NEW JERSEY STATE POLICE

Practical Guide to
INTELLIGENCE-LED POLICING

CPT
CENTER FOR POLICING TERRORISM
AT THE MANHATTAN INSTITUTE

HARBINGER

Colonel Joseph R. Fuentes
Superintendent
New Jersey State Police

September 2006

CPT
CENTER FOR POLICING TERRORISM
AT THE MANHATTAN INSTITUTE

The *New Jersey State Police Practical Guide to Intelligence-Led Policing* provides an example of the fundamental processes that state and local law enforcement are adopting to operationalize Intelligence-Led Policing (ILP). The Manhattan Institute is distributing this guide to political and public safety leaders to help foster a common understanding of the concepts and methods for adopting intelligence as the foundation of law enforcement operations and sound decision-making.

The *Guide* is a reference document for officers on patrol, detectives in the field, analysts, and senior leadership. It acknowledges that the primary responsibility of state and local police organizations is to *prevent* crime and terrorism. The starting point for First Preventers is to leverage an intelligence apparatus that communicates clearly, shares information broadly, and focuses resources according to a commander's intent.

We thank the New Jersey State Police for the opportunity to bring the Manhattan Institute's resources to bear in developing this practical application of ILP theory. The *Guide*, which is one of many positive benefits achieved as a result of this partnership, reflects the NJSP's vision for how policing will be done in the Information Age. We especially recognize the support and professionalism of Superintendent Joseph R. Fuentes, Lieutenant Colonel Frank Rodgers, Detective Sergeant First Class Ray Guidetti, Detective I Greg Demeter, and analysts Dean Baratta and Justin Wagner. We also express our appreciation for the immense contributions of Dr. Jerry Ratcliffe of Temple University, whose intellectual work fueled this effort.

In addition, this *Guide* would not have been possible without dedicated support from several key supporters, chief among them the leadership at Harbinger/ICx Technologies and Mr. Marty Gross.

Our heartfelt appreciation to you all.

Sincerely,

Timothy P. Connors
Director, Center for Policing Terrorism
tconnors@manhattan-institute.org

J. Michael Barrett
Harbinger/ICx Technologies
Fellow in Homeland Security
mbarrett@manhattan-institute.org

The Project Committee to Integrate Intelligence-led Policing Within the New Jersey State Police

September 26, 2006

Ray Guidetti
Detective Sergeant First Class

Greg Demeter
Detective I

Dean Baratta
Analyst

Justin Wagner
Analyst

Frank E. Rodgers
Lieutenant Colonel
Deputy Superintendent of Investigations
New Jersey State Police

J. Michael Barrett
Research Fellow
Harbinger/ICx Technologies
Manhattan Institute

Gerard LaSalle, Ph.D.
Professor
East Stroudsburg University

John Rollins, J.D.
Researcher
Center for Homeland Defense and
Security Naval Postgraduate School

To our Readers:

Five years ago, our nation was violently attacked and thousands of innocent Americans died at the hands of international terrorists. A third of those victims resided in New Jersey, reminding us that terrorism is truly a local issue. Moreover, eleven of the nineteen hijackers spent time in New Jersey planning and executing the dreadful assault on America. Their presence here illuminates an existing vulnerability in our free society - terrorists are capable of carrying out attacks from our backyards. This alarming discovery has thrust policing into a new era, an era that requires police organizations to manage risk more effectively and efficiently. For the State Police, policing in the Homeland Security Era has involved significant architectural and process changes.

A year ago, the Deputy Superintendent of Investigations commissioned a project to design and produce a manual to guide intelligence operations within the State Police. At the time, the Investigations Branch was undergoing a wholesale transformation to increase its efficiency and effectiveness of operations. Central to the Branch's reorganization was elevating the stature of the intelligence function. Prior to the reorganization only select members of the Branch were responsible for collecting and sharing intelligence. After the reorganization, all Branch members would bear this vital and essential duty. As the reorganization project evolved, so did the intelligence manual project. The final report before you is the culmination of a year's work and a great deal of collaboration among a team of dedicated professionals. It reveals a document that has expanded from its original design and now focuses on the intelligence-led policing construct currently being integrated within the State Police to create a mission capable force in an "all crimes, all hazards, and all threat" environment.

The NJSP Practical Guide to Intelligence-led Policing was born from the Superintendent's mandate that in order to secure our homeland and sustain our hometown way of life we must revolutionize the manner in which we police. We deliver this report in response to this mandate. We certainly expect it will challenge the status quo of how policing is performed within the State Police.

