California Association of Licensed Investigators, Inc.
Legislation Committee
908 21st Street.
Sacramento, CA 95814

John H. Eppick Chairman
818 247-6690

August 5, 2005

Richard A. Hertling
Deputy Assistant Attorney General
Office of Legal Policy
4234 Robert F. Kennedy Building
950 Pennsylvania Avenue, NW
Washington DC 20530

RE: OLP Docket No. 100

Dear Mr. Hertling:

I am writing on behalf of the California Association of Licensed Investigators (CALI), the largest association of its kind in the world. Members are comprised of both licensed private investigators and licensed private patrol operators and number approximately 2000 members.

Both industries, by their very nature, have a substantial interest in an efficient, accurate, and complete repository of criminal history information. This letter responds to the Department's request for comments regarding the development of a report required by Section 6403 of the Intelligence Reform and Terrorism Prevention Act of 2004.

CALI is a member of the National Association of Investigators and Security Services (NCISS), an association representing 44 state associations and over 1000 additional individual members. In addition, NCISS participates in a coalition entitled Security Companies Organized for Legislative Action (SCOLA) also representing guard, investigative, armored car and alarm industries. We support SCOLA's letter to you.

An allied association, the National Association of Professional Background Screeners (NAPBS) submitted a letter, which our organization supports as well. NAPBS is a professional trade organization for the background screening industry. Further, during this comment period, you received comments from Lester Rosen, an attorney and president of Employment Screening Resources, Novato, CA. Mr. Rosen provides comments and outlines his extensive experience with the subject of interest.

Our association wholeheartedly endorses and agrees with the opinions, suggestions, and comments offered by these two organizations and Mr. Rosen.

A number of state regulatory agencies, including California, submit fingerprints to the Department of Justice as part of the licensing process. This is done either through the submission of fingerprint cards or electronically through Live Scan. The results of the fingerprint check ensure regulators and employers that those with criminal backgrounds are not hired in positions of trust. We are optimistic about the potential of allowing state agencies leave to submit fingerprints electronically through the Integrated Automated Fingerprint Identification System (IAFIS) and believe this is an encouraging step. Many states need assistance in processing criminal histories in a timely manner due to the lack of personnel. This may, at least, be a partial solution.

Private databases have tremendous value for all employers and are essential for thorough background checks as part of the hiring process. These databases are utilized to supplement both state and federal records as experience has demonstrated that courts are often slow to forward information. Employers, therefore, often find it prudent to use information from private databases, confirming then by physical courthouse searches to identify an individual with the criminal record. Access to criminal history information contained in the federal database would provide additional critical data, particularly in those states not having the statutory authority for access.

In addition, licensed individuals need to conduct accurate and timely pretrial and post trial witness background investigations for both criminal and civil litigation or as part of fraud investigations including workers compensation fraud. Private databases have tremendous value for security industry employees and are essential for thorough background investigations.

There is a strong argument that "name-only" checks cannot be relied upon. The commercial sector has tools to match data submitted to them, such as names, birth dates, addresses, driver's license numbers and social security numbers. To adequately ensure accuracy, the name must be matched against two or more personal identifiers submitted by the subject, or matched to historical databases.

At the same time, individuals who are the subject of criminal history record information must be told about the practices, procedures and policies for the collection, maintenance, use and disclosure of criminal history information. They must be given a right of access to the information, and be provided a method to correct erroneous information, including the right to see a record of the disclosure of the information; and enjoy effective remedies for violations of any applicable privacy and information standards.

Employers need more information. The employer is responsible for most acts committed by its employees. An individual applying for employment may have been arrested many times but then slipped through the legal process. When an employee is hired into a job of trust, this lack of information creates risk to the employer, its employees, and the public at large. Therefore, a decision maker within the employer company should have access to all available information and be able to weigh this information against the job description.

We believe laws are needed with strong sanctions and severe criminal penalties for misuse of personal information. These sanctions and penalties would include severe criminal and civil fraud statues enacted to punish identity thieves, to prohibit disclosure of individual financial information, to provide for both privacy invasion and deceptive practices tort law, and to punish and deter violations of an individual's privacy rights.

At the same time, personal information held in databases should not be available to the general public.

In summary, CALI and its members ascribe to the following:

- *To acquire individually identifiable information only from sources known as reputable;*
- *To restrict the distribution of non-public information through safeguards appropriately regulated for the type and use of the information;*
- *To prohibit the reselling of raw data obtained from an data provider;*
- *To support denying sales of personal identifying information to the general public through the internet;*
- *To prohibit reselling of raw data obtained from a data provider;*
- *To protect an individual's personal information by supervising the destruction of documents containing such information;*
- *To increase penalties, with heavy fines and strong criminal sanctions for the misuse of personal information;*
- *To support a thorough credentialing of new accounts by data providers and current clients where a review indicates a new check is in order;*
- *To enact legislation requiring data providers to notify customers of breeches;*
- *To prohibit use of social security number on identification documents such as health card, insurance cards, driver's licenses and state permits; and*
- *To allow access to personal data by licensed individuals who can demonstrate a need and have submitted to a background investigation.*

Thank you for the opportunity to provide our views on this important topic. If you have questions, please do not hesitate to contact me at 818-400-0700.

Sincerely,

John Eppick

Legislation Chair