEDICAL FILES, CRIMINAL RECORDS, OR
 EMPLOYMENT HISTORY.
3. A BREACH/COMPROMISE INCIDENT OCCURS WHEN IT IS SUSPECTED OR
 CONFIRMED THAT PII IS LOST, STOLEN, OR OTHERWISE AVAILABLE TO
 INDIVIDUALS WITHOUT A DUTY RELATED OFFICIAL NEED TO KNOW. THIS
 INCLUDES, BUT IS NOT LIMITED TO, POSTING PII ON PUBLIC-FACING
 WEBSITES; SENDING VIA EMAIL TO UNAUTHORIZED RECIPIENTS; PROVIDING
 HARD COPIES TO INDIVIDUALS WITHOUT A NEED TO KNOW; LOSS OF
 ELECTRONIC DEVICES OR MEDIA STORING PII (I.E., LAPTOPS, THUMB
 DRIVES, CD'S, ETC.); USE BY EMPLOYEES FOR UNOFFICIAL BUSINESS; AND
 ALL OTHER UNAUTHORIZED ACCESS TO PII.
4. ALL ARMY COMMANDS (ACOM), ARMY SERVICE COMPONENT COMMANDS (ASCC),
 DIRECT REPORTING UNITS (DRU), ARMY STAFF, PROGRAM EXECUTIVE OFFICES
 (PEOS), AND AGENCIES WILL ENSURE REPORTING AND NOTIFICATION OCCURS
 IAW THE FOLLOWING PROCEDURES.
4.1. REPORT ALL INCIDENTS INVOLVING THE ACTUAL OR SUSPECTED
 BREACH/COMPROMISE OF PII TO THE UNITED STATES COMPUTER EMERGENCY
 READINESS TEAM (US-CERT) WITHIN ONE HOUR OF DISCOVERY AT
 HTTP://WWW.US-CERT.GOV. IF COMPUTER ACCESS IS NOT AVAILABLE, PII
 INCIDENTS CAN BE REPORTED TO A 24/7 TOLL FREE NUMBER AT
 1-866-606-9580 FROM THE OFFICE OF THE ADMINISTRATIVE ASSISTANT (OAA)

TO THE (SEC) OF THE ARMY OR US-CERT AT (703) 235-5110 WHICH IS ALSO MONITORED 24/7. IN MOST INSTANCES, THE INDIVIDUAL DISCOVERING THE INCIDENT SHOULD REPORT DIRECTLY TO THE US-CERT IN ORDER TO MEET THE ONE HOUR TIMELINE. AT THE SAME TIME, AN EMAIL SHOULD BE SENT TO PII.REPORTING@US.ARMY.MIL, WHICH NOTIFIES ARMY LEADERSHIP THAT AN INITIAL REPORT HAS BEEN SUBMITTED. THIS EMAIL SHOULD INCLUDE THE US-CERT REPORTING NUMBER AND PROVIDE A BRIEF SYNOPSIS AND CONTACT INFORMATION FOR THE INCIDENT.

4.2. THE INDIVIDUAL DISCOVERING THE BREACH/COMPROMISE, IN COORDINATION WITH THE COMMAND/AGENCY THAT CREATED THE DATA IF KNOWN, MUST REPORT ALL INCIDENTS INVOLVING THE ACTUAL OR SUSPECTED BREACH/COMPROMISE OF PII TO THE ARMY FREEDOM OF INFORMATION/PRIVACY ACT OFFICE (FOIA/PA) WITHIN 24 HOURS OF DISCOVERY. THE REPORTING FORMAT AND SUBMISSION GUIDELINES ARE LOCATED AT HTTPS://WWW.RMDA.ARMY.MIL/ORGANIZATION/PA-GUIDANCE.SHTML. SUBMIT UPDATED REPORTS REFLECTING THE RESULTS OF INVESTIGATIVE EFFORTS, REMEDIAL ACTION AND NOTIFICATION EFFORTS OF AFFECTED INDIVIDUALS AS THEY BECOME AVAILABLE. THE ARMY FOIA/PA IS THE CENTRALIZED OFFICE FOR ALL ARMY PII INCIDENT REPORTING, INFORMATION, AND STATISTICS.

4.3. CONTINUE TO FOLLOW EXISTING INTERNAL COMMAND PROCEDURES TO NOTIFY LOCAL COMMAND OFFICIALS. THIS INCLUDES BUT IS NOT LIMITED TO SERIOUS INCIDENT REPORTS, CONTACTING THE ARMY OR REGIONAL COMPUTER EMERGENCY RESPONSE TEAM FOR NETWORK INTRUSION INCIDENTS, AND NOTIFICATION OF CREDIT CARD COMPANY, LOCAL LAW ENFORCEMENT, PRIVACY ACT OFFICIALS AND THE PUBLIC AFFAIRS OFFICE. INTERNAL COMMAND NOTIFICATION MAY NOT DELAY THE ONE HOUR US-CERT OR 24 HOUR ARMY FOIA/PA OFFICE REPORTING REQUIREMENTS.

