U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Forensic Intelligence Models:

Assessment of Current Practices in the United States and Internationally

February 2023

Tara Garvey
Greggory LaBerge
Julie Wartell

NCJ 305898

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

U.S. Department of Justice
Office of Justice Programs
810 Seventh St. N.W.
Washington, DC 20531

Nancy La Vigne, Ph.D.
Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
Strengthen Science • Advance Justice
NIJ.ojp.gov

Office of Justice Programs
Building Solutions • Supporting Communities • Advancing Justice
OJP.gov

The National Institute of Justice is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

Opinions or conclusions expressed in this paper are those of the authors and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Background

Modern law enforcement is transitioning from reactive policing to proactive, intelligence-led, and data-driven policing to increase efficiency, transparency, public trust, and public safety. This document summarizes NIJ's Forensic Intelligence Framework Initiative, a project in which subject matter experts examined the implementation of forensic intelligence models that support law enforcement operations and modernization efforts to inform the development of a forensic intelligence framework. It also provides an overview of considerations for implementing forensic intelligence activities, such as organizational structure, key partnerships, enhanced communications, and the development of resources (technologies, workflows, policies, and training). The project included an initial workshop in Washington, D.C., during which federal partners presented their agencies' work relating to forensic intelligence. The project continued by concentrating on a detailed study of seven sites — five domestic U.S. sites and two international sites — that represent various levels of forensic intelligence implementation. The sites selected were:

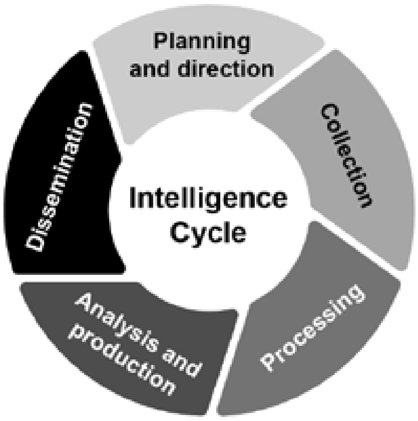
- Cuyahoga County Prosecutor's and Medical Examiner's Offices and Case Western Reserve University, Cleveland, Ohio
- Denver Police Department, Denver, Colorado
- Milwaukee Police Department, Milwaukee, Wisconsin
- New Jersey State Police, West Trenton, New Jersey
- Philadelphia Police Department, Philadelphia, Pennsylvania
- Australian Federal Police, Canberra, Australia
- Neuchâtel Police and the University of Lausanne, Switzerland

In addition to the knowledge gained through the site visits, this report is based on the subject matter experts' collective experience working in the field, the published literature on the topic, and discussions with other subject matter experts.

What Is a Forensic Intelligence Model?

A forensic intelligence model is a set of operations that expand on other forms of intelligence (e.g., criminal and spatial intelligence). Forensic intelligence is generated through the analysis of scientific (i.e., forensic) data, often enhanced by combining other sources of intelligence, such as human intelligence and open-source intelligence. Like other forms of intelligence, it is used to drive operations within a law enforcement agency to identify crime trends, assist with deployment and operations, drive investigations, and enhance public safety. A forensic intelligence model is often incorporated into intelligence-led policing approaches to crime detection and investigation based on the intelligence cycle, a well-established model for conducting intelligence operations. The intelligence cycle (exhibit 1) is a dynamic process in which planning, operations, collections, and analysis are coordinated to develop raw information into finished intelligence products that can be disseminated to leadership, policymakers, and other end users.

Exhibit 1. The Intelligence Cycle



Note: Forensic intelligence models are based on the intelligence cycle, which is a well-established model for conducting intelligence operations.

Planning and direction are the first steps in any intelligence operation. In this first stage, intelligence requirements are established to determine the types of information that need to be collected. Comprehensive intelligence programs that fully utilize the intelligence cycle in their operations, like the New Jersey State Police Regional Operations and Intelligence Center and the Philadelphia Police Department, have standing intelligence requirements that guide their overall intelligence collection efforts. When programs include intelligence derived from forensic science, identifying the available data types that can support these requirements is necessary. Forensic intelligence data do not often include the raw data derived from forensic examinations. Often, it is the forensic result, such as an identification of a person/thing or associations, that shows a link between multiple crime events. For example, the specific genotype results that constitute a DNA profile are typically important for the forensic case, but the fact that the DNA profile from a specific person was linked to multiple crime scenes would be of intelligence value. The data sources may include National Integrated Ballistic Information Network (NIBIN) correlations, drug analysis data, Combined DNA Index System (CODIS) hits, fraudulent documents, digital media evidence, latent print matches, and other forensic results (exhibit 2). Planning and direction can be at both the strategic and tactical levels. At the tactical level, planning includes case-specific requirements. At the strategic level, planning and direction are based on patterns and trends for the purposes of planning, decision-making, and resource allocation. As this process is cyclic, intelligence produced from these requirements will support future planning and direction.[1]

Exhibit 2. Examples of Types of Data Used in Intelligence Analysis

Forensic Science Data Types (Results)	Other Data Types
• DNA results • Latent print results • Firearms and ballistics results • Gunshot residue results • Crime gun eTrace results • Test fires and cartridge case comparison results correlations • Drug identifications • Shoe marks linkages • Questioned documents (e.g., handwriting) identifications and linkages • Digital evidence identifications and linkages • Forensic databases o Next Generation Identification o Automated Fingerprint Identification System (AFIS) o CODIS o NIBIN o Other internal databases	• Calls for service • Crime reports • Arrests • Spatial/base maps • Field interviews • Gang data • Demographic data • Drug prices • Drug market locations • Medical examiner overdose death toxicology data • Pawn shop data • Gun retailer data • Data on individuals on parole/probation • Automated license plate reader data • Camera footage • Open-source data

The **collection** of information or data aligned with the intelligence requirements is the next step in the intelligence cycle. A key to the success of any forensic intelligence program is the collection of forensic data. Regardless of the data source, a successful program requires timeliness in the receipt, examination, and reporting of forensic results to generate actionable intelligence products and downstream action planning. Intelligence products that are not timely or actionable cease to be intelligence and may be relegated to dated crime statistics and trends. Therefore, the collection of forensic data and the ability to push the information forward in the intelligence cycle are critical elements for success.

Once the forensic science provider releases data, various entities are responsible for **processing, collation, and analysis** to produce actionable intelligence products. From the basic use of forensic data to investigate and target specific types of patterns, crimes, and individuals, forensic intelligence programs enhance these capabilities to include a more sophisticated analysis of the forensic data in combination with other sources of intelligence to generate finished products for both tactical and strategic purposes.

Dissemination of actionable intelligence can be accomplished by traditional methods of releasing finished strategic or tactical analytic products, often through an intelligence unit, to specified end users and by other less formal means such as local, regional, or national conference calls or meetings. These forums allow for the participation of not only the primary agency but also federal, state, and local partners, often resulting in strong collaborations and additional operational support. Any dissemination procedure should include a coordination process in which forensic science personnel review the intelligence product for technical accuracy prior to release.

