THE DEPUTY SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

JUL 15 2005

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: DoD Policy for Biometric Information for Access to U.S. Installations and Facilities in Iraq

1. REFERENCES

a. HSPD-6, "Integration and Use of Screening Information" (http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html)

b. HSPD-11, "Comprehensive Terrorist-Related Screening Procedures" (http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html)

c. HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html)

d. Federal Information Processing Standard (FIPS) 201 (http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf)

e. Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect America" (27 August 2004) (http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html)

f. OMB M-04-04, "E-Authentication Guidance for Federal Agencies" (http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf)

g. OMB M-05-05, "Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services" (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf)

h. OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions the E-Government Act of 2002" (http://www.whitehouse.gov/omb/memoranda/m03-22.html)

i. DoD Directive 1000.25, 19 July 2004, "Personnel Identity Protection"

j. DSD memorandum, 27 December 2000, "Executive Agent for the Department of Defense (DoD) Biometrics Project"

2. PURPOSE. To improve force protection for all U.S. and Coalition personnel in Iraq, the Department of Defense requires the capability to collect biometric data, establish biometrically-

Iraq

OSD 12922-05

based identity authentication and management procedures, and issue a biometrically-based, secure credential for all persons requesting access to U.S. bases and installations. Given the grave threat U.S. and Coalition forces face in Iraq, priority will be given to the implementation of a system meeting these requirements.

a. This policy establishes the requirement to collect biometric, biographic, and other identifying information from non-screened, non-U.S. persons seeking access to U.S. bases and installations in Iraq.

b. Annex A to this memorandum defines the standards for the collection and processing of biometric data referenced in this policy.

c. Subsequent policy will address policies and procedures for screening, credential issuance and management, expanded data sharing, and implementation of similar policy beyond Iraq.

3. DEFINITIONS

a. U.S. person. A citizen of the United States, an alien lawfully admitted for permanent residence to the United States, or a member of the U.S. Armed Forces.

b. non-U.S. person. Individual who does not meet the criteria of "U.S. person."

c. screened. An individual who has undergone a background check to identify those individuals who may pose a threat. Coalition force military members and other official representatives of Coalition member governments are considered screened. An individual who has been screened is not required to undergo additional screening as described in this policy.

d. non-screened. Not meeting the criteria defined in "screened."

4. POLICY

a. USCENTCOM personnel will collect biometrics, biographic, and other identifying information from non-screened, non-U.S. persons requesting access to U.S. bases and installations in Iraq.

b. At a minimum, fingerprints, facial photos, and iris scans will be collected. All information collected will be transmitted to the Biometrics Fusion Center (BFC) for storage in the Automated Biometric Identification System. The BFC will conduct a search of the data against all appropriate domestic and international databases. Match results will be forwarded back to USCENTCOM and provided to the intelligence community for analysis in support of the adjudication process. USCENTCOM-designated representatives will determine whether to issue a badge and allow access to the base.

c. The BFC will make all biometric match results and contextual data associated with biometric collection available to USCENTCOM and other authorized U.S. government agencies. Data collected under this policy will be stored indefinitely in support of the War on Terrorism.

d. Within the Iraqi theater of operations, CDRUSCENTCOM can authorize the sharing of intelligence information associated with biometric match results and contextual data with DoD organizations, authorized U.S. government agencies, and Coalition partners provided:

(1) All requests are in writing.

(2) The information requested is in support of a valid operational requirement.

e. Guidance for information sharing beyond this scope will be developed as delineated in section 5 of this policy.

5. RESPONSIBILITIES

a. The Under Secretary of Defense for Intelligence (USD(I)) has primary staff responsibility for this policy. USD(I) will coordinate with Under Secretary of Defense for Policy, the Joint Staff, and the DoD Executive Agent for biometrics to establish, within 60 days of this policy, policies and procedures governing the biometric match and analysis process. In addition, the aforementioned parties will establish a process for the review of requests to share biometric, biographic, and other identifying data collected.

b. The Secretary of the Army, as DoD Executive Agent for biometrics, will oversee the activities of the BFC and issue detailed guidance addressing standards and requirements pertaining to biometric data collection, transmission and storage, and update such guidance as needed.

c. The Under Secretary of Defense for Personnel and Readiness, in coordination with USD(I) and the Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)) will develop policies for credential issuance associated with this policy.

d. USCENTCOM will develop implementation guidance addressing the collection, transmission, screening, and issuance of a biometrically enabled identification card to non-U.S., non-screened individuals seeking access to U.S. bases and installations in Iraq. USCENTCOM will also establish procedures for disposition of individuals denied base access privileges. USCENTCOM will publish guidance on the sharing of any biometric or biographical intelligence incorporating the requirements discussed in section 4 of this policy.

