IJIS Institute

CONTRACTOR PERSONNEL BACKGROUND CHECKS

IJIS Institute White Paper

Joint Committee Task Force

Criminal Justice Information Services Program Advisory Committee (CPAC) and the IJIS Public Safety Technical Standards Committee (IPSTSC)

September 2011

Principal Contributors

CPAC
- Bruce Kelling, Athena Advanced Networks
- Vijay Mehra, KYM Advisors
- Dwight Hunter, Hunter Research
- David Gavin, IACP

IPSTSC
- Steve Hoggard, Spillman Technologies
- Robert Turner, CommSys Incorporated
- Tom Dewey, Advanced Justice Solutions
- Michael Smith, Spillman Technologies

THE IJIS INSTITUTE
- Greg Trump

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following additional contributors and their sponsoring companies for supporting the creation of this document:

Bruce Kelling, *Athena Advanced Networks*
Vijay Mehra, *KYM Advisors*
Dwight Hunter, *Hunter Research*
David Gavin, *IACP*
Steve Hoggard, *Spillman Technologies*
Robert Turner, *CommSys Incorporated*
Tom Dewey, *Advanced Justice Solutions*
Michael Smith, *Spillman Technologies*

CONTENTS

INTRODUCTION

The IJIS Institute commissioned a task force to conduct a study on the FBI Criminal Justice Information Service (CJIS) background check process for contractor personnel. Initial findings indicated:

- Providers and practitioners exhibited widespread confusion and misunderstanding regarding the CJIS policy and its related processes. This specific background check process can introduce complications that affect cost and time delays on information system projects and support activities.
- Issues are complex and multi-faceted, especially when dealing in a multi-state environment. Such an example might be someone working for a company located in one state, living in another, and working on projects in several other states.
- Questions may arise about an employee's personal life and how often contractor personnel should be re-verified. As with much of the information sharing issues encountered in general, agencies are reluctant to rely on the work or conclusions of other agencies (although, the spirit of information sharing developing across the nation may help solve this problem). For example, a person working on a regional system may need to be verified by each agency participating in the system.
- Technology will help. Next Generation Identification (NGI) is a great solution that could be used to conduct rapid background checks on current contractor certification. This "rap-back" program could provide a way for a contractor certification system to be updated, though policy, process and procedures still need to be developed in order to support such background "monitoring".

The task force conducted several studies on multi-level policy and technology solutions such as:

- Education/training programs for industry
- Clearing houses or central repositories for contractor certification based on finger-print and photo identification
- Multi-stage clearance processes that would provide a temporary clearance based on a background check conducted within the past "n" years in order to provide more time for an updated background check. This temporary clearance would eliminate some of the delays currently encountered.
- A recertification process due every "n" years

Recognizing that with the exception of an industry training program, industry can support solutions, but the solutions must come from the practitioner community. The FBI CJIS Security Officer is currently studying and working on many of the issues brought forth in this paper. The IJIS Institute recommends:

- The FBI CJIS Security Officer continue to study the issues and develop recommendations to take forth to the Advisory Policy Board (APB) process
- The IJIS Task Force work closely with and support the FBI CJIS Division to help create short and long range solutions.

OVERVIEW

Most systems supporting the Criminal Justice Information Technology environment are provided by industry. Many of the companies providing these products and services are members of the IJIS Institute. As technology and its associated business models change, IJIS Institute members are often at the forefront of such changes.

The CJIS security policy covers many aspects of information system security; members of the IJIS Institute are often called for consultation on how best to implement these policy requirements for local agencies. Often referred to as "service providers", most IJIS institute member companies deliver systems and solutions that comply with the requirements of the security policy.

The IJIS Institute and its members understand and support the need for background checks. The purpose of this paper is to note the shortcomings and gaps in practice that have been observed in the current policy. These observations are collectively drawn on the experience of IJIS Institute member companies.

Procedures currently used for the background checks of service provider employees indicate several gaps and loopholes. The challenge is not necessarily the policy, rather, how the policy is interpreted and how procedures are implemented from state to state to comply with the policy guidelines.

BACKGROUND

IJIS Institute service providers are among the leading companies that deliver and support software applications for local agencies, such as, but not limited to, Computer Aided Dispatch (CAD) systems, Records Management Systems (RMS), and information sharing platforms. These systems are at the front of law enforcement interaction with the public and provide collection points of information which will then be aggregated to regional, state and federal CJIS information systems. These systems, however, are subject to the requirement of the CJIS security policy.

IJIS Institute service providers, unlike most local agency personnel, provide systems to many different local agencies. Most of the commercially significant providers have in excess of 200 installed sites in more than 20 states.

SUPPORTING BACKGROUND CHECK REQUIREMENTS

Service providers understand the requirement and need for employee background checks. In fact, most companies do extensive background checks of new employees during the hiring process in order to prevent investing time, money and resources in someone only to find they are ineligible to work in the CJIS environment. Much like their government counterparts, service providers are just as interested in validating an employee's background for the same reasons.

The latest version of the CJIS security policy attempts to improve background check of contractors. It appears this policy was written more towards the idea of a resident contractor at a single agency versus a service provider employee that supports many agencies in different states.

ENVIRONMENTAL CHALLENGES

As service providers, companies are faced with an environment having several problems that impact them as well as end user customer agencies. Problems regularly encountered revolve around the following areas:

- Lack of consistency in application and documentation
- Logistical challenges
- Re-verification parameters

CONSISTENCY OF APPLICATION

One of the frustrations that companies encounter is the inconsistent application of background checks. The security policy calls for a "fingerprint based background check in the state of residency". On the surface this seems simple enough; however, there are a number of different issues in actual practice.