A key to the success of any forensic intelligence model is the collection of forensic data. Regardless of the data source, a successful model requires timeliness in receiving, examining, and reporting forensic results to allow for the generation of actionable intelligence products and downstream action planning.

Implementation of Forensic Intelligence Models

The intelligence community has long used scientific data, including forensic data, to drive its intelligence operations. The concept of incorporating the collection and analysis of scientific data into intelligence operations is not new. However, most law enforcement agencies, especially at the state and local levels, have not used forensic science data to their full potential. Over the past 15 years, as many of these agencies began incorporating fusion centers, intelligence units, crime gun intelligence centers, or even a single, dedicated analyst into their operations, using forensic data for intelligence purposes has become feasible. Law enforcement agencies have begun to see the value of forensic data as a form of intelligence that can be used to support operations rather than simply supporting court cases, particularly for local or regional issues such as prolific gun violence, serial sexual assaults, or the opioid epidemic.

A forensic intelligence model should incorporate all the components of the intelligence cycle. Completely using the processes within the intelligence cycle is the goal of any intelligence operation. Focusing on state and local U.S. sites, two agencies — the New Jersey State Police Regional Operations and Intelligence Center and the Philadelphia Police Department — demonstrated the full use of this process in a comprehensive intelligence operation that included a forensic intelligence program. Of note, each of these organizations is structured with a separate intelligence unit. Both organizations have a fusion center that collaborates with its agency's forensic science components.

It is worth noting the capability of a fusion center and how it lends itself to supporting this type of forensic intelligence model. Fusion centers are intelligence centers located across the United States to support a state, region, or territory. These centers were originally created to combat terrorism and have taken on a broader role in providing intelligence analysis for all criminal activity in their area of operation through partnerships with federal, state, and local agencies. These partnerships are not only with other law enforcement agencies but also with community partners such as public health agencies, private corporations, fire and emergency medical services, and emergency management agencies. Often, representatives of the partner organizations are located at the fusion center. The structure allows for full execution of the intelligence cycle due to the capabilities that are housed in these centers, including intelligence analysts, technology, data sources, and federal, state, and local partners. The ability to incorporate forensic intelligence with other forms of intelligence to provide comprehensive and timely products is a benefit of having access to an intelligence center.

A forensic intelligence model should incorporate all the components of the intelligence cycle. Completely using the processes within the intelligence cycle is the goal of any intelligence operation.

The domestic and international sites examined in this project demonstrated that agencies with differing degrees of formal intelligence infrastructure and resources can successfully use forensic intelligence to direct their operations at different levels. Like other intelligence operations, forensic intelligence is a scalable capability that can be used in various agencies. The core of every intelligence program involves many or all steps of the intelligence cycle with different implementation approaches based on local, regional, state, or national agency involvement. Analyzing how these agencies have adapted their operations to use the intelligence cycle can provide insight into an effective forensic intelligence model.

Recommendations for the Development of a State or Local Forensic Intelligence Program

The magnitude of a forensic intelligence program may, at first, appear overwhelming. However, identification of the benefits, requirements, and challenges can support its implementation (see exhibit 3). Forensic intelligence programs can be created in a variety of sizes, scopes, and areas of responsibility. While a formal forensic intelligence program, coordinated by an intelligence unit in collaboration with a forensic science laboratory and investigative units, might be the most comprehensive example of fully utilizing the intelligence cycle, law enforcement has demonstrated that smaller, area-focused programs can provide immense value.

Exhibit 3. Forensic Intelligence Model Implementation Benefits, Requirements, and Challenges

Benefits	Requirements	Challenges
Transparent intelligence-led and data-driven policing	Dedicated staff	Lack of resources
Enhanced investigations and closure rates	Support of leadership	Lack of leadership or front-line buy-in
Improved interoperability and communication	Modern technology	Volume of data due to increasing crime
Increased public safety	Access to timely data	Interoperability and shared access to information

The impact that forensic intelligence initiatives can have on forensic science service providers is significant. Forensic laboratories operate in a "zero error" culture of accreditation according to international standards, which usually means that cases take significant time to complete; this kind of culture is often not compatible with efforts to use forensic results in the intelligence data stream. Too often, limited resources within crime laboratories are used to perform extra examinations in preparation for court proceedings, while other investigations may become backlogged or go "cold." Agencies that embrace forensic intelligence must acknowledge that a cultural shift is needed around the role of forensic science. Forensic science should be resourced to allow for probative evidence to be processed quickly enough to produce actionable intelligence that links crimes, identifies perpetrators of crime, absolves innocent persons from suspicion, and increases public safety. This is the mission of modern, data-driven, intelligence-led policing.

Examples of early efforts to change this culture can be seen mainly in the United States with the development of screening and processing for NIBIN shell casing correlations. Processing time in the network is measured in hours rather than months or years, as part of the minimum operating standards for sites required by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).[2] Similarly, organizations such as the Philadelphia Police Department are using Rapid DNA technology to augment their traditional CODIS laboratory techniques. Outside of the United States, Switzerland developed a rapid drug identification program that was validated and tested at the University of Lausanne and implemented by police in the canton of Neuchâtel to get drug results almost immediately for tracking the use and spread of illicit drugs. In each of these cases, forensic science has not minimized the objectivity, quality, or integrity of its examinations but acknowledges the incredible power that scientific data, when used responsibly, can add to intelligence, investigations, and public safety.

As the need for objective data expands in policing strategy, forensic laboratory service providers will need to evolve their reporting strategies to allow for the expanding role of intelligence-based testing protocols. These changes are now emerging, with forensic scientists, intelligence analysts, and investigators being trained on the appropriate use of forensic intelligence, including learning about both its capabilities and limitations. Agencies like the New Jersey State Police, Denver Police, and Philadelphia Police have shown that training, dedicated streamlined workflows, and process improvements that provide accurate and timely results allow forensic scientists, analysts, and investigators to maximize the use of forensic intelligence.

Experience within the United States and internationally has highlighted several essential elements that lead to successful forensic intelligence programs. Although not all elements are necessary to get started, they should all be considered and implemented to have the highest likelihood of success.

Organizational Structure

While forensic intelligence programs are collaborative partnerships between intelligence, forensic science, and investigative functions, they are best coordinated by an adequately resourced intelligence unit. Ideally, this unit would be within the primary law enforcement agency providing collaborative services, such as the police department's intelligence unit, a regional intelligence fusion center, or a state intelligence center. This is preferred because the primary law enforcement agency is the lead agency that has access to the various intelligence sources that make an intelligence program successful. In a large city, the primary agency is the local police department. In a state where there are many small, independent law enforcement agencies, state police may be more appropriate. It is also important to note that most forensic laboratories, investigative units, and intelligence units still reside in a law enforcement agency. Further, based on existing models of success within the U.S. intelligence community, the ideal location to produce intelligence is within an intelligence entity. Even within the CIA, the Directorate of Analysis serves as the central coordinating and production entity, working with the Directorate of Science and Technology and the Directorate of Operations.