Following this roadmap to change, impelled by a sense of urgency to prevent the next terrorist attack or respond to the next man-made or natural disaster, the State Police has adopted a paradigm of policing aimed at interpreting the environment we police. The 3i Model of intelligence-led policing, crafted by the renowned Dr. Jerry Ratcliffe of Temple University, has provided us with the philosophical foundation needed to anchor policy and strategy. Over the past year, Dr. Ratcliffe has repeatedly provided his expertise in order to assist us in preparing this reference guide. We are grateful for his interest and enthusiasm in this revolutionary State Police project.

Applying the precepts of intelligence-led policing within our long established legal framework designed to guarantee our civil liberties requires a delicate balance between security and liberty. We are especially thankful to Deputy Attorney General Dave Rebuck of the New Jersey Attorney General's Office for his attention to detail needed to ensure we did not "push the envelope" with our application of the intelligence report. His guidance was reverberated in the advice of Jim Wilson and the team at the Institute for Intergovernmental Research (IIR). Having the endorsement from this true group of professionals on the intelligence report chapter will assist us in maintaining the true value of intelligence collection without corroding the same liberties we are empowered to defend.

Achieving proficiency in intelligence-led policing requires specific process changes to "operationalize" philosophy. We are indebted to the Manhattan Institute Center for Policing Terrorism for helping us work toward and realize this overarching goal. Director Tim Connors has been instrumental in providing subject matter experts that our team could consult concerning policy, strategy, and the operations of intelligence. The wisdom of Harbinger/ICx Technologies Research Fellow J. Michael Barrett is woven through the pages of this guide. His professionalism, wit, and overall dedication to the project – underscored by his notion that securing America requires distinct process changes – have served to reorient our bearing on many instances. We will always consider him part of our team.

It is true that the State Police cannot achieve the paradigm of intelligence-led policing without a robust analytical workforce. Today we continue to work toward this end and are forever grateful for the insights and acumen of Marilyn Peterson. Working in cooperation with our team she has supplied our analysts with the training requisite of a professional analytical apparatus. Her curricula will perpetually counsel our next generation of analysts in the skill sets needed to achieve success in this domain. As one of the nation's leading voices on intelligence analysis, we are indebted to her counsel.

This monograph is a practical guide primarily concerned with the principles that generate policy, both current and future, regarding the way the State Police interprets intelligence-led policing. It is intended to challenge its readers to come to terms with intelligence-led policing. Contained throughout this guide is a host of references deliberately placed to supply the basic vocabulary of intelligence-led policing. Once a language is standardized and a baseline familiarity is attained, our efforts to achieve strategy will be maximized. It is then that our leadership can focus their attention on the forces that help and hinder efforts to achieve the State Police's overall intelligence-led policing strategy.

Practical guides come in two types. Some are a presentation of rules; others deal largely with the principles that underlie such rules. This guide follows the latter. As such, it requires action by the reader to be effective. In other words, this guide addresses the many problems inherent to policing in the Homeland Security Era and provides the reader with the principles for solving such problems. However, the problems to be solved are practical and require action at the level of the individual. It is our hope that the knowledge conveyed in this guide will engender action in the form of creating policy, strategy, training, and operations needed to solve the practical problems of policing in the new era.

We complete our project with a great sense of accomplishment. We thank those who have contributed to it over the last year and provided the crucial insight necessary for such a mass undertaking. We are certain that we will be a better policing organization for it. Most importantly, this month is the anniversary of the September 11, 2001 terrorist attacks. It serves as a reminder of why we cannot ever waver in our resolve to defend America through effective policing.

Ray Guidetti
Detective Sergeant First Class
New Jersey State Police

Table of Contents

FOREWORD

This *New Jersey State Police (NJSP) Practical Guide to Intelligence-led Policing* details the processes that the NJSP has adopted in order to operationalize the principles of Intelligence-led Policing (ILP). It was written to ensure that all members of the NJSP share the same understanding of the concepts and vernacular that we have embraced to institutionalize intelligence as the foundation of all operations. The need for this guide was born from the understanding that before any law enforcement organization can benefit from the use of intelligence its members must truly understand the fundamental concepts linked to the application of intelligence and ILP. In essence, this guide is a reference for the trooper on patrol, our analysts, detectives in the field, and the NJSP's senior leadership. It acknowledges that we recognize that our primary responsibility as a state policing organization is to prevent and disrupt crime and terrorism and that we will do so by leveraging an intelligence apparatus that communicates clearly, shares information, and focuses resources.