The policy is clear on the need for a background check in the state of residency; though, many times, because the request for the check surfaces in the state of the project, the fingerprint background check is completed in the state of the project and not the state of residency.

If the contracting agency requests a state-based check be performed by the state where the employee resides, then an information exchange agreement is required before the state-based check can be returned to the contracting agency. This process is many times not understood nor followed.

In some states, where there is a state level program for certification of products, some companies are more visible to the state, yet other companies are not and their checks are handled inconsistently. Other states require more stringent checks for all companies.

Generally, practitioners are not well versed on the need for and the process of conducting employee background checks, especially when considering multi-state implications. With many employees working in a virtual environment or being consistently on the road, there is clearly room for confusion.

LOGISTICAL CHALLENGES

The goal of the fingerprint is to verify a person's identification by using the Integrated Automated Fingerprint Identification System (IAFIS) or NGI systems. The fingerprint requirement has created several dramatic logistical challenges for service providers and agencies.

For one, fingerprints are expensive. They involve the individual, a Livescan or print card, and a fingerprint technician to capture the person's prints. The capture of fingerprints is a lengthy process, and because an agency bills for a technician's time, it is also expensive. This expense is generally billed to the service provider since the agency taking the prints rarely has a contractual agreement with service providers. Employees do not always live in the immediate proximity of the contracting agency; therefore, fingerprints are taken, produced on a ten-print card, forwarded to the contracting agency, who then submits the card to the state system for a background check.

Those in government may take the position of "it's the service provider's problem," when dealing with the steps involved in obtaining a background check. This view is true, however, like most other commercial entities, service providers must recover costs associated with "doing business." These costs are included directly through specific charges with the contracting agency, or indirectly by raising the cost of products, services or labor charges.

There are other logistical challenges that impact a contracting agency as well. Scheduling, for one, can be a problem if the logistics of fingerprinting are an issue. As an example, one state has a six month delay or more in processing ten-print cards. Consequently, most agencies in that state require a Livescan be used for capturing fingerprints. This becomes even more logistically challenging since most states are unable to share prints between disparate state systems, therefore, the employee must visit the state of the contracting agency, or a certified Livescan contractor must visit the service provider's facility to capture prints. Regardless, either option is costly.

RE-VERIFICATION AND MAINTENANCE

One of the greatest concerns to service providers are those employees who undergo a background check, having committed a crime at some point, thereby making them ineligible to work in the CJIS environment. Employees can be assigned to long term projects, some multi-year in duration, during which an employee could commit a crime making them ineligible. Unless the crime involved their employment, the employer may never know a crime had been committed.

The "rap-back" capability of the NGI system will improve this situation, though it now introduces another set of challenges. As employees move from company to company and project to project, many agencies will attach their information. If an employee becomes ineligible, all of the agencies that have worked with this individual are notified. The challenge may arise when a person is no longer working with a company or project involving that agency, yet they receive the notification, thus beginning another cycle of investigations on a person who is no longer relevant.

One of the greatest gaps in the policy is the management of employee departures and hiring. When an employee is brought onto a "project", which is typically a new system implementation, they are checked by the local contracting agency. If an employee is brought into the customer support organization that provides remote telephone and system support to local agencies in many states, there is the possibility of no background check beyond that of the employer. Support organizations vary in size from a few individuals, to 25 or more. Local agencies, for the most part, are aware of the problem, yet most choose to ignore the issue, trusting the company has followed proper procedure.

RECOMMENDATIONS

The IJIS Institute proposes the following recommendations to alleviate the challenges of background checks, including:

- Education/training programs for industry
- Clearing houses or central repositories for contractor certification based on fingerprint and photo identification
- Multi-stage clearance processes that would provide a temporary clearance based on a background check conducted within the past "n" years in order to provide more time for an updated background check. This temporary clearance would eliminate some of the delays currently encountered.
- A recertification process due every "n" years

Recognizing that with the exception of an industry training program, industry can support solutions, but the solutions must come from the practitioner community. The FBI CJIS Security Officer is currently studying and working on many of the issues brought forth in this paper. The IJIS Institute recommends:

- The FBI CJIS Information Security Officer continue to study the issues and develop recommendations to take forth to the APB process
- The IJIS Task Force work closely with and support the FBI CJIS Division to help create both short and long range solutions.

ABOUT THE IJIS INSTITUTE

The IJIS Institute unites the private and public sectors to improve critical information sharing for those who provide public safety and administer justice in our communities. The IJIS Institute provides training, technology assistance, national scope issue management, and program management services to help government fully realize the power of information sharing.

Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus in Ashburn, Virginia, the IJIS Institute has grown to nearly 200 member and affiliate companies across the United States.

The IJIS Institute does its valuable work through the contributions of its member companies. The IJIS Institute thanks the Emerging Technologies Advisory Committee for their work on this document.

The IJIS Institute also thanks the many companies who have joined as members that contribute to the work of the Institute and share in the commitment to improving justice, public safety, and homeland security information sharing.

LINKS TO MORE INFORMATION

The IJIS Institute
http://www.ijis.org

ACRONYMS

- APB: Advisory Policy Board
- CAD: Computer Aided Dispatch
- CJIS: Criminal Justice Information Services
- CPAC: CJIS Program Advisory Committee
- IAFIS: Integrated Automated Fingerprint Identification System
- INSH: Information Sharing Committee
- IPSTSC: IJIS Public Safety Technical Standards Committee
- NCIC: National Crime Information Center
- NGI: Next Generation Identification
- RMS: Records Management Systems