The location of the forensic intelligence program depends on the number of agencies and laboratories involved and the scope of the intelligence effort. If possible, an agency should consider forming a forensic intelligence team within its intelligence unit whose members serve as the primary analysts for a forensic intelligence program. In some instances, a holistic forensic intelligence program may not be feasible — but elements of the timely use of forensic data for a targeted purpose can have an impact, as in Milwaukee's NIBIN/ Crime Gun Intelligence Center program. This approach can foster the development of an expanded forensic intelligence program as successes are realized.

The Philadelphia Police Department provides an example of a comprehensive forensic intelligence model for a self-sufficient major city. Maintaining the city's investigative, intelligence, and forensic responsibilities, the Philadelphia Police Department controls all features included in the intelligence cycle. Through the collaboration of the Office of Forensic Science and Intelligence Bureau, the department has implemented programmatic changes that include forensic laboratory workflow modifications, the release of forensic reports and leads, and timely transfer and use of these forensic data by the intelligence analysts to generate and disseminate intelligence products for the investigators. While this model is ideal for major city police departments, it is also scalable for smaller agencies that have primary control over all aspects of the intelligence cycle.

Depending on an agency's size, intelligence leadership may be at the executive level or lower in the organization (but still with the support of the executive level). Every successful model examined in this study had a command-level champion who also led the forensic intelligence effort, either through the forensic science or intelligence sections of their organization. These champions need to be strong leaders who can obtain staff buy-in to the changes that are required — from evolving the role of forensic science as an intelligence tool rather than a limited investigative tool, to collaborating across units and agencies on data, analysis, and products.

> ***While the comprehensive forensic intelligence model is ideal for major city police departments, it is also scalable for smaller agencies that have primary control over all aspects of the intelligence cycle.***

Academic partnerships may bring value to the forensic intelligence program. These partnerships may be useful for research and evaluation related to new capabilities, technology transfers, or formal program evaluations. This is especially true for forensic service providers and law enforcement agencies that do not have the resources to conduct independent research and program evaluations. This was best demonstrated by the Cuyahoga County, Ohio, program and their collaborations with Case Western Reserve University and by the Neuchâtel police in collaboration with the University of Lausanne.

Policies and Communication

Agency policies must be updated across forensic science, investigation, and intelligence operations to incorporate the needs of the forensic intelligence model. Forensic laboratories should encourage flexibility in data handling, whereby laboratory personnel can streamline data flow from laboratory information management systems to departmental records management and intelligence systems. Laboratories should also develop policies on when and how to report investigative leads and interact with investigators or the intelligence unit to maintain objectivity and minimize cognitive bias. Investigative units should develop policies that incorporate the use of forensic intelligence as a standard practice. Consideration should be given to establishing policies for monitoring and tracking follow-up activities related to investigative leads. Intelligence units should develop policies on the coordination and dissemination of forensic intelligence products to ensure the reliability and accuracy of the investigative leads.

Policies and procedures that govern a program's key components should be developed for continuity of operations. These components include training, data-sharing mechanisms, data types, analytic product templates, the review process, dissemination, and briefing.

> ***Policies and procedures that govern the key components of the forensic intelligence program should be developed for continuity of operations.***

Programs should develop feedback loops for all staff (including officers, investigators, analysts, and forensic scientists) to encourage engagement, create a team atmosphere, and monitor opportunities for improvement. Programs should consider establishing a primary point of contact in each forensic discipline for communications with the intelligence program personnel to maintain scientists' productivity, mitigate potential cognitive bias, facilitate data sharing, and expedite the review process. Communication policies on the dissemination of products should be created to ensure that appropriate staff members receive the products. Although agencies may need to maintain operational security on some products, agencies should avoid "siloed" dissemination to prevent missed opportunities.

Data and Technology

Having the right data and technology is vital to a successful forensic intelligence program. Although each part of the program has unique data and technology needs, consideration should also be given to the specific needs for sharing data, using technology tools, users, and products.

Forensic data need to be available in a timely manner to be useful for intelligence purposes. The ability of the forensic laboratory to shift its workflow practices and emphasize an intelligence-driven approach is key to the success of any forensic intelligence program. Memorandums of understanding should be established for sharing data between different agencies. These allow for the sustainability of data sharing regardless of personnel changes.

Establishing data-sharing methods, either manual or automated depending on the systems available, is critical. Certain databases and data-sharing opportunities may be confined by federal and state laws, but many of the collected data can be shared. Agencies need to understand their jurisdictions' laws regarding what data can be collected, how those data must be maintained, with whom they can be shared, and for what purposes.

While external vendors may play a role in developing initial data integration and interoperability processes, agencies should avoid any requirements that would necessitate vendor engagement for routine, day-to-day data integration processes or longer-term data storage needs. Whenever possible, agencies need to maintain ownership of, access to, and control of their data. Any vendor agreements on data storage or sharing platforms must cover the agency's inherent data rights and ownership.

The data types and means of collecting, storing, and managing the data will vary by forensic intelligence program, agency size, and crime problem focus, among other factors. When implementing forensic intelligence programs, personnel who understand the data needs of both forensic scientists and intelligence analysts should be involved in the discussions and implementation of technology tools.

Products and Dissemination

Intelligence products should be disseminated and briefed to the appropriate end users in a timely fashion to drive operations and support management-level decision-making. Forensic intelligence personnel should be aware of trend analysis and how it can be used as forensic intelligence with the ability to inform investigative personnel. Integration of multiple forms of intelligence in products can enable stronger analysis and conclusions. Forensic intelligence should be used in combination with other forms of intelligence, such as human and open-source intelligence, whenever possible. Procedures should be established for a product review process, including coordination with the appropriate laboratory supervisor for a technical review of any products using forensic data.

Training

A successful forensic intelligence program requires integration between a law enforcement agency's forensic science, intelligence, and investigative components. A collaborative training program that brings together intelligence analysts, forensic scientists, and investigators is one method for developing relationships between these components. This should include specific training for each component as well as cross-training and continued refresher training.

Analysts should receive training on the capabilities and limitations of forensic science, including an understanding of each forensic laboratory unit's capabilities, data sources, report formats, and methods for follow-up activities associated with the forensic data. Forensic scientists should be provided an overview of their role in the investigative process and the intelligence cycle with an understanding of how the data they produce can be used to enhance operations. Emphasis must be placed on when and how forensic scientists should interact with investigative and intelligence staff to maintain the safeguards set in place to prevent cognitive bias. Investigators should be trained on the capabilities and limitations of forensic data, the operational use of forensic data, and any follow-up actions required after being provided with forensic intelligence products.