A Word about Law Enforcement & Intelligence

Intelligence is often referred to as a powerful tool in a law enforcement organization's arsenal. It has the capacity to provide leaders with an operational picture of the environment that requires focused resources. It can aid analysts in determining how an organization should tackle problems. Moreover, it can provide operators with the requisite knowledge for centering investigations on specific targets. In sum, intelligence, as a structure, a process, and a product, is capable of strengthening a law enforcement organization's approach to better understanding the environment in which they police.

Just as intelligence is a powerful tool, it can be a potent enemy to a free society when practiced outside its legal boundaries. As a western democracy, the United States offers its citizens a considerable amount of liberty. The freedom to exercise this right is, in turn, contingent upon the law enforcement community exercising prudent restraint when striking a balance between protecting freedoms and ensuring security. The Tenth Amendment of the U.S. Constitution, also known as the "Police Powers Amendment," affords the States the authority to exercise sovereignty from the federal government in producing state initiatives. It endows the States with the authority to provide for their independent security – security from crime and terrorism. Although collecting intelligence on our citizens is a powerful tool for preventing crime and stopping terrorism, the police may do so only in a manner consistent with the Constitution. As a professional and ethical policing organization, it is our duty to ensure that when collecting and reporting information that is sensitive in nature, we do so with the highest degree of prudence toward protecting the rights of our citizens.

To safeguard the citizens of New Jersey from overzealous intelligence practices that may threaten the freedoms of our citizens, the NJSP will always exercise the highest degree of caution and professionalism when employing intelligence operations. In designing this guide, the NJSP was sensitive to the tenets outlined in *Title 28 Code of Federal Regulation, Part 23, and the Attorney General Guidelines on the Collection, Handling, Storage and Dissemination of Intelligence in New Jersey*. However, since it is outside the scope of this document to address all of the legal considerations involving the application of intelligence, readers are reminded to continually refer to the above-mentioned documents for direction.

Frank E. Rodgers
Lieutenant Colonel
Deputy Superintendent of Investigations
New Jersey State Police

EXECUTIVE SUMMARY

Recent decades have witnessed a rapid spread of communications and other technologies across all facets of society, enabling small and previously disassociated groups to better coordinate their activities and learn from each other in furtherance of their objectives. While such advancements have increased productivity and cooperation for the population overall, they have also created new opportunities for those outside the law, including organized criminal elements and terrorists. As a result, today's criminals are displaying increased sophistication and operational agility in their efforts to subvert law and order. These changes in the individuals and organizations carrying out criminal and other activities have culminated in the need to modernize the NJSP's business processes to optimize the allocation of resources and concentrate efforts in a more structured manner.

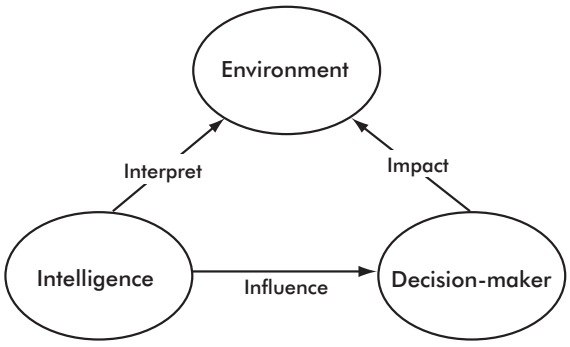

Figure 1. 3i Model of Intelligence-led Policing adapted from Ratcliffe

As New Jersey navigates toward a new normalcy focused on homeland and hometown security, it must improve its information and intelligence sharing capabilities. The series of processes and procedures the NJSP has adopted to meet these challenges is an adaptation of the 3i Model of Intelligence-Led Policing (ILP). The 3i Model (see Figure 1) introduced by Dr. Jerry Ratcliffe of Temple University is an approach to policing and resource allocation that places a great deal of emphasis on interpreting the criminal environment in order to influence decision-makers and create desired impacts upon the criminal environment. Collecting and analyzing information to produce finished intelligence products will provide decision-makers with situational awareness and a common understanding of the operating environment. Once informed, decision-makers can impact their environment through strategic, operational, or tactical initiatives.

Implementation of ILP at the NJSP is comprised of four main components: the reorganization of the Investigations Branch to better facilitate rapid deployment of intelligence and investigative assets as needed; the adoption of the Intelligence Cycle to support better situational awareness; the creation of a Regional Operations and Intelligence Center (ROIC), which is designed to provide tactical situational awareness; and use of strategic planning and intelligence-driven analyses to set priorities and allocate resources (see Figure 2 below).