Gordon England
ACTING

Attachment:
As stated

DEPARTMENT OF DEFENSE
BIOMETRICS MANAGEMENT OFFICE (BMO)

DoD STANDARDS FOR COLLECTING AND PROCESSING BIOMETRIC DATA FOR FORCE PROTECTION IDENTITY SCREENING

1. REFERENCES

a. DSD memorandum OSD 05872-05, 29 March 2005, "Force Protection Identity Screening Policy for Base Access"

b. "Products Certified for Compliance with the FBI's Integrated Automated Fingerprint Identification System Image Quality Specifications" (http://www.fbi.gov/hq/cjisd/iafis/cert.htm)

c. Electronic Fingerprint Transmission Specification (EFTS), January 1999 (http://www.fbi.gov/hq/cjisd/iafis/efts_70.pdf)

d. American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST)- ITL 1-2000, September 2000, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information" (ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf)

e. ANSI/INCITS 385-2004, May 2004, "Face Recognition Format for Data Interchange." This standard is copyrighted and licensed copies are available from the DoD BMO.

f. NIST Best Practice Recommendations for the Capture of Mugshots, Version 2.0, September 1997 (http://www.itl.nist.gov/iad/vip/face/bpr_mug3.html)

g. DoD Biometrics Management Office Web site - http://www.biometrics.dod.mil

h. FBI Procedure on Taking Legible Fingerprints (http://www.fbi.gov/hq/cjisd/takingfps.html)

i. ANSI/INCITS 379-2004, May 2004, "Iris Image Interchange Format." This standard is copyrighted and licensed copies are available from the DoD BMO.

j. DA Form 2663-R, "Fingerprint Card" (http://www.apd.army.mil/pub/eforms/pdf/a2663_r.pdf)

k. ASD(NII) memorandum, 5 August 2005, "Establishment of a DoD Automated Biometric Identification System (ABIS)"

l. DoD Electronic Biometric Transmission Specification (EBTS), Version 0.9.4 (Draft), 21 April 2005

2. BIOMETRIC COLLECTION PROCESSES AND RESPONSIBILITIES

a. **Fingerprints.** There are two accepted methods for the collection of fingerprints: electronic and paper-and-ink.

- The electronic, or "live scan," method provides for a near-real-time capability to transmit collected fingerprint data for searching and matching against the data stored in large-scale automated fingerprint identification systems (e.g., the FBI's Integrated Automated Fingerprint Identification System (IAFIS)) (reference b).
- The paper-and-ink method has long been used in the United States and other countries. Latent fingerprint examiners prefer this method as it provides a greater level of detail of the fingerprint than live scan. This allows increased opportunities for matching partial latent prints, such as those obtained from a criminal or terrorist site, to an original fingerprint sample. In addition, a paper-and-ink fingerprint card can be digitized for use with an electronic fingerprint capture device. This method may increase the time required to identify an individual because the needed conversion equipment is not always readily available and requires some processing.
- In all cases, the transmission of fingerprint and biographical data shall adhere to the internationally accepted and most current EFTS version (v7.0 at the time of this printing) (reference c).
- Both methods allow for adherence to the appropriate image quality standards, as defined in Appendix F of the EFTS v7.0; however, the electronic or "live scan" method is preferred. The paper-and-ink method will only be used as a last resort and only if the electronic means of collection is not available.

For electronic collection:

- To ensure interoperability, all electronic fingerprint sensors, commonly known as "live scan" devices, used by DoD to collect fingerprints from applicants shall appear on the FBI-certified devices list. In addition, all fingerprint images shall conform strictly to the ANSI/NIST-ITL 1-2000 standard (reference d) and Appendix F of the EFTS v7.0 (reference c).
- 14-image fingerprint collection is required (10 rolled images, separate images of each thumb, and two four-finger slap prints) (reference c, reference k).
- 500 pixels per inch (ppi) resolution at nominal 15:1 Wavelet-packet Scalar Quantization (WSQ) compression is required, as stated in reference c.
- If collected, 1,000 ppi Joint Photographic Experts Group (JPEG) 2000 images shall also be stored in the EFTS file when possible.

The live scan devices referred to above capture the entire area of the fingerprint surface from one edge of the fingernail to the other and from the crease of the first joint to the tip of the finger. DoD organizations shall not use "flat" fingerprint devices when collecting fingerprint data for enrollment from applicants.

b. **Face ("Mug shots").** ANSI/INCITS 385-2004, "Face Recognition Format for Data Interchange" (reference e) is the U.S. national standard that governs the electronic representation

of facial images. Moreover, this standard is based on earlier extensive technical guidance from NIST regarding the collection of mug shot data (reference f). Relevant information from ANSI/INCITS 385-2004 and NIST regarding the collection of mug shots is provided below.

At a minimum, five facial photos shall be taken from the subject. The photo angles for applicants shall be:

- F – Full Face Frontal
- R – Right Profile 90 degrees
- L – Left Profile 90 degrees
- I – Angle Pose 45 degrees Right Side
- E – Angle Pose 45 degrees Left Side

The camera lens orientation shall be:

- Pointed to the front of the person photographed, aligned approximately in the center of the face, and taken from a distance of approximately 5 feet.