Operations

Forensic intelligence should be incorporated into an overarching law enforcement intelligence operation. This provides access to additional data sources, analytic tools, and analytic training opportunities for the agency. A key component in the success of any program is collaboration between the intelligence, investigative, and forensic science units.

Forensic intelligence should be incorporated into an overarching law enforcement intelligence operation.

It is no coincidence that every forensic intelligence program reviewed during this study had a solid crime gun intelligence program. Milwaukee's forensic intelligence program, limited to crime gun intelligence, provides an example for many departments on where to start. The emphasis on crime gun intelligence and the strong partnerships between local law enforcement and ATF throughout the country may provide an ideal foundation for an agency interested in forensic intelligence. Establishing a crime gun intelligence program, which utilizes forensic intelligence, will provide the new user a template on which to expand into other areas of forensic intelligence as success is realized.

Resources

To adopt a forensic intelligence model that provides intelligence-led policing through data-driven policies, agencies must commit resources to these efforts. In addition to adequate staffing, essential resources include funding for the necessary technology, training, and time to develop policies, procedures, and partnerships. Agencies have taken various approaches to meeting these needs, mostly using existing resources, developing partnerships with federal agencies, and obtaining grant funds when possible.

Forensic laboratories should evaluate their analytical capacity with respect to the volume of requests for analysis. All parties should be informed of the laboratory's internal and external capabilities to allow for the best selection of examinations and analyses. If the laboratory's capacity is insufficient to provide timely and actionable intelligence, agencies should seek funding to enhance or expand its capacities. Enhancements may be made to facilities, staffing, instruments, technology, and outsourcing; however, agencies may consider process improvements and automation technologies to streamline workflows before investing in larger capital projects.

Intelligence units, or those carrying out analytical functions, should be evaluated for their analytical capacity and capability. Where capacity or capability is insufficient, enhancements, expansion, or partnerships may be considered. Investigative units also require an evaluation of their capacity, capabilities, and access to intelligence data. Where warranted, operational workflows may need to be improved or additional resources requested.

Framework

Exhibit 4 details the major components that are required to develop a forensic intelligence model. These components can be used to establish a performance matrix for evaluating the progress of forensic intelligence model development.

Exhibit 4. Forensic Intelligence Model Performance Matrix

Program Element	Evaluation Factors
Policies	Policies and procedures established for • Sharing data • Reviewing products • Communicating between intelligence and forensic science units • Feedback between intelligence, investigative, and forensic science units
Forensic laboratory workflow	Workflow changes implemented to produce timely data on • Firearms • Chemistry (e.g., drugs, toxicology) • DNA • Latent prints
Data sharing	• Establish the types of data that are available • Procedures for data transfer — manual or automated • Establish time frames for data-sharing routine: daily, weekly, monthly • Procedures for other data requests
Products	• Types of analytic products • Number of products • Impact of products
Dissemination methods	Methods used to disseminate forensic intelligence • Products • Alerts • Meetings • Conference calls
Training	• Presence of an internal training program • Number of trainings held • Number of personnel trained (intelligence, forensic science, and investigative personnel)
Resources	Staffing of • Forensic scientists • Intelligence analysts • Investigators • Analytic technology platforms specialists • Infrastructure (laboratory space, analyst workstations)

Comparison of Forensic Intelligence Programs

Operational Use of the Intelligence Cycle

Across the different forensic intelligence program models that were reviewed, the implementation of the intelligence cycle varies. See exhibit 5 for comparisons across the seven sites. Both the New Jersey State Police Regional Operations and Intelligence Center and the Philadelphia Police Department fully utilize the intelligence cycle, with the ability to collect and analyze various data sources into distributable, actionable intelligence in a timely manner. The New Jersey State Police Regional Operations and Intelligence Center manages its intelligence operations at a statewide level by coordinating the activities of multiple law enforcement agencies, forensic science laboratories, and public health organizations. The Philadelphia Police Department uses this model within the context of a major city department that maintains all the investigative, forensic, and intelligence activities for the city of Philadelphia, which allows for the collection of data and dissemination of intelligence by analysts to investigators.

New Jersey State Police

The New Jersey State Police coordinates forensic intelligence efforts across the state, handling 21 counties and 565 municipalities. The effort is led by the Regional Operations and Intelligence Center and supported by the New Jersey State Police Forensic and Technical Services Section as well as other independent county laboratories. The forensic section coordinates laboratory activities with the Regional Operations and Intelligence Center to meet the needs of the forensic intelligence program. This program demonstrates a strong cohesion between its different elements, which has been strengthened by the recent aligning of the New Jersey State Police's forensic and intelligence units under that same executive command structure.

The forensic intelligence is produced through structured intelligence operations within the New Jersey State Police Regional Operations and Intelligence Center, which is the state's fusion center. The Regional Operations and Intelligence Center has several sections that use forensic data in their intelligence production, including the Office of Drug Monitoring and Analysis (for its drug monitoring initiative) and the Information and Intelligence Bureau (for its NIBIN/Crime Gun Intelligence program and DNA program). The Regional

Exhibit 5. Comparison of Forensic Intelligence Models

Site	Planning and Direction	Forensic Data Collection	Processing, Analysis, and Production	Intelligence Dissemination
Cuyahoga County, Ohio	Tactical, case-specific requirements	Local and county law enforcement agencies, crime laboratory at medical examiner's office, public health partners	Cuyahoga County Prosecutor's Office intelligence analysts and Case Western Reserve University personnel	State and local law enforcement and public health departments
Denver Police Department (DPD)	Tactical, case-specific requirements	DPD Forensic Division	Investigators and Crime Gun Intelligence Center Task Force personnel; Denver Health Department	Field operations, public notification for drug findings
Milwaukee Police Department (MPD)	Tactical, case-specific requirements	Fusion Division/ Forensics Division	Crime Gun Intelligence Center personnel, MPD crime analysts	MPD supervisors/ investigators; local, state, regional, and national law enforcement partners
New Jersey State Police (NJSP)	Strategic, tactical, standing, and case-specific requirements	NJSP and county forensic laboratories	NJSP Regional Operations and Intelligence Center intelligence analysts	Regional, state, and national partners; local and state law enforcement for action
Philadelphia Police Department (PPD)	Strategic, tactical, standing, and case-specific requirements	PPD Office of Forensic Science	PPD Intelligence Bureau/Delaware Valley Intelligence Center intelligence analysts; Crime Gun Intelligence Center personnel	Executive team, command staff, investigators, regional/national partners
Australian Federal Police (AFP)	Strategic, tactical, standing, and case-specific requirements	Technical and forensic information collected from AFP Forensic Laboratory as well as state and territory forensic laboratories; forensic data are fused with other data sources using an all-source model	AFP forensic intelligence analysts	Broad dissemination to internal and external partners (forensics, intelligence, investigations, executive)
Neuchâtel Police Department	Tactical, case-specific requirements	Neuchâtel Police Department's Forensic Science and Crime Intelligence Division	Forensic investigators	Cantonal police commanders and investigators, regional partners

Operations and Intelligence Center has developed partnerships with other New Jersey State Police units as well as law enforcement and public health organizations across federal, state, and local organizations to collect the necessary data for intelligence analysis. It has also standardized statewide data collection and data-sharing methods for firearms, DNA, and drugs. As an example, the Office of Drug Monitoring and Analysis established relationships with forensic laboratories across the state to receive drug chemistry analysis in support of its drug monitoring initiative. The office is currently in the process of deploying an automated system that receives the drug data and allows for data cleaning, quality control, advanced analytics, and visualization of the intelligence. The Regional Operations and Intelligence Center produces both strategic and tactical intelligence products that include daily, weekly, monthly, quarterly, and yearly trend analyses as well as analysis of emerging trends and threats.

