	Interstate Commission for Juveniles	Opinion Number: 01-2015	Page Number: 1
ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters			
Description: ICJ authority to conduct records checks for another state on juveniles not subject to ICJ.	Dated: February 24, 2015 Revised: March 1, 2018 ¹		

Background:

Pursuant to ICJ Rule 9-101(3), the ICJ Executive Committee has requested an advisory opinion regarding the requirements of the Compact and ICJ Rules on the following issue:

Issues:

ICJ member states are receiving occasional requests to conduct records checks on juveniles not currently involved in the ICJ process, but as a matter of courtesy. This has caused members of the ICJ Executive Committee, who have become aware of this practice, to pose a number of concerns related to the legal authority to conduct such records checks.

Applicable Compact Provisions and Rules:

ICJ Article I, in relevant part, provides that:

It is the purpose of this Compact, through means of joint and cooperative action among the Compacting states to: . . . (J) establish a system of uniform data collection **of information pertaining to juveniles subject to this Compact** that allows access by authorized juvenile justice and criminal justice officials; (emphasis supplied).


ICJ Article III (K) provides that:

The Interstate Commission shall collect standardized data concerning the interstate movement of juveniles as directed through its rules which shall specify the data to be collected, the means of collection and data exchange reporting requirements. Such methods of data collection, exchange and reporting shall insofar as is reasonably possible conform to up-to-date technology and coordinate its information functions with the appropriate repository of records. (emphasis supplied).

ICJ Rule 2-102(1)¹ provides as follows:

“As required by Article III (K) of the compact, the Interstate Commission shall gather, maintain and report data regarding the interstate movement of juveniles who are supervised under this

¹ This Advisory Opinion has been revised to reflect ICJ Rules in effect March 1, 2018. The previously published opinion is available upon request from ICJadmin@juvenilecompact.org.

	Interstate Commission for Juveniles	Opinion Number: 01-2015	Page Number: 2
ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters			
Description: ICJ authority to conduct records checks for another state on juveniles not subject to ICJ.	Dated: February 24, 2015 Revised: March 1, 2018 ¹		

compact and the return of juveniles who have absconded, escaped or fled to avoid prosecution or run away.”

ICJ Rule 2-106² provides as follows:

“Upon request by a member state ICJ Office, other member state ICJ Offices may share information regarding a juvenile who crosses state lines to determine if they are or may be subject to the ICJ.”


Analysis and Conclusions:

The above referenced provisions of the ICJ Compact and Rules, clearly evince an intent to provide authority to the ICJ member states to collect, maintain, report, and exchange data ‘concerning’ or ‘pertaining’ to the “interstate movement of juveniles who are ‘subject to’ and ‘supervised under this Compact.’” These provisions further permit such data to be collected and exchanged with regard to “the return of juveniles who have absconded, escaped or fled to avoid prosecution or run away.” See ICJ Article III (K); ICJ Rule 2-102(1) and ICJ Rule 2-106.

Both the foregoing provisions of the ICJ and the ICJ Rules require the Compact member states to implement the law enforcement and public protection aspects of the Compact through “a system of uniform data collection,” (See Article I (J)) and shall be by means of, “[S]uch methods of data collection, exchange and reporting shall insofar as is reasonably possible conform to up-to-date technology and coordinate its information functions with the appropriate repository of records,” (See Article III (K)).

Consistent with these requirements, the Commission has developed the Juvenile Interstate Data System (JIDS), as referenced above. Because of the sensitive nature of this information, as was previously pointed out in ICJ Advisory Opinion 01-2014, the JIDS ‘application,’ as set forth in JIDS’ Security documentation, “. . . is an electronic workflow system that facilitates state-to-state transfers, returns and travel for juveniles.” Access to the system is required through a “secure web portal provides automation to paper-based processes and creates accountability through all steps in the process. InStream maintains Advanced Encryption Standards defined by the National Institute of Standards and Technology (NIST) for content storage and

² To provide additional guidance regarding this issue, ICJ Rule 2-106 was adopted September 27, 2017, effective March 1, 2018.

	Interstate Commission for Juveniles	Opinion Number: 01-2015	Page Number: 3
ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters			
Description: ICJ authority to conduct records checks for another state on juveniles not subject to ICJ.	Dated: February 24, 2015 Revised: March 1, 2018 ¹		

transmission.” (See ICJ Ad. Op. 01-2014 and the JIDS Security Newsletter, attached and incorporated by reference therein). Further, JIDS meets the criteria set forth by NLETS, the interstate justice and public safety network for the exchange of law enforcement, criminal justice, and public safety related information and is furnished through a web service which is utilized by the U.S. Department of the Treasury and the U.S. Department of State, among others, which require secure data exchange. Additionally, all information contained in JIDS is encrypted.

It is apparent that while collection and dissemination of data is authorized under the Compact provisions and ICJ Rules, this authority is limited by the terms of the Compact to **“data ‘concerning’ or ‘pertaining’ to the “interstate movement of juveniles who are ‘subject to’ and ‘supervised under this Compact.’”** See ICJ Art. III (K) and ICJ Rule 2-102(1). Additionally, the Commission has, as it is legally obligated to do, engaged in the ‘due diligence’ required to protect this information from both unauthorized access and disclosure by ICJ member states through the establishment and maintenance of the JIDS system as described above.

