D H E C

PROMOTE PROTECT PROSPER

South Carolina Department of Health
and Environmental Control

MEMORANDUM

To: Aaron Gantt, Chief
Bureau of Radiological Health

Jim Peterson, Director
Division of Radioactive Material and Licensing

From: Nancy S. Layman
Chief Attorney for Health Regulation

Date: December 10, 2007

RE: Agreement State Authority to Fingerprint

You have requested a legal opinion in response to the June 21, 2007 query from the U.S. Nuclear Regulatory Commission (NRC). The NRC wanted the "Agreement States" to provide citations to "any State statutes, regulations, or other laws that might affect a State's ability to collect fingerprints or the use of information obtained as a result of the required FBI identification and criminal history records check."

SHORT ANSWER

As of 2007, while numerous South Carolina statutes require fingerprinting of certain licensees and other employees, no South Carolina statutes, regulations or other laws specifically preclude the State from collecting fingerprints. When persons are

fingerprinted, the State Law Enforcement Division is the agency designated by statute as the repository for storing fingerprint records and the only agency charged with dissemination of that information, pursuant to applicable statutory authority.

DISCUSSION

On August 8, 2005, Section 652 of the Energy Policy Act of 2005 (EPAct) amended Section 149 of the Atomic Energy Act (AEA) to require fingerprinting and a Federal Bureau of Investigation (FBI) identification and criminal history records check for ". . . any individual who is permitted unescorted access to . . . radioactive material or other property subject to regulation by the [Atomic Energy] Commission that the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks." Further, it is required that "All fingerprints obtained by an individual or entity . . . shall be submitted to the attorney General of the United States through the Commission for identification and a criminal history records check." 42 C.F.R. 23 §2169(a)(2) (2005).

Under Section 274b of the AEA, the Commission enters into agreements with States and thereby assumes AEA regulatory authority for the protection of the public health and safety over certain nuclear materials, including those in the possession of Increased Controls (IC) licensees. States then use their AEA authority to administer programs to regulate these radioactive materials. In accordance with the AEA Section 149, as amended by the EPAct, the Commission has determined that the materials possessed by the IC licensees are of such significance to the public health and safety as to

warrant fingerprinting and FBI criminal history records check. Thus, Agreement States are authorized to implement the requirements of Section 149 for their IC licensees without additional authorization in State statute.

However, the NRC has recognized that some Agreement States may have laws that impose prohibitions or limitations on the collection and use of fingerprints and criminal history information. In its June 21, 2007 letter to Agreement State Radiation Control Program Directors, the Director of the Division of Materials Safety and State Agreements of the NRC requested that the State Radiation Control Program Directors report any State statutes, regulations or other laws that might affect a State's ability to collect fingerprints or the use of information obtained as a result of the required FBI identification and criminal history records check.

A. <u>The Role of SLED</u>

The South Carolina Law Enforcement Division Criminal Justice Information System (SLED/CJIS), acting as the State's central criminal justice information repository, "shall collect, process, and store criminal justice information and records necessary to the operation of the criminal justice information system" of the State Law Enforcement Division. S.C. Code Ann. Regs. 73-21(A) (2006). "The SLED/CJIS is comprised of the State Crime Information Center (SCIC), which includes the Computerized Criminal History (CCH) department, the Criminal Records Department, and such other departments as may be deemed necessary." *Id*. The fingerprint records of all persons arrested in the State, as well as the records of those who voluntarily submit fingerprints on SLED forms, are turned over to the State's Criminal Records Department. That Department "has the responsibility of collecting, processing and storing all fingerprint

cards and dispositions of persons arrested in the State." Regulation 73-21(A)(2) The Supervisor of the Criminal Records Department serves as custodian of records. "Fingerprints will be the basis for establishing computerized criminal history . . . The Criminal Records Department is responsible for the timely processing of all supporting documents for criminal history record information as provided to the SLED/CJIS by other criminal justice agencies." *Id*. Once SLED processes the information, it forwards the documentation to the FBI/CJIS Division in Clarksburg, West Virginia. *Id.*

B. <u>Dissemination of Information</u>

The SLED Criminal Justice Information System operates and maintains the information system that supports the "collection, storage, retrieval and dissemination of criminal history record information, both intrastate and interstate." Regulation 73-23(A). It makes available to bona fide criminal justice agencies[1], upon request, "any information which will aid these agencies in the performance of their official duties, *provided that the dissemination of such information will not be a violation of state or federal laws and regulations restricting its use."* Regulation 73-23(A) (Emphasis added.) Pursuant to Regulation 73-23, SLED/CJIS is authorized to disseminate criminal history record information, "unless sealed [by law or regulation], to private persons,[2] governmental entities, businesses, commercial establishments, professional organizations, charitable organizations and others."

---

[1] Criminal Justice Agency means "any governmental agency or sub-unit which as its principal function performs the administration of criminal justice pursuant to a statute or executive order . . . ." Regulation 73-20(B).

[2] Generally, the only private persons who may gain access to criminal records are the persons on whom the records are kept. *See,* Regulation 73-24(A).

The issue of whether the dissemination of criminal records information to those without a legitimate need for the information or without the necessary statutory authority has been the subject of a case brought before the U.S. Supreme Court. A group of reporters in the District of Columbia attempted to gain access to the "rap sheet" of a crime family member, Charles Medico, using the federal Freedom of Information Act. The reporters argued that the information was a matter of public interest. The government argued that the rap sheet was protected by an exemption in the FOIA (Exemption 7(C)), which prevented an unwarranted invasion of personal privacy.[3] After considering the balance between the individual's privacy interest in maintaining the rap sheets against the public's interest in their release, the Court held that "…[A] third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no 'official information' about a Government agency, but merely records what the Government happens to be storing, the invasion of privacy is unwarranted." United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, et al., 489 U.S. 749, 780, 109 S.Ct. 1468, 1475 (1989).