Further, dissemination of the intelligence is a key component of this program; the Regional Operations and Intelligence Center not only releases products but also hosts regional, statewide, and national conference calls and training courses and provides outreach. Of note, the Regional Operations and Intelligence Center's Information and Intelligence Bureau uses its three regional real-time crime centers, which support the north, central, and south regions of the state, for dissemination of intelligence from the bureau's statewide NIBIN program. Analysts within the real-time crime centers work as a team to develop and distribute tactical forensic intelligence products using the NIBIN hit data in support of identifying and arresting people responsible for criminal activity within the regional areas and statewide. Many law enforcement agencies across the United States have adopted a real-time crime center model for the distribution of information, intelligence, and tactical support.

A major challenge overcome by the Regional Operations and Intelligence Center was implementing its programs statewide. At the state level, the Regional Operations and Intelligence Center receives forensic data from New Jersey State Police forensic science laboratories as well as through partnerships with the independent county forensic science laboratories. The diverse collection sources that feed forensic information to the center present a challenge that a multiagency system must address. Therefore, any forensic intelligence effort that supports multiple collection sites must broker strong and collaborative agreements to emphasize the importance of data collection and reporting timeliness from all partners.

The New Jersey State Police provides a strong example of a comprehensive forensic intelligence program that fully utilizes the intelligence cycle to coordinate activities across multiple jurisdictions, integrating and analyzing data to release actionable intelligence. The in-house capabilities of the regional fusion center and partnership with the state's forensic laboratories and other agencies provide the New Jersey State Police with the critical elements — intelligence analysts, technology, data sources, and federal, state, and local partners — for establishing a robust program (see exhibit 4 for model program elements).

Philadelphia Police Department

The Philadelphia Police Department developed a comprehensive Technical Intelligence Program that includes a crime gun intelligence center (NIBIN program), firearms trends, drug intelligence, DNA analysis (e.g., genetic genealogy, Rapid DNA), and computer forensics/digital media evidence, as well as the integration of other key forensic data into intelligence operations. The department's Office of Forensic Science provides the results of forensic analyses and database queries to the department's Intelligence Bureau for tactical and strategic intelligence products. These products incorporate not only forensic data but also multiple intelligence sources when applicable.

> ***Any forensic intelligence effort that supports multiple collection sites must broker strong and collaborative agreements to emphasize the importance of data collection and reporting timeliness from all partners.***

All products involving forensic intelligence are subjected to a practice, common in the intelligence community, known as coordination. Before dissemination, each product is reviewed for technical accuracy by the appropriate forensic laboratory manager. This process preserves the integrity of the intelligence product from potential bias on the part of individual forensic scientists. Intelligence products are disseminated and briefed to all end users, from executives to investigators. The products have become a standard resource for the Philadelphia Police Department's detectives and command staff, as well as a staple in COMPSTAT and Weekly Shooting Review meetings.

Additionally, the Philadelphia Police Department collaborates with ATF for its crime gun intelligence center, the FBI for its regional computer forensic laboratory, and public health sources for drug intelligence. Of note, the department's in-house Intelligence Bureau also maintains the Delaware Valley Intelligence Center, the regional fusion center for the Philadelphia metropolitan area. Like New Jersey's Regional Operations and Intelligence Center, the Philadelphia Police Department uses a fusion center model within the context of the fourth-largest police department in the nation, serving the sixth-largest U.S. city. The department maintains all the investigative, forensic, and intelligence activities for the City of Philadelphia, which allows for the systematic control of all collection, analysis, and dissemination of intelligence. The department's executive leadership allows this model to be successful; the forensic, investigative, and intelligence executives collaborate on daily case analytic requirements, department data and access interoperability, and longer-term programs to support the use of forensic science data in intelligence operations. While the department has initiated a comprehensive approach to forensic intelligence, it continues to explore the expansion of these capabilities through staffing increases and improvements to interoperable technology systems.

Denver Police Department

Although the Denver Police Department does not use a fusion center or intelligence unit model, it has created well-functioning forensic intelligence programs with its available units. These programs include the Expedited DNA and Latent Print Database Investigative Lead programs, the Fentanyl Monitoring System, and the NIBIN/Crime Gun Intelligence Center Regional Anti-Violence Enforcement Network task force. The intelligence production is driven by the forensic laboratory through crime gun intelligence center operations with the Regional Anti-Violence Enforcement Network task force and in collaboration with public health organizations for drug interdiction programs. Unlike the other sites studied, there are no crime analysts directly involved with Denver's forensic intelligence efforts; analytic work is performed by crime laboratory statistical staff in collaboration with the task force, investigators, and public health personnel.

In Denver, a close working relationship between the police department's Major Crimes Division and Forensics and Evidence Division accomplishes the coordination of forensics operations with investigations. As in Philadelphia, Denver crime laboratory leadership provides data to the intelligence and investigative divisions, facilitating rapid understanding of the meaning of the data and any important links that exist. Laboratory statistical analysts send data to investigators weekly in reports that have evolved into real-time mapping functions. Coupled with existing case follow-up policies, these reports put forensic science at the front end of investigations instead of being used much later in investigations, as is the case in many cities.

Both Philadelphia and Denver demonstrate models for major cities. Each features a full-service forensic science provider in which the forensic intelligence efforts align scientific activities with the intelligence and investigations they support through the executive forensic science leadership.

Timely scientific testing is critical to the success of any forensic intelligence program. Several of the model programs studied in this report worked diligently to streamline data from their laboratory information management systems to allow statistical analyses and further intelligence product development.

As laboratories generate results in a timely manner or change procedures to allow presumptive or intelligence-driven leads, investigative personnel are increasingly expected to apply this intelligence in an equally timely way. In response to cold case CODIS matches accumulating in Denver, the Denver Police Department changed its policy to require a 24-hour evaluation of any forensic database matches (to people) for all DNA/CODIS and fingerprint results from the Automated Fingerprint Identification System (AFIS). This ensures that the value of the forensic science results to the investigation is not lost over time. This policy has changed how cases are assigned to detectives across the police department, with cases being investigated by teams instead of a single detective. As the use of forensic data becomes more common with intelligence-driven policing programs, forensic laboratories need to evaluate their operations to ensure timely results while maintaining the levels of quality expected from the forensic sciences. Equally, investigative and intelligence units need to verify that the forensic science results are useful and communicated effectively to maximize impact.

