



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

CHIEF INFORMATION OFFICER

FEB 2 2004

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Department of Defense (DoD) Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from "Red Force" Personnel

Biometrics, specifically fingerprints, are a critical tool in conclusively linking a person to past terrorist or criminal actions, as well as determining or validating a person's identity. It has come to my attention that DoD organizations are currently using electronic systems that do not comply with the internationally accepted standard to collect fingerprint data from "red force" personnel, *i.e.*, detainees, internees, enemy prisoners of war, and foreign persons of interest as national security threats. As a result, the fingerprint data produced is not interoperable with the Federal Bureau of Investigation (FBI)'s Integrated Automated Fingerprint Identification System (IAFIS) and other U.S. Government and foreign fingerprint systems that do meet the standard.

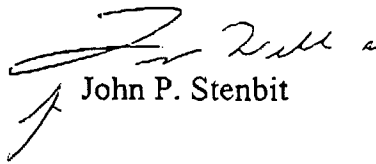
This problem must be rectified as soon as possible. In fighting the Global War on Terrorism, standardization and interoperability are key tenets of success and the Department cannot afford to operate systems that do not fully communicate and share fingerprint data on "red force" personnel with other U.S. Government systems.

Effective immediately, all new acquisitions or upgrades of electronic fingerprint systems used by DoD Components to collect "red force" fingerprint data must (1) conform with the Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology-ITL 1-2000 and (2) be certified to be interoperable with the FBI's IAFIS. The "red force" fingerprints thus gathered can then be readily shared so they can be searched against all relevant databases, including over 46 million fingerprint records in the FBI's database, the tens of millions of fingerprint records in other U.S. Government databases, and a like number in the searchable databases of cooperating allies. This new interoperability will provide U.S. forces with a powerful offensive capability. Systems currently in use that do not meet the criteria outlined above must either be upgraded or replaced by December 31, 2004.



For clarification, this memorandum does not apply to electronic systems used to collect fingerprint data from U.S. military, civilian, and contract personnel.

For technical questions or comments relating to this matter, please contact the DoD Biometrics Fusion Center (BFC) at (304) 842-0730 Extension 2233, or [helpdesk@dodafc.army.mil](mailto:helpdesk@dodafc.army.mil). They will also provide detailed information on the EFTS and the FBI certification process.



John P. Stenbit

## DISTRIBUTION LIST:

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  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION  
DIRECTOR, NET ASSESSMENT  
DIRECTOR, FORCE TRANSFORMATION  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES