

The New York Times

Fingerprinting Glitches Are Said to Hurt Antiterror Effort

By Jeff Gerth

WASHINGTON, Oct. 26

Problems in searching fingerprint databases have left the American military unable to check fully the identities of thousands of detainees in Iraq and Afghanistan, raising concerns that they might be releasing suspects prematurely, according to Pentagon officials and documents.

The Defense Department, in the field, has used a mobile system that records fingerprints of suspects, but it cannot always search for a match in other government databases.

In a memorandum last February, the Pentagon said the fingerprinting "problem must be rectified as soon as possible" to fight terrorism more effectively. It required that all new electronic fingerprinting systems comply with accepted standards.

The situation has improved since then, said John D. Woodward Jr., the director of the Defense Department's Biometrics Management Office. But he added, "We still need to improve."

Mr. Woodward said the memorandum resulted from complaints in late 2003 from the Federal Bureau of Investigation that the fingerprint data being collected in Iraq and Afghanistan by the Pentagon was not as compatible with other databases as it should be.

Mr. Woodward, citing "national security concerns," declined to say how many prints had gone unprocessed as a result. Another official, who asked not to be identified because of the sensitive nature of the information, said it exceeded 16,000 at the time of the memorandum.

Fingerprint matches have led to the identification and imprisonment of people accused of terrorism, a success story advertised by Defense Department officials. But it is unclear if the inability to search fingerprint records has allowed someone guilty of terrorist acts to be released.

For more than 100 years, fingerprinting has relied on primitive, inexpensive equipment. A person would put his fingers on an ink pad and then roll them onto a piece of paper. A full set of 10 prints, if properly transmitted, can be searched against the F.B.I.'s 47 million records and other government databases. Matches, even with inked prints, can be made in 15 minutes.

Ink pads and paper were the technology of choice for the F.B.I. agents who first went to Afghanistan in November 2001, said Michael Kirkpatrick, who recently retired as head of

the F.B.I.'s criminal information system. Eventually, both in Iraq and Afghanistan, the F.B.I. also used systems that electronically took 10 fingerprints and met global standards. Those customized portable units can cost \$10,000 each. Meanwhile, the Pentagon was using its own system, the Biometrics Automated Toolset, or B.A.T., developed by the Army.

It had a more modest purpose, Mr. Kirkpatrick said. Instead of checking other databases to ascertain a person's identity, it only sought to know whether "you ever encountered this particular person before," a question answered by searching your own internal database, he explained. The Army system also sometimes relied on only two fingerprints or used equipment that was not certified to interact with other databases.

The F.B.I. in late 2003 brought the deficiencies to the attention of Mr. Woodward, who had just taken over the Pentagon's biometrics office. Mr. Woodward, in turn, relayed those concerns to senior military officials.

About the same time, an Army report on Iraqi prisons found other problems with fingerprints, even though the prisons were using certified equipment. The report, by Maj. Gen. Donald J. Ryder, found ineffective central administration and inadequate data networks for processing information about the 4,300 people who had been interned.

A brief version of General Ryder's comments were incorporated into the report on abuses in Abu Ghraib prison last February by Maj. Gen. Antonio M. Taguba.

That same month the Pentagon's chief information officer, John P. Stenbit, ordered the fingerprint problem rectified.

"It has come to my attention," Mr. Stenbit wrote in a widely distributed memorandum, that Defense Department "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."

He directed that, "effective immediately, all new acquisitions or upgrades of electronic fingerprint systems" must meet certain standards, including being interoperable with the F.B.I.'s fingerprint database.

Mr. Woodward, in an interview, said substandard equipment was compounded by a lack of training in the fingerprint system. Army officials did not make anyone available to discuss B.A.T. Proper fingerprint matches, said Mr. Kirkpatrick, have been "an intelligence bonanza" with detainees in Iraq and Afghanistan.

As an example of a fingerprinting accomplishment, Mr. Woodward cited the case of Mohamed al-Kahtani, a Saudi and the presumed 20th hijacker in the plans for the Sept. 11, 2001, attacks. Held in Guantánamo, Mr. Kahtani did not initially disclose his identity.

But F.B.I. agents were able to match his prints against those taken when he was denied entry into the United States in Orlando, Fla., in August 2001.

Last August, Army intelligence officials said a fingerprint match saved lives in Iraq. They noted that prints from an Iraqi detained in July matched the prints of a suspicious Iraqi detainee who was freed in September 2003. The man's prints, according to an account in the Army News Service, were entered into a database during his first detention. He was then jailed, keeping him from fighting American troops. The Army is home to one of the world's leading fingerprint experts, Ed German, said Mr. Kirkpatrick and Mr. Woodward. He heads the intelligence unit of the Army's criminal investigative command. Earlier this year, Mr. German complained internally that substandard equipment was put in use even after Mr. Stenbit's memorandum, but was told to muffle his complaints, according to the official who asked not to be identified.

Mr. German, reached by telephone, declined to comment.