CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity
Writer's Direct Dial: 202-408-7407
Writer's Email: eellman@cdiaonline.org

August 2, 2005

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

Re: Docket No. OLP 100; Criminal History Background Checks; Request for Comments

Dear Mr. Hertling:

This comment is in response to the above captioned matter that appeared in the Federal Register on June 6, 2005. The Department of Justice (DOJ) is seeking public input in the drafting of a report to Congress under Section 6403 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (IRTPA). This section

> requires the Attorney General to report to Congress on statutorily required criminal history record checks conducted by the [DOJ]. As part of this report, the Attorney General is required to make certain recommendations to Congress for improving, standardizing, and consolidating the existing statutory authorizations, programs, and procedures for the conduct of criminal history record checks for non-criminal justice purposes, such as licensing and employment.

70 Fed. Reg. 32849 (June 6, 2005). By way of background, CDIA was founded in 1906 and is the international trade association that represents more than 300 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services. We are pleased to be able to offer a comment.

General Background

While we completely agree with the Congressional findings in Sec. 6402(a) of IRTPA,[1] we disagree with the implication of Sec. 6402(d) that the public sector should have a monopoly on the ability to perform criminal background checks of private security officers. IRTPA suggests that private security firms use

[1] In Sec. 6402(a) Congress found that: private security protection is increasing; private security officers supplement public law enforcement and help reduce crime; private security officers touch many Americans lives on a daily basis in apartment buildings, residential communities, office buildings, hospitals, and more; cooperation between the public and private sectors are required to reduce the threat of terrorist attacks; private security officers should be "thoroughly screened"; and that "the American public deserves the employment of qualified, well-trained private security personnel".

public databases to screen employees. However, we feel strongly that the goals of Congress, as laid out in IRTPA, are completely satisfied when private security firms use private screening resources. In fact, society at large is best served when all background screening, for all purposes, by both the public and private sectors, are conducted by the private sector drawing upon both public and private data.

Commercial background screening companies have extensive expertise in building, maintaining, integrating, and disseminating information from disparate public and private sources. Unlike members of the public sector, CDIA member companies have the vast experience and technical proficiency to interpret public records data from thousands of sources which ultimately benefit a broad range of societal interests relative to background screening. The information used by CDIA members may come from their own databases or data obtained from other commercial vendors. Since searching a database is not always enough for a proper criminal screen, commercial criminal background screeners also cull criminal histories from over 3,000 courts in the United States using experts in the collection, management, and integration of that data and the intricacies therein. In addition, commercial background screening companies may, to the extent allowed by law, conduct a fingerprint search. Using their advanced technology commercial screeners can harness information from a variety of public and private sources at the federal, state, and local levels.

Specific Responses

In response to the specific questions raised in the request for comment, we now respond to some of the fifteen specific statutory factors raised in the Federal Register notice upon which the DOJ must base its recommendations.

Sec. 6403(d)(1). The effectiveness and efficiency of utilizing commercially available databases as a supplement to [Integrated Automated Fingerprint Identification System] IAFIS criminal history information checks.

Response. Criminal history information integrated and disseminated by commercial screening companies provides an excellent supplement to IAFIS checks. Commercial criminal history screening companies can often provide more comprehensive information than just fingerprint information. Not all fingerprint data is captured and not all criminal history information collected by state or local jurisdictions is provided to IAFIS.

Since access to fingerprint data is important for criminal screens, we recommend increased access to government fingerprint databases for commercial criminal screening companies.

Sec. 6403(d)(2). Any security concerns created by the existence of these commercially available databases concerning their ability to provide sensitive information that is not readily available about law enforcement or intelligence officials, including their identity, residence, and financial status.

Response. The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. Sec. 1681 *et seq*., provides a comprehensive regulatory scheme for consumer reporting agencies, consumer reports, and those that furnish data to and use data from consumer reporting agencies. Among other things, consumer reporting agencies cannot provide a consumer report except to users with certain permissible purposes. Id, at Sec. 1681b. Also, consumer reporting agencies must

> require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report.

Id., Sec. 1681e(a). To reduce the instances of security breaches, there are statutes and rules governing the disposal of consumer information derived from consumer reports. *Id*., Sec. 1681w; 16 C.F.R. Part 682. In addition to legal obligations, there are ethical obligations as well. CDIA members must be good stewards of the data which is entrusted to them and these obligations are taken seriously. CDIA members employ security experts and use advanced technologies to prevent data breaches.

Sec. 6403(d)(3). The effectiveness of utilizing State databases.

Response. As noted above, CDIA believes that the private sector is most adept at piecing together disparate data from a wide array of sources and making them available to their customers to fulfill beneficial services such as employment screening, residential screening, fraud prevention, and more.

Sec. 6403(d)(5). Privacy rights and other employee protections, including (A) Employee consent; (B) Access to the records used if employment was denied; (C) The disposition of the fingerprint submissions after the records are searched; (D) An appeal mechanism; and (E) Penalties for misuse of the information.