The information, about which the ICJ Executive Committee is concerned in making this opinion request, is described as “records checks on juveniles not currently involved in the ICJ process, but as a matter of courtesy.” Thus, the express language of the foregoing Compact statute provisions in Article I (J) and Article III (K) as well as Rule 2-102(1) does not appear to authorize the collection or sharing of information concerning the interstate movement of juveniles who are not ‘subject to’ or ‘supervised under’ this Compact. As the U.S. Supreme Court has determined with respect to statutory construction, “Our first step in interpreting a statute is to determine whether the language at issue has a plain and unambiguous meaning ... [O]ur inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent.” See *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997).

Summary:

In sum, the express language of the foregoing Compact Statute provisions in Article I (J) and Article III (K), as well as Rule 2-102 (1), does not appear to authorize the collection or sharing of information concerning the interstate movement of juveniles who are not ‘subject to’ or ‘supervised under’ this Compact. However, pursuant to Rule 2-106, state ICJ Offices may share information regarding a juvenile who crosses state lines to determine if they are or may be subject to the ICJ.

JIDS Security Newsletter

Sent May 1, 2012

In preparation for the implementation of the Juvenile Interstate Data System (JIDS), the Technology Committee is publishing a number of short articles as part of the preparation process. Each article will discuss an aspect of the implementation with the goal of helping your staff to be prepared for a new way of doing business.

Overview of JIDS Security

JIDS is a web-based application developed for the Interstate Commission for Juveniles by InStream, Inc. The equipment to host JIDS is provided by Amazon on their government cloud servers.

The JIDS application is an electronic workflow system that facilitates state-to-state transfers, returns and travel for juveniles. The application's secure web portal provides automation to paper-based processes and creates accountability through all steps in the process. InStream maintains Advanced Encryption Standards defined by the National Institute of Standards and Technology (NIST) for content storage and transmission.

Site Security

InStream

Building security requires key card access at multiple points of entry into the building, into server areas, and document conversion work areas 24/7. Visitors are required to sign in when entering the InStream offices and are accompanied at all times.

The facility has security patrols during all non-business hours and is equipped with alarm monitoring and cameras at point of entry. Random audits occur on security logs, e-mail transmissions, system security and physical security.

Amazon Web Service

Amazon Web Service (AWS) datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass a two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services,

and documents how to use those features. AWS's compliance framework covers FISMA, PCI DSS, ISO 27001, SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), and HIPAA.

Amazon's Federal Government Customers include:

- Recovery Accountability and Transparency Board
- U.S. Department of the Treasury
- National Renewable Energy Laboratory at the U.S. Department of Energy
- U.S. Department of State
- U.S. Department of Agriculture
- NASA Jet Propulsion Laboratory
- European Space Agency

Amazon Web Service meets the following criteria set forth by NLETS, the interstate justice and public safety network for the exchange of law enforcement, criminal justice, and public safety related information:

- Provides a secure environment with redundant technical infrastructure and onsite expertise monitoring hardware and connectivity 24/7/365
- Monitored by both fixed and pan-tilt/zoom security cameras
- Protected by intrusion detection system with panic button activation
- Two-factor authentication for building access
- Biometric authorization for data center access
- Extensive pre-employment background investigation process for employees with data access
- On-site building security and data center monitoring staffed 24/7/365
- Robust, scalable, private, secure network
- Back-up generator and uninterrupted power supplies to ensure no loss of power
- Network racks are equipped with temperature and humidity sensors that are centrally monitored
- Site is protected by sophisticated, dual fire suppression systems
- Secondary hosting services are located at a Disaster Recovery location, allowing for multiple business continuity plans
- Remote services provided 24/7/365 by on-site technicians

Application Security

JIDS is a web-based application developed by InStream, Inc. and hosted by Amazon Web Service for ICJ. InStream is responsible for implementation and maintenance of all technical security controls protecting the application, as well as administrative controls dealing with the development and support of the application. ICJ is responsible for the administrative controls related to the operation of the application.

Encryption

All information contained in JIDS is encrypted. Security features include:

- Encryption for documents 'at rest' and document storage

- IIS SSL compatible (a secure infrastructure based on public-key cryptography by using digital certificates with Secure Sockets Layer (SSL))
- Allows changing Anonymous & IUSR IIS accounts
- File permissions securable by NTFS and security groups
- Able to encrypt plain-text passwords
- 128 bit encryption

Authentication

Users are uniquely identified to the system by their email address authenticated with a password.

Password Requirements

Passwords shall:

- be a minimum length of eight (8) characters, a mix of lowercase, uppercase and one special character
- not be a dictionary word or proper name
- not be the same as the User ID
- be changed within a maximum of every 90 days
- not be identical to the previous ten (10) passwords
- not be transmitted in the clear outside the secure location
- not be displayed when entered

A user will be allowed five (5) login attempts before being locked out.

Password Recovery

Users have the ability to reset their passwords by requesting a recovery that will facilitate the user being able to reset their password.

Authorization

All data is properly secured with specific rights customized to a group, project or user based on their role. JIDS uses a role based access control model to ensure that individual user access rights are sufficient to perform their required job functions. The workflow set up in JIDS requires review and sign-off at several levels to ensure processes are reviewed and approved as they progress through the system.