Image format requirements:

- All photographs shall be taken in color.
- The images shall preferably be stored using a JPEG file format. The minimum acceptable resolution shall be 640 pixels (vertical) by 480 pixels (horizontal) with 24-bit color. (Note that this requirement may require turning the camera 90 degrees on its side in order to achieve the required resolution.) As a general guide, a format shall be used with sufficient resolution to allow a human examiner to ascertain small features such as moles and scars that can be used to verify identity.
- The width-height aspect ratio of the captured image shall be 1:1.33.
- Digital cameras and scanners used to capture facial images shall use square pixels with a pixel aspect ratio of 1:1.
- The subject's captured facial image shall always be in focus from the nose to the ears. When photographed, subjects shall not be allowed to wear any glasses, sunglasses, headgear, headdress, or other items obscuring the area photographed.
- A placard or similar mechanism containing, at a minimum, the applicant's full name (first, middle, last, tribal/grandfather's name) shall be positioned at least 6 inches away from the subject's face, preferably at the top or bottom of the photograph. Whenever possible, require the applicant to handwrite his or her own name on the placard.

The facial image being captured (full-face pose) shall be positioned to satisfy all of the following conditions:

- The approximate horizontal midpoints of the mouth and bridge of the nose shall lie on an imaginary vertical straight line positioned at the horizontal center of the image.
- An imaginary horizontal line through the center of the subject's eyes shall be located

at approximately the 55 percent point of the vertical distance up from the bottom edge of the captured image.

- The width of the subject's head shall occupy approximately 50 percent of the width of the captured image. This width shall be the horizontal distance between the midpoints of two imaginary vertical lines. Each imaginary line shall be drawn between the upper and lower lobes of each ear and shall be positioned where the external ear connects to the head.
- Desired subject illumination shall be achieved using a minimum of three balanced light sources, conditions and resources permitting.
- Appropriate diffusion techniques shall also be employed, with lights positioned to minimize shadows and eliminate hot spots on the facial image. These hot spots usually appear on reflective areas such as cheeks and foreheads.
- Flash techniques such as use (or nonuse) of flash fill to reduce red eye, shadows around the nose and mouth shall be considered.

c. **Iris.** All iris images shall be collected to the JPEG standards outlined in EBTS Version 0.9.4 (reference l).

- An iris-imaging device shall collect separate images of the left and right irises of each applicant.
- Each iris record shall be labeled as the right or left iris, and shall be associated with all other biometric and biographic data collected on the applicant.

Current commercial iris collection devices, including those suitable for operational use typically cue the user when acceptable imaging conditions have been achieved. These conditions include the following:

- The subject's eye shall be open to the greatest extent possible, with the iris occluded (i.e., concealed by the eyelid and/or eyelashes) no more than 30 percent; the orientation of the iris image shall be right side up (i.e., the upper eyelids in the upper part of the image); further, for right eyes the tear duct shall be on the right side of the image, and for left eyes the tear duct shall be on the left side of the image.
- The presentation of the iris to the imaging device shall be aligned to the subject's head, so that a horizontal line between the pupils is within +/- 10 degrees of the horizontal plane of the iris-imaging device; also, the subject shall remove any eyeglasses and contact lenses to optimize the enrollment quality.

Transmission requirements are as follows:

- Transmissions of iris data to the DoD ABIS shall include fields defined in EBTS V 0.9.4 (reference l).

3. EBTS COMPLIANCE

Fingerprint and mug shot data shall be formatted and transmitted in accordance with the most current version of EBTS (Version 0.9.4 as of this printing). Specific guidance regarding EBTS V 0.9.4 compliance is as follows:

- Biometric collection units shall have the capability to electronically submit EBTS transactions and receive responses (search results) in an automated fashion from the DoD ABIS.
- The local biometric collection system shall automatically keep an audit log of biometric submissions and responses.
- All transactions, as described in the EBTS V 0.9.4, for searching persons requesting access to U.S. bases and installations shall be submitted as a "Miscellaneous Applicant" transmission.

071805

SECFILES FULL RECORD DETAIL

Print Date: **7/18/2005**

DOCUMENT TYPE: **RESPONSE** ATTACHMENT:
OSD CONTROL **OSD 12922-05** DOC **7/15/2005** DOR **7/6/2005** SIGNATURE CASE:
FROM **DEPSEC ENGLAND** TO **SA SN SAF JCS USD DA COMB**
SUBJECT **DOD POLICY FOR BOIMETRICS INFORMATION FOR ACCESS TO U.S. INSTALLATIONS AND FACILITIES IN IRAQ**
KEYWORDS **MULTI-MEMO FORCE PROTECTION**
COMMENTS **SENT E-MAIL, 18 JUL 05.**
FN Iraq SEC **U** OCN
REFERENCE DOCUMENTS
STATUS CODE DECISION DECISION DATE PRIORITY ACTION REPORT:
AGENCY ACTION ASSIGNED DOC SUSPENSE: SUSPENSE
SUSPENSE COMPLETE ACD COORDINATION
PAGES **3** ENCLOSURES **1**
SUSPENSE STATUS

PACKAGE VIEW:
ACTION MEMO
RESPONSE

CREATED BY: **barnwell**

DISTRIBUTION: OFFICE COPIES
ADC **OWI**
ADD **RWI(MM)**
SGN **RWI**
GC **RWI**

JS,
This was Got minute
green mtg. Helmer
wanted a copy to JCS.

JS,
7/15

Pull – Red mtg
Pg 1.