Figure 2. Four components of ILP implementation

This *New Jersey State Police Practical Guide to Intelligence-led Policing* is a comprehensive resource outlining the NJSP's philosophy of ILP to achieve better situational awareness through the collection of data and the creation, dissemination, and cataloguing of intelligence products. These products will drive strategic decision-making and structured resource allocation to enable the NJSP to appropriately meet current and future challenges. This guide also defines the processes associated with intelligence that will be incorporated into NJSP-wide crime prevention and emergency management strategies. The primary aspect of this process is grounded by the need to establish a common understanding of the operating environment, a task that is achieved through the combined efforts of the Investigations Branch's formal Intelligence Cycle and the Regional Operations and Intelligence Center (ROIC)'s real-time situational awareness efforts.

Intelligence-led Policing (ILP)

Intelligence-led policing is a collaborative philosophy that starts with information, gathered at all levels of the organization that is analyzed to create useful intelligence and an improved understanding of the operational environment. This will assist leadership in making the best possible decisions with respect to crime control strategies, allocation of resources, and tactical operations. The adoption of ILP processes requires a concerted effort by all parties, including analysts, operators, and senior leaders. For analysts the key components of this process include the creation of tactical, operational and strategic intelligence products that support immediate needs, promote situational awareness, and provide the foundation for longer-term planning. For operators it requires becoming both better data collectors and better consumers of intelligence related products. This means shifting from emphasizing post-event evidence collection to constantly gathering all relevant data and ensuring it is provided for entry into appropriate databases, as well as drawing from the intelligence analysts and relevant databases all the information that is needed to support ongoing operations. Finally, adopting the ILP process requires senior leadership to actively engage the analysts and the operators to ensure the leadership has a sufficient picture of the operating environment and that it can act to distribute resources according to conclusions and priorities drawn from this understanding.

SECTION ONE: The NJSP Approach to Intelligence-led Policing

Information, Data and Intelligence

Unprocessed **information**, or raw **data**, represents the principle element of knowledge and as such is a critical input for rational decision-making. It can be used to create awareness and provide direction for ongoing and future activities. When properly analyzed and evaluated it can then be turned into a derivative known as "intelligence." In other words, information that has been transformed through evaluation and analysis into intelligence can be used to create a value-added product tailored to fulfill the requirements of its consumers.

Intelligence is the synthesis of known data/information and analytical reasoning to create a determination about the overall operating environment. Unfortunately, *intelligence* is often incorrectly used interchangeably with the terms *data* or *information*. In the past problems have arisen when law enforcement agents have misused official intelligence or when the general public has misunderstood the nature of the data being collected. For these reasons, it is important that particular care is taken when describing the nature of the information in question. Data/information refers simply to the raw information that is collected but has not been analyzed. It is critical that wide varieties of data/information be collected for two reasons: First, data is often perishable in nature and will be lost forever if it is not collected and catalogued at the time it is first encountered; and second, seemingly innocuous data might become critical in light of further analysis, which is akin to how all evidence at a crime scene is carefully catalogued in case it later becomes relevant to the case. Intelligence is the product of careful evaluation and analysis of all the collected data. Intelligence is then disseminated in reports and other products that enable operators, analysts, and senior leadership to better understand our collective operating environment and to drive appropriate resource allocation.

> Information is the principle element of knowledge that enables rational decision-making

Information/Data + Analysis = Intelligence

The Tradition of Intelligence in the NJSP

The New Jersey State Police has maintained an active intelligence component for several decades, and has a history of anticipating changes to the criminal environment. In April 1967, then-Superintendent Colonel David B. Kelly dedicated a group of detectives to investigate organized crime by creating an Intelligence Bureau. Through the continued efforts of Colonel Kelly and other members of the State Police, the legislature enacted new laws governing electronic surveillance, witness immunity, and a creation of a statewide grand jury to focus on organized crime.

In the decades that followed, the focus of organized crime investigations changed, and the Intelligence Bureau

addressed these challenges with the addition of three regional intelligence units. When the first casino opened in Atlantic City in 1976, NJSP commanders recognized the need to also develop intelligence on organized crime in the casino industry, and the Intelligence Bureau expanded to include a Casino Intelligence Unit. Throughout the 1980s, detectives assigned to the Intelligence Bureau both spearheaded and assisted the NJSP's Organized Crime Bureau to investigate and prosecute numerous high profile organized crime cases. In the 1990's, the intelligence initiatives expanded to include drug trafficking and street gang activities. For nearly 40