Response. Subjects of criminal screens are given far more rights and protections if the screen is conducted by a commercial company acting as an intermediary between the consumer and the end user, rather than by a government agency or by an end user directly. Government agencies and direct employer screens are not required to adhere to the strict privacy and consumer protection precepts of the FCRA. Whenever an employment screening company provides reports on job applicants or employees for employers, it acts as a consumer reporting agency and it must comply with the FCRA. The FCRA also imposes certain obligations on employers who use these reports. Before requesting a consumer report on a prospective or current employee, the employer must tell the individual in writing[2] that the employer is going to obtain the report, and the employer must get the individual's written authorization to obtain the report. 15 U.S.C. Sec. 1681b(b).

If an employer decides to take an adverse action, whether based entirely or even just in part, on information in a consumer report, the individual has the right to see the consumer report that formed the basis for the employer's decision. Therefore, *before* taking the adverse action, the employer must provide the individual with a copy of the report and an FTC compliant "Summary of Consumer Rights," which will have been provided by the consumer reporting agency along with the consumer report.

Within three days of taking the adverse action, employers must give the individual notice of the adverse action. The adverse action notice must include, among other things: (1) a statement that adverse action has been taken based on a consumer report; (2) the name, address, and phone number of the consumer reporting agency that provided the report; and (3) a statement of the person's right to receive a free copy of his or her report within 60 days and the right to dispute with the consumer reporting agency the accuracy or completeness of the information contained in the report. *Id*., Sec. 1681b(b)(3).

If a report includes public record information that is likely to have an adverse effect upon a consumer's ability to obtain employment, the consumer reporting agency must either: (1) notify the consumer when the public record information is reported, giving the consumer the name and address of the employer requesting the report; or (2) maintain strict procedures designed to insure that this public record information is complete and up to date. *Id*., Sec. 1681k.

[2] There are a few narrow circumstances where employment notices need not be in writing, but those are not discussed here. See, 15 U.S.C. Secs. 1681b(b)(2)(B), (C); 1681b(b)(3)(B),(C); 1681b(4); 1681a(x).

Violations of the FCRA by consumer reporting agencies, data furnishers, or data users may be pursued in federal or state court, by consumers, state attorneys general, or the FTC. Further, violations of state-FCRAs may also be brought in state court by consumers and other state officials authorized to bring such actions.

Sec. 6403(d)(8). Which requirements should apply to the handling of incomplete records.

Response. When the FCRA applies (see the preceding response) consumers have a right to dispute the completeness or accuracy of the information contained in a criminal background check. *Id*., Sec. 1681i.

Sec. 6403(d)(10). The type of restrictions that should be prescribed for the handling of criminal history information by an employer.

Response. Criminal histories used by employers supplied by a commercial background check company operating as a consumer reporting agency would be governed by the FCRA and the protections in that Act serve as sufficient consumer protections.

Sec. 6403(d)(15). Any other factors that the Attorney General determines to be relevant to the subject of the report.

Response – Social Security Numbers. Full Social Security numbers (SSNs) are critical for performing adequate criminal screens. In recent years a number of federal and state courts have limited access to all or parts of SSNs in public records. See, Fed. R. Bankruptcy P. 1005. Anything less than full SSN access will reduce the effectiveness of a criminal background check and could do substantial harm to the public health and safety.

We live in a very transient society. There are 14 million annual address changes in the U.S., 43 million vacation and second homes, and 3.8 million marriages and divorces annually with attendant name changes. In addition, 4.5 million Americans have one of two last names (Smith or Johnson), 14 million have one of ten last names, 26.6 million females have one of ten first names and 57.7 million males have one of ten first and last names. As was noted by the Federal Trade Commission "Social Security numbers today are a vital instrument of interstate commerce. With 300 million Americans, many of whom share the same name, the unique 9-digit Social Security number is a key identification tool for business." *Hearing on Identity Theft Before the Senate Commerce, Science and Transportation Comm.*, June 16, 2006 (109th Cong.) (statement of the Federal Trade Commission).

Public records should remain public for the benefit of the public. The only way law enforcement, employers, security companies, and others can ever hope to sort out legitimate and non-legitimate SSN holders and track individuals across state lines for effective criminal screens is through full access to SSNs from as many disparate sources as possible, including court records.

Response – Bulk Access to Court Records. Criminal record screens can be enhanced to protect society at large by encouraging federal and state courts to provide access to criminal records in bulk electronic transmissions. These bulk transmissions should be limited to qualified commercial screening companies which certify that they comply with the FCRA.

In sum, commercial background screening companies are regulated by a number of federal and state laws; their information comes from disparate public and private data sources which offer "one of the most reliable and comprehensive sources of [identifying] information", *Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcom. on Social Security*, June 15, 2004 (107th Cong.) (statement of J. Howard Beales, III, Director of the

Bureau of Consumer Protection, Federal Trade Commission). Commercial background screening companies provide valuable and in some cases critical assistance to public and private sector customers; and society is best served when these companies are used to perform background checks.

We hope that this comment has been helpful to you. Please feel free to contact us for additional information or questions.

Sincerely,

Eric J. Ellman
Director and Counsel, Government Relations