Identity and Intelligence Analytics

A Report to the Governor, House Appropriations Committee, and Senate Finance Committee

November 2014

Colonel W. Steven Flaherty
Superintendent

Colonel W. S. (Steve) Flaherty
Superintendent

(804) 674-2000

Lt. Colonel Robert B. Northern
Deputy Superintendent

COMMONWEALTH OF VIRGINIA

DEPARTMENT OF STATE POLICE
P. O. Box 27472, Richmond, VA 23261-7472

November 15, 2014

TO: The Honorable Terence R. McAuliffe, Governor of Virginia

The Honorable Charles J. Colgan
Co-Chairman of the Senate Finance Committee

The Honorable Walter A. Stosch
Co-Chairman of the Senate Finance Committee

The Honorable S. Chris Jones
Chairman of the House of Appropriations

Pursuant to Item 414 (0) of the 2014 Appropriation Act, I am respectfully submitting herewith, a *Report on Identity and Intelligence Analytics*. The report is a compilation of the Department's research on the potential implementation of the Intelligence Analytics System.

Respectfully,

W. S. Flaherty

Superintendent

WSF

Enclosure

Background

In accordance with Item 414 (0) of the 2014 Appropriation Act, the Department of State Police has reviewed the costs and benefits of acquiring state-of-the-art identity intelligence and intelligence analytics systems for use by the Department of State Police and other Virginia law-enforcement agencies.

Review and Response

On February 24, 2014, a meeting was held in the office of Delegate Steve Landes. The meeting was attended by executives from SHINE Systems and Technologies and the Superintendent of State Police, Colonel W. Steven Flaherty. There was consensus at the meeting that the SHINE product, CHAIN, was not a viable solution at this time, and that Virginia law does not allow such collections of biometrical data on a citizen unless certain crimes have been committed by that individual. It should also be noted that the product, CHAIN, had not yet been developed.

The Virginia Department of State Police has entered into a contractual agreement with Palantir Technologies to replace its legacy intelligence and analysis capability with a state-of-the-art intelligence management system called the Virginia Intelligence Management System or VIMS. This system meets the Department's present needs regarding intelligence analytics, and complies with Virginia law.

VIMS is a customized, intelligence management system that handles collection, management, retention and dissemination of intelligence according to the Virginia Fusion Center's workflow and in accordance with state and federal law. VIMS has a federated-search capability that interfaces with numerous traditional law enforcement data sources to support investigations only under the auspices of reasonable suspicion of criminal activity. This methodology, that intuitively assembles lawfully collected and maintained law enforcement information on suspected or known criminal activity, is commonly referred to as "intelligence analytics." The contract between Palantir Technologies and the Virginia Department of State Police is VITA-compliant, and includes a maintenance agreement in effect through 2018. The total cost of this initiative is $2.18 million.

Currently, there are legal prohibitions in Virginia related to biometric data collection unless there is a conviction of certain crimes. Furthermore, the analytic processes for biometric data have yet to be fully developed by SHINE Systems and Technologies for law enforcement purposes. In addition, there is a lack of legally collected biometric data sources. Moreover, current Virginia law covering "Government Data Collection and Dissemination Practices" requires that such biometric data have a clearly established need in advance of collecting and building "identity intelligence" counterparts.

“§ 2.2-3800. Short title; findings; principles of information practice.

A. This chapter may be cited as the "Government Data Collection and Dissemination Practices Act."

B. The General Assembly finds that:

1. An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

2. The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

3. An individual's opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and

4. In order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

C. Recordkeeping agencies of the Commonwealth and political subdivisions shall adhere to the following principles of information practice to ensure safeguards for personal privacy:

1. There shall be no personal information system whose existence is secret.

2. Information shall not be collected unless the need for it has been clearly established in advance.

3. Information shall be appropriate and relevant to the purpose for which it has been collected.

4. Information shall not be obtained by fraudulent or unfair means.

5. Information shall not be used unless it is accurate and current.

6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.

7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse. On and after July 1, 2004, no agency shall display the social security number of a data subject on a student or employee identification card,

except that for universities and colleges that have such a prevention plan for misuse of personal information in place on or before July 1, 2004, in compliance with this section, the date shall be January 1, 2005. On and after July 1, 2006, no agency shall display an individual's entire social security number on any student or employee identification card.

9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.

10. The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

D. After July 1, 2004, no agency, as defined in § 42.1-77, shall send or deliver or cause to be sent or delivered, any letter, envelope or package that displays a social security number on the face of the mailing envelope or package or from which a social security number is visible, whether on the outside or inside of the mailing envelope or package."

The Government Data Collection and Dissemination Practices Act (GDC) prohibits the Department from gathering, storing and analyzing biometric data unless "**the need for it has been clearly established in advance.**" Furthermore, an interpretation should be made as to whether "combating terrorism" or "solving crimes" is a "**need clearly established in advance.**" Section C. 3 states "**Information shall be appropriate and relevant to the purpose for which it has been collected.**" Stated differently, every piece of biometric data gathered, stored and analyzed must have a specific and relevant nexus to the reason it has been collected.

Therefore, before requirements or cost assessments for an "identity intelligence and analytics" software or database can be proposed, Virginia law must be changed, in order to make such efforts legal in the Commonwealth.