4.4. REPORT ANY INCIDENT INVOLVING THE POSSIBLE COMPROMISE OF ARMY NETWORKS TO THE APPROPRIATE REGIONAL COMPUTER EMERGENCY RESPONSE TEAM (RCERT). IF ANALYSIS CONDUCTED BY THE ARMY COMPUTER EMERGENCY RESPONSE TEAM (ACERT) CONFIRMS POSSIBLE PII LOSS, THE RCERT NOTIFIES THE APPROPRIATE UNIT INFORMATION ASSURANCE OFFICER TO INITIATE PII LOSS REPORTING IAW PARAGRAPH 4.1. THE ARMY FOIA/PA OFFICE WILL PROVIDE A COPY OF ALL ARMY PII REPORTS RECEIVED INVOLVING AUTOMATION EQUIPMENT TO THE ACERT THEATER OPERATIONS CENTER FOR SITUATIONAL AWARENESS AND ANALYSIS.

4.5. THE ORGANIZATION RESPONSIBLE FOR SAFEGUARDING THE PII AT THE TIME OF THE INCIDENT MUST NOTIFY THE AFFECTED INDIVIDUALS. IN ACCORDANCE WITH REFERENCE A. ABOVE, LOW/MODERATE/HIGH RISK OR HARM DETERMINATIONS AND THE DECISION WHETHER NOTIFICATION OF INDIVIDUALS IS MADE, REST WITH THE HEAD OF THE ARMY COMMAND/AGENCY WHERE THE BREACH OCCURRED; HOWEVER, ALL DETERMINATIONS OF HIGH RISK/HARM REQUIRE NOTIFICATION. WHEN THE ACTUAL ARMY ACTIVITY WHERE THE INCIDENT OCCURRED IS UNKNOWN, BY DEFAULT THE RESPONSIBILITY FOR REPORTING THE INCIDENT AND NOTIFICATION OF AFFECTED INDIVIDUALS LIES WITH THE ORIGINATOR OF THE DOCUMENT OR INFORMATION. NOTIFICATION SHOULD BE MADE BY AN INDIVIDUAL AT A SENIOR LEVEL (I.E., COMMANDER, DIRECTOR) TO REINFORCE TO IMPACTED INDIVIDUALS THE SERIOUSNESS OF THE INCIDENT. A SAMPLE NOTIFICATION LETTER IS AVAILABLE AT WWW.RMDA.ARMY.MIL.

4.6. COMMANDERS AND SUPERVISORS WILL ENSURE THE APPROPRIATE REMEDIAL ACTION(S) ARE TAKEN WHEN PII IS LOST OR COMPROMISED. AT A MINIMUM,

IF PII IS LOST AS A RESULT OF NEGLIGENCE OR FAILURE TO FOLLOW ESTABLISHED PROCEDURES, THE INDIVIDUAL(S) RESPONSIBLE WILL RECEIVE COUNSELING AND ADDITIONAL TRAINING REMINDING THEM OF THE IMPORTANCE OF SAFEGUARDING PII. ADDITIONAL REMEDIAL ACTIONS MAY INCLUDE PROMPT

********* START OF SECTION 2 *********

QQQQ

REMOVAL OF AUTHORITY TO ACCESS INFORMATION OR SYSTEMS FROM INDIVIDUALS WHO DEMONSTRATE A PATTERN OF ERROR IN SAFEGUARDING PII AS WELL AS OTHER ADMINISTRATIVE OR DISCIPLINARY ACTIONS AS DETERMINED APPROPRIATE BY THE COMMANDER OR SUPERVISOR.

5. THE ARMY G-3/5/7 POINT OF CONTACT IS MR. ROBERT DICKERSON, CHIEF, ARMY FREEDOM OF INFORMATION/PRIVACY OFFICE, COMM: 703-428-6513, DSN: 328-6513, E-MAIL: ROBERT.DICKERSON1@CONUS.ARMY.MIL.

DISTRIBUTION:

PRINCIPAL OFFICIALS DOD HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER

U.S. ARMY FORCES COMMAND

U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY MATERIEL COMMAND

U.S. ARMY EUROPE

U.S. ARMY CENTRAL

U.S. ARMY NORTH

U.S. ARMY SOUTH

U.S. ARMY PACIFIC

U.S. ARMY SPECIAL OPERATIONS COMMAND

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC COMMAND

EIGHTH U.S. ARMY

UNITED STATES ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND

U.S. ARMY MEDICAL COMMAND

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

U.S. ARMY CRIMINAL INVESTIGATION COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. ARMY MILITARY DISTRICT OF WASHINGTON

U.S. ARMY TEST AND EVALUATION COMMAND

U.S. ARMY MILITARY ACADEMY

U.S. ARMY RESERVE COMMAND

U.S. ARMY ACQUISTION AND SUPPORT

U.S. ARMY INSTALLATION MANAGEMENT COMMAND

EXPIRATION CANNOT BE DETERMINED