Denver's program shows that an agency can implement a functional forensic intelligence program with existing forensic and investigative staff in collaboration with partners. Although including intelligence analysts or an intelligence unit would more completely address the intelligence cycle and make more comprehensive intelligence packages possible, the leadership of Denver's forensic laboratory and collaboration with partners provide the foundation for this program's success. Without this program, the Denver Police Department would be missing investigative leads. The program's success illustrates the scalable nature of forensic intelligence programs.

It must be noted, however, that Denver's model may be less successful for a law enforcement agency that does not have its own forensic science laboratory or does not resource its forensic science laboratory as a critical component of its organizational and command structure. Additionally, without an integrated department intelligence unit, this program's success will continue to be limited to the intelligence data available to the laboratory, crime gun intelligence center, and public health partners.

Both Philadelphia and Denver demonstrate models for major cities. Each features a full-service forensic science provider in which the forensic intelligence efforts align scientific activities with the intelligence and investigations they support through the executive forensic science leadership. Similar to how the CIA benefits from its Directorate of Science and

Technology, law enforcement agencies like the Philadelphia and Denver Police Departments that have existing forensic science laboratories as part of their organizations benefit from the internal expertise and direct source of scientific data. Both the Philadelphia and Denver laboratories produce forensic science results in coordination with their police departments' investigative and intelligence personnel. In both cases, forensic laboratory executives have coordinated changes in processing workflows, data structure, and data flow to ensure that technical results are provided in a timely manner, which is central to the agencies' use of forensic intelligence as actionable intelligence. In Philadelphia, the forensic, investigative, and intelligence executives collaborate on daily case analytic requirements, department data and access interoperability, and longer-term programs to support the use of forensic science data in intelligence operations. Similarly, in Denver, forensic laboratory leadership is driving changes in the laboratory information management system and the police department's records management system to allow rapid data storage, access, and analysis in near real time using widely available databasing tools and visualization software. In both cases, forensic science data are provided to downstream consumers such as intelligence analysts, criminal investigators, and field task forces that further refine the data for intelligence use. Without enough *collection* capabilities, it is impossible to produce forensic intelligence-driven products that combine forensic data with other demographic data — such as people involved, automated license plate reader information, addresses, and case narratives — into intelligence packets or reports that are sent to investigators.

Milwaukee Police Department

In contrast with the New Jersey, Philadelphia, and Denver programs, the forensic intelligence program in the Milwaukee Police Department consists solely of a crime gun intelligence center using NIBIN correlations. The crime gun intelligence center, a collaboration between the Milwaukee Police Department's crime analysts and investigators and ATF personnel, produces mainly tactical products to support operations. These tactical products allow the investigators to link people, places, and weapons to multiple incidents. In addition to disseminating intelligence products regionally, the collaborations include a series of meetings for sharing data and discussing the path forward on cases. Further, the Milwaukee Police Department has created an internal database to track all NIBIN hits and link cases. This program uses the intelligence cycle for one type of forensic science data, NIBIN correlations, which are generated, collected, and analyzed within the fusion division of the Milwaukee Police Department. The Milwaukee program represents one aspect of a forensic intelligence model focused on crime guns; such a model has been discussed by ATF's National Crime Gun Intelligence Governing Board, the National Institute of Justice, and the Bureau of Justice Assistance.[3] The Milwaukee Police Department has a forensic crime laboratory where forensic analysis such as testing drug chemistry and extracting DNA and latent prints from evidence is conducted. DNA is not further analyzed by the department but is sent to the state crime laboratory for further analysis and comparison. The forensics division is a step in the department's forensic intelligence model.

Cuyahoga County

Cuyahoga County, Ohio, represents a unique situation in that its forensic intelligence effort is managed through the Crime Strategies Unit of the county prosecutor's office and the county medical examiner, in conjunction with the Begun Center at Case Western Reserve University. Specifically, the Cuyahoga County forensic intelligence efforts include a sexual assault kit task force, crime strategies unit/crime gun intelligence center, and heroin/opioid overdose initiatives.[4] All of these programs have collaborators from other entities, including federal, state, and local law enforcement; public health agencies; and academia. Although the efforts are not managed by an in-house forensic science provider, they are coordinated with regional and state laboratories. All the forensic intelligence work occurs at the county level, where the county prosecutor gathers data from across 59 municipalities. Forensic laboratory services are an important part of the work but are not involved in the management or coordination of forensic intelligence efforts. Timely forensic science results are sourced from local law enforcement agencies' NIBIN results, toxicology testing from the county board of health/medical examiner, and the county crime laboratory operated by the medical examiner's office. The products that are generated are both tactical and strategic, depending on the program. The prosecutor's office also hosts and participates in meetings and conference calls with partners to aid in information sharing and the prioritization of, and follow-up on, cases.

Of note, data collection is a challenge in Cuyahoga County because the lead agencies are not law enforcement agencies and are not grouped within a single organization. This difficulty demonstrates the need for data-sharing memorandums of understanding, where applicable, to obtain and sustain data access for effective intelligence use. Challenges for a prosecutorial forensic intelligence program may include the lack of direct data access, disconnects between prosecutorial staff and investigative staff, perceptions of bias if intelligence requirements are drafted after prosecutorial theories are developed, and potential delays in incorporating forensic intelligence results into policing strategies such as patrol assignments and preventive policing efforts.

Due to the organizational structure of its program, which generates products primarily from the prosecutor's office, Cuyahoga County can implement specific projects that use a modified intelligence cycle. Although these projects have an impact, the framework may lack the ability to expand into a comprehensive forensic intelligence program due to the disconnect between law enforcement investigations, intelligence analysts, and end users. However, the success of Cuyahoga County's individual program areas shows the utility of forensic intelligence and establishes a foundation for the larger efforts needed to create a comprehensive forensic intelligence program.

Neuchâtel Police

The international sites in Switzerland and Australia have different organizational structures than those adopted by the U.S. state and local law enforcement agencies, but their operations demonstrate comprehensive use of the intelligence cycle.

In Switzerland, the Neuchâtel Police's Forensic Science and Crime Intelligence Division integrates forensic science and intelligence operations at the cantonal law enforcement level (analogous to state-level law enforcement in the United States). The forensic programs within the Neuchâtel Police include footwear analysis, latent prints, questioned documents, and cyber investigations. Personnel within this division collect physical evidence at crime scenes and produce intelligence analysis. Most of the personnel are generalists, but some have specialties developed at the undergraduate or graduate level in the School of Criminal Justice at the University of Lausanne. The analysis produced within the Neuchâtel Police is mainly tactical, relating to specific investigations and crime series. The police department actively shares forensic intelligence and further intelligence with neighboring states' police forces through the regional intelligence fusion center, which maintains a dedicated interstate intelligence system. The collaboration with the University of Lausanne provides more strategic types of analysis as well as the development of technology, such as regional databases and fieldable technology to support operations. Participation of the police Forensic Science and Crime Intelligence Division in the weekly operational meetings allows the police department to utilize forensic intelligence in operational planning.