C. South Carolina Statutory Provisions for Fingerprinting

An increasing number of statutes in South Carolina provide for fingerprinting individuals, either for identification purposes or to ascertain previous criminal convictions. Some statutes provide for fingerprinting as one form of identification that may be submitted prior to a person being granted a license (as an alternative, e.g., to a photograph), *See*, S.C. Code Ann § 40-2-35 (2001 and Supp. 2006),

[3] South Carolina's FOIA has a similar provision. (Matters exempt from disclosure include "Information of a personal nature where the public disclosure thereof would constitute unreasonable invasion of personal privacy.") S.C. Code Ann. § 30-4-40(a)(2) (2007).

"Regulation of Certified Public Accountants and Public Accountants." Most frequently, fingerprinting is required of a person to determine whether he has a criminal record, usually when he is seeking a certain type of license or employment with the State. *See*, S.C. Code Ann § 40-35-40 (2001 and Supp. 2006), "Long Term Health Care Administrators." S.C. Code Ann. Regs. 73-25(4) (Supp. 2006) ("All personnel who are allowed to access criminal history record information must be subjected to a criminal history background investigation in accordance with SLED policy.") S.C. Code Ann. § 40-47-36 (2001 and Supp. 2006) ("Each applicant [physicians and surgeons] may be required to furnish a full set of fingerprints . . . .") S.C. Code Ann. § 20-7-3097 (2004 and Supp. 2006) (Department of Social Services employee in "childcare licensing or "child protective services divisions... shall undergo a state fingerprint review . . . .") S.C. Code Ann. 59-25-115 (2004) ("All persons applying for initial certification to become certified education personnel in this State shall undergo a state fingerprint review . . . .") S.C. Code Ann. § 59-63-50 (2004) (authorizing fingerprinting of school children in kindergarten and grades one through twelve "when the parent of a child requests in writing that his child be fingerprinted for identification purposes for the protection of the child").

On the federal level, in 1986 Congress authorized release of criminal-history information to licensees or applicants before the Nuclear Regulatory Commission. *See*, 42 U.S.C.§ 2169(a). "Congress has authorized rap-sheet dissemination to banks, local licensing officials, the securities industry, the nuclear-power industry, and other law enforcement agencies." U.S. Dep't of Justice, 765, 1477.

D. Challenges to Fingerprinting

Laws permitting fingerprinting in non-criminal cases have been challenged in the Courts. In 1969, plaintiffs representing three different stock exchanges challenged a New York State law requiring all employees of member firms of national security exchanges registered with the Securities and Exchange Commission and employees of affiliated clearing corporations to be fingerprinted as a condition of employment. Thom v. New York Stock Exchange, et al., 306 F. Supp. 1002 (1969). Plaintiffs argued that the statute was unconstitutional in that it constituted an invasion of privacy, an illegal search and seizure, punishment without due process of law and denial of equal protection under the Fourteenth Amendment. The plaintiffs specifically argued that they had the right *not* to be fingerprinted absent a criminal charge or other compelling state purpose.

The Court stated, "The day is long past when fingerprinting carried with it a stigma or any implication of criminality. Federal and state courts alike, in upholding fingerprinting requirements, have rejected any such view." *Id*. at 1008. The Court added that "Fingerprinting in noncriminal contexts today is even more widespread. It is required of all employees of United State government agencies and departments." *Id.* The Court concluded that "The actual inconvenience is minor; the claimed indignity, nonexistent; detention, there is none; nor unlawful search; nor unlawful seizure." *Id*.

More recently, a union challenged an amendment to the amended Atomic Energy Act. Utility Workers Union of America, AFL-CIO, v. Nuclear Regulatory Comm'n, 664 F.Supp.136 (1987). The 1986 amendment had directed the NRC to require nuclear reactor licensees to fingerprint each individual who was permitted unescorted access to nuclear power facilities or access to "safeguards information" and to submit the fingerprints to the NRC for identification and a criminal history records check. The

Plaintiffs claimed violations of privacy rights and the Fourth Amendment, which prohibits unreasonable searches and seizures. The Court held that "Using fingerprints to verify the identity and any existing criminal history of workers with access to vital areas or safeguards information is a rational method of clearing these workers. Therefore, the statute at issue here does not violate the right to privacy of the plaintiff's members."*Id*. at 139. It also found that "the fingerprinting it mandates does not constitute an unreasonable search and seizure." *Id.*

The UWUA case summed up the general law of the United States regarding fingerprinting in non-criminal contexts: "[I]n non-criminal contexts, courts have regularly upheld fingerprinting of employees." *Id*. at 138.

CONCLUSION

The uses of fingerprinting have evolved from documenting criminals to verifying identities and checking backgrounds for purposes of employment and licensing. Following the terrorist activities of September 11, 2001, Congress has expanded the use of fingerprinting, justifying it as being in the interest of national safety. At present, there are no South Carolina laws or regulations that might affect the State's ability to collect fingerprints or to use information obtained as a result of the required FBI identification and criminal history records check of Increased Controls licensees. The Office of General Counsel will continue to monitor future legislation in regard to this matter.