Call to Action

A Global Unified Message Regarding Information Sharing

We encourage agency leaders to adapt advances in technology and use best practices identified in this call to action to enhance information sharing.

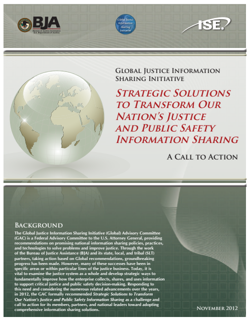
- Plan for Information Interoperability
- Use Trusted Providers and Systems
- Apply Best Practices

Challenge

Since September 11, 2001, great advances have been made in sharing information among federal, state, and local partners, as realized by the efforts made to connect criminal intelligence and criminal justice databases, federate database searches, and develop shared services. While these steps have vastly improved information sharing, the adoption of new information technology (IT) has been uneven. Development and implementation of new policies associated with IT advances take time and often do not adequately consider information sharing goals.

Background

The 2012 Global Justice Information Sharing Initiative Call to Action, titled "**Strategic Solutions to Transform Our Nation's Justice and Public Safety Information Sharing**," recommended more effective, efficient, and coordinated technical, policy, and funding activities for IT solutions and practices. The recommendations have not changed, even though IT and sharing capabilities have evolved. The Criminal Intelligence Coordinating Council (CICC) established a multipartner Criminal Intelligence/Information Technology Crossroads Committee (CI/IT) to better coordinate the actions of agencies and associations facing similar IT and policy challenges and issues that have emerged from modern IT. The Crossroads Committee developed and approved the information sharing best practices described in this call to action to help address the complex information sharing environment.



BJA

ISE.

GLOBAL JUSTICE INFORMATION SHARING INITIATIVE

STRATEGIC SOLUTIONS TO TRANSFORM OUR NATION'S JUSTICE AND PUBLIC SAFETY INFORMATION SHARING

A CALL TO ACTION

BACKGROUND

The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) is a Federal Advisory Committee to the U.S. Attorney General, providing recommendations on promising national information sharing policies, practices, and technologies to solve problems and improve justice. Through the work of the Bureau of Justice Assistance (BJA) and its state, local, and tribal (SLT) partners, taking action based on Global recommendations, groundbreaking progress has been made. However, many of these successes have been in specific areas or within particular lines of the justice business. Today, it is vital to examine the justice system as a whole and develop strategic ways to fundamentally improve how the enterprise collects, shares, and uses information to support critical justice and public safety decision-making. Responding to this need and considering the numerous related advancements over the years, in 2012, the GAC formally recommended *Strategic Solutions to Transform Our Nation's Justice and Public Safety Information Sharing* as a challenge and call to action for its members, partners, and national leaders toward adopting comprehensive information sharing solutions.

NOVEMBER 2012

Global Justice Information Sharing Initiative

Issued May 2019

PLAN

Plan for System Interoperability

Data owners should prioritize information interoperability (e.g., the ability of computer systems to access and exchange information) in order to share data efficiently, in accordance with applicable laws. This will allow better allocation of resources to plan and implement technical solutions, as well as to increase connectivity and information sharing among partners. Actions include developing:

- Information sharing policies and practices.
- Enhancements to existing data sharing capabilities and partnerships.
- A three- to five-year information sharing plan.

USE

Use Trusted Providers and Systems

Agencies are encouraged to incorporate nationwide information sharing programs into their policies and plans to leverage existing trusted information sharing platforms. These providers and systems include the following:

- RISSIntel (28 CFR Part 23)—Criminal Intelligence
- HSIN-Intelligence (HSIN-Intel)—Intelligence-Focused Community of Interest on HSIN
- FBI N-DEx—Records Management Systems
- ODMAP/ODFORM—Drug Overdose Reporting
- FirstNet—Communications/Operations
- National Incident-Based Reporting System (NIBRS)—Crime Reporting
- Nationwide Officer Safety Event Deconfliction—Event Deconfliction
    - Case Explorer, RISSafe, or SAFETNet
- Nationwide Deconfliction Pointer Solution—Target Deconfliction
- Deconfliction and Information Coordination Endeavor (DICE)—Investigative Deconfliction
- Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—Suspicious Activity
- eTrace—Crime Gun Tracing
- Bomb Arson Tracking System (BATS)—Reporting Bombing/Explosive and Arson Incidents
- National Seizure System (NSS)—Drugs, Weapons, and Currency Seizure
- National Missing and Unidentified Persons System (NamUS)

The resources listed above and many additional resources are available on key information sharing systems, including Regional Information Sharing Systems (RISS), Homeland Security Information Network (HSIN), Law Enforcement Enterprise Portal (LEEP), El Paso Intelligence Center (EPIC), International Justice and Public Safety Network (Nlets), and Intelink.

APPLY

Apply Best Practices

Data owners are encouraged to incorporate lessons learned and information sharing best practices to improve access to data while ensuring privacy, civil liberties, and civil rights protection and data security. Specific lessons learned include the following:

- Ensure that new technology applications are implemented in conjunction with agency policy.[1]
- Remain cognizant of vendor motivations; your data has value. Also ensure data storage location and ownership when purchasing a new IT product.
- Develop and apply national data information sharing standards (e.g., NIST, NIEM/LEXS, NIEF/GFIPM/SAML) as appropriate to enhance interoperability.
- Ensure that new vendor products support data owners' information sharing objectives.
- Research partner capabilities to avoid duplication and/or incompatible data repositories.
- Consider participation in the CI/IT Crossroads Committee to remain aware of current issues and concerns.[2]

[1] International Association of Chiefs of Police Technology Policy Framework–http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf

[2] Email cicc@iir.com to request participation in the CI/IT Committee.

BJA
Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant Number 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative and the Office of the Director of National Intelligence, National Security Partnerships. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or Office of the Director of National Intelligence.