Australian Federal Police

The forensic intelligence program of the Australian Federal Police — the only program with federal jurisdiction reviewed — includes weapons technologies intelligence (identification and classification of improvised explosive devices and chemical, biological, radiological, and nuclear weapons), forensic drug intelligence, illicit firearm types and classes, biometric technologies, DNA and fingerprints, ballistics, documents and counterfeiting, digital evidence, and geospatial intelligence. Further, the intelligence division coordinates many types of information, such as forensic evidence, human intelligence, signals intelligence, open-source intelligence, and imagery-based intelligence.

The forensic disciplines covered are more indicative of a federal program that covers traditional crime as well as national security issues. The Australian Federal Police's forensic intelligence program has established an intelligence unit within the agency's forensic science laboratory, where scientists are trained to be intelligence analysts. They produce strategic assessments using forensic data as well as intelligence bulletins and tactical intelligence to support criminal investigations.

The Australian model requires federal services to be provided from local or provincial police forces, and the federal police coordinate complex investigations cross-jurisdictionally. The major challenge of this model has been data collection at a national level; the Australian Federal Police is in the process of developing data collection standards and databases to overcome this issue. Although this model has worked for federal law enforcement in Australia, it is likely not the best model for U.S. state and local operations for multiple reasons, including personnel and technology resources and the pace of state and local operations.

Training

A component common to most of the forensic intelligence models reviewed is an internal training program. Denver, Philadelphia, New Jersey, Neuchâtel, and Australia all have internal training programs, not only to educate forensic, investigative, and analytical personnel but also to assist with coordinating the forensic intelligence efforts. Training is, in addition, a way of obtaining buy-in for using the intelligence by demonstrating its value to, and impact on, operations. The Denver Police Department provides all investigators with training on the use of forensic intelligence and monitors the timely and proper use of intelligence. The Philadelphia Police Department trains forensic science, intelligence, and investigative personnel on the types and operational uses of forensic data. As a state agency, the New Jersey State Police Regional Operations and Intelligence Center provides outreach and training to law enforcement statewide through courses on the uses and benefits of forensic intelligence. The Australian Federal Police provides training courses for forensic personnel and law enforcement to aid in the success of its forensic intelligence program. In all these cases, training is provided not only to current personnel but also to new recruits, as this is key to sustaining the use of intelligence in law enforcement operations.

Data and Technology

From the basic use of forensic data to investigate and target specific types of patterns, crimes, and individuals, forensic intelligence models enhance these capabilities to include a more sophisticated analysis of forensic data in combination with other sources of intelligence to generate finished products for both tactical and strategic purposes. Many of the seven study sites have developed databases and data tools to handle the processing and analysis of forensic science data in combination with other data types typical of intelligence units. Traditionally, forensic science was used to aid a specific investigation or court case; however, the development of forensic databases has widened the applications for forensic data. For example, the success of DNA analysis and the ability to link serial cases, such as sexual assaults, have led to generally accepted policies across the United States to “test all” sexual assault evidence kits (whether a suspect is known or unknown). Likewise, most of the forensic intelligence programs examined originated in response to specific problems, such as increased gun violence in Milwaukee, New Jersey, Cleveland, Denver, and Philadelphia.

The data that are vital to forensic intelligence models vary depending on the crime and program. For all crime types, the criminal case itself, and other intelligence attached to the case and the suspects, it is critical to be able to connect to the additional forensic data that are collected and developed. For example, gun violence efforts include tracing information on firearms, shell casings and bullets, gunshot detection system hits, DNA profiles, and fingerprints. Sexual assault programs focus on the DNA collected through sexual assault kits and subsequent DNA matches. Critical drug-related data include the chemical identification and toxicology analysis of controlled substances and overdose events. While the sites studied in the United States are primarily focused on violent crime and drugs, some programs, such as in Philadelphia, also maintain questioned documents databases for crimes such as bank robbery and deed forgeries. It is also common for DNA and latent print data to establish criminal patterns that can be used for property crimes and other nonviolent offenses. However, the inclusion of nonviolent crime data was more common within the international sites. Switzerland has a robust forensic intelligence model for property crimes, as does Australia for forgery and cybercrime. The additional data incorporated in these models include tire tread and footwear marks, digital information from electronic devices such as computers and cell phones, and questioned documents.

Data sources common to all the forensic intelligence sites studied are the laboratory information management systems used in forensic laboratories and the records management systems used by law enforcement agencies to track crime, arrest, and property/evidence reports. In the United States, there are separate technologies for specific types of databases: CODIS for DNA, AFIS for latent prints, NIBIN for firearms, and other technologies, such as gunshot acoustic detection systems and digital evidence databases. In addition to these, technology varies across the different sites based on the participating agencies, the specific crimes that are focused on, and whether the programs are local, state, or federal (see exhibit 6).

Exhibit 6: Common Technologies in Law Enforcement Agencies

Technology	Purpose
Laboratory Information Management System	Stores data related to cases that are received and processed by the forensic laboratory
Records Management System	Stores crime, arrest, traffic, property/evidence, and other data collected by patrol and investigations
Computer-Aided Dispatch	Stores call and response data, both by the community and officers
Intelligence Database	Stores information collected about activities occurring with specific people, places, and things and the reliability of the sources
Web-Based Dashboard	Provides a means to analyze and visualize data and information from a variety of sources
Geographic Information System	Provides a means to map and spatially analyze data from a variety of sources

In addition to the technology used to store data, several tools are commonly used to conduct analysis, develop products, and communicate to users and the public. These include spreadsheets (both simple and more complex) and databases for data storage, manipulation, and analysis. Some of the most common analytic tools include geographic information systems, social network analysis, link analysis, and digital media evidence analytic platforms. Lastly, several sites have created interactive, web-based "dashboards" to allow users to easily share data and trends, in addition to typical tools such as Adobe PDF and Microsoft PowerPoint for sharing information and reports. The primary problem identified by every site is interoperability; siloed information can make intelligence analysis more manual, problematic, and time-consuming, or even impossible.

The sites in Denver, Philadelphia, and New Jersey are making efforts to change data flow from laboratory information management systems into broader data management initiatives within their respective police agencies. Recent upgrades to the records management system in Philadelphia allow automatic access and data transfers between the records management system and the laboratory information management system, which are intended to improve the effectiveness and efficiency of the forensic intelligence program by importing data into the intelligence analysis platforms used by analysts. The Denver Crime Laboratory has changed all database match reporting to allow geolocations and case-linked demographic information to be viewed in real time at the police department's real-time crime information center. These efforts record criminal activities and the people linked to specific crimes and locations, allowing investigative leads to be derived more quickly. Older systems relied on inefficient case-by-case reviews to access similar information.

As resources become available and forensic intelligence models advance their use of technology, web-based dashboards that collect, process, analyze, and provide visualization of the intelligence will become more widely used. Several of the sites studied are using web-based dashboards to share data and information across partners and with the public. In Denver, the forensic laboratory has enhanced existing platforms with custom programming to easily compile and analyze forensic data. Intelligence products are created by and for investigators. The Regional Operations and Intelligence Center in New Jersey has purchased a platform from a company that automatically receives and cleans various data, then performs advanced analysis and visualization of the intelligence. Platforms have been developed for both New Jersey's Office of Drug Monitoring and Analysis and its NIBIN/ Crime Gun Intelligence Center program. These systems have access to multiple data sources in addition to forensic science data. As forensic intelligence programs obtain access to more advanced technology platforms that handle the collection, processing, analysis, and dissemination of data, these programs' use of the intelligence cycle will become a more automated and continuous process.

Challenges for Implementing a Forensic Intelligence Model

A major challenge from an intelligence perspective revolves around access to data and technology. Many agencies have multiple data platforms that were developed as stand-alone systems, making data integration difficult. Specifically, most laboratory information management systems were established for collecting case information, not for intelligence purposes. These systems were traditionally created to track laboratory processes and results for individual cases. However, forensic intelligence requires the ability to assess patterns and trends within the forensic data, and to combine the results with data from other sources. This mismatch between the capabilities of existing laboratory information management systems and the needs of forensic intelligence programs probably represents the largest impediment to the intelligence process, as accessing data in an efficient and timely manner is key to that process. All the programs studied began with the manual collection of forensic data; they are slowly overcoming the lack of automation in data sharing and analysis as agencies obtain the technology needed to access and analyze the data in a more real-time fashion.

For regional, state, and national programs, data integration problems may be compounded by political, jurisdictional, or logistical restrictions. For example, crime gun intelligence programs have historically been hampered by the inability to easily digest eTrace or NIBIN results from proprietary software programs; local agencies have had to capture these results manually within their own systems. However, enhanced partnerships with ATF through crime gun intelligence centers and the development of the ATF NIBIN Enforcement Support System — an intelligence tool for analyzing crime gun and NIBIN linkages — are making this process easier for local forensic intelligence programs.

Interoperability is also an issue between local organizations. In some cases, intelligence activities have been inhibited by an inability to share data across multiple organizations. For example, Cuyahoga County has experienced data access issues because the lead agencies in its forensic intelligence program are not law enforcement agencies and are not within one organization. In these situations, the lead forensic intelligence organization and partner agencies should establish working groups to review data systems and develop feasible technology solutions for data sharing. Administrative and jurisdictional impediments can often be solved through well-defined data-sharing memorandums of understanding between the partner agencies.

About the Authors

Tara Garvey

Tara Garvey is currently a deputy director within the Philadelphia Police Department Intelligence Bureau, supporting the chief inspector in the development of policies, procedures, and operations. She previously served as the deputy director of the Delaware Valley Intelligence Center, where she managed daily operations to include the development of all analytical products and collaborations with other agencies. She has been with the Philadelphia Police Department since January 2013. Garvey is a graduate of Rutgers University and The George Washington University, where she received a doctorate in genetics through a joint program with the National Institutes of Health (NIH). She completed an NIH postdoctoral fellowship at the National Institute of Allergy and Infectious Diseases. From there, she worked as a biotechnology patent examiner at the United States Patent and Trademark Office. Garvey then joined the Central Intelligence Agency, where she originally worked in the Directorate of Science and Technology as a technical intelligence officer, supporting various operations, intelligence analyses, and research and development projects that included an assignment working with In-Q-Tel. Based on her extensive technical knowledge and ability to develop practical solutions, she had the opportunity to further expand her operational expertise by working as a special skills officer in the Counterproliferation Center of the National Clandestine Service.

Greggory LaBerge

Greggory LaBerge has been the director of the Denver Police Department Forensics and Evidence Division since 2005 and has worked for the Denver Police Department since 1996, with specializations in management, crime scene investigations, forensic intelligence implementation, statistics, and forensic genetics. He has provided support to the forensic and broader scientific communities through NIJ-funded research and teaching in the United States and internationally in collaboration with the U.S. Department of State. LaBerge has served on several local, state, and federal committees and boards related to forensic science and medical genetics, and has served on the Colorado Dental Board. He has completed post-doctoral work in cancer genetics through collaborations at Yale University, and he teaches and conducts research at the University of Colorado School of

Medicine as an adjunct professor in the Pediatrics Department. LaBerge holds a bachelor of science degree in molecular biology and genetics from the University of Guelph in Ontario, Canada; a master of science degree in biostatistics; and a doctorate in human medical genetics from the Anschutz Medical Campus at the University of Colorado.

Julie Wartell

Julie Wartell has spent over 25 years working with local, state, and federal criminal justice agencies and communities around crime analysis, research, and prevention, including serving as a crime analyst for police and prosecution, managing a regional crime mapping initiative, conducting research and evaluation for nonprofits, serving as an NIJ fellow, and serving as an independent advisor. Wartell has performed a wide range of research and analysis of crime problems, conducted studies of police and prosecutor processes, and assessed information technologies. She has conducted extensive training and presentations to officers, prosecutors, analysts, and the international community on topics related to analyzing crime and problem solving. Wartell has edited or authored numerous publications and teaches and conducts research at the University of California, San Diego. She holds a master's degree in public administration from San Diego State University and a postgraduate diploma in applied criminology and police management from the University of Cambridge, England.

Endnotes

1. Global Justice Information Sharing Initiative, *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States: Findings and Recommendations,* Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance, October 2007, https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other.

2. Bureau of Alcohol, Tobacco, Firearms and Explosives, "Minimum Required Operating Standards for National Integrated Ballistic Information Network (NIBIN) Sites," Washington, DC: U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, July 2018, https://www.atf.gov/firearms/docs/undefined/mrosnibinsitesauditstandardspdf.

3. National Crime Gun Intelligence Governing Board, *Crime Gun Intelligence: An Evidence-Based Approach to Solving Violent Crime,* Washington, DC: U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, 2020, https://crimegunintelcenters.org/wp-content/uploads/2021/04/CGI-Best-Practices-Handbook-2020.pdf; Crime Gun Intelligence Centers, "CGIC Concept," https://crimegunintelcenters.org/cgic-concept/; and Police Foundation, "Five Things You Need To Know About Crime Gun Intelligence Centers," https://crimegunintelcenters.org/wp-content/uploads/2017/12/5-THINGS-to-Know-About-Crime-Gun-Intelligence-Centers.pdf.

4. Numerous publications have been generated from this work and can be found at https://case.edu/socialwork/begun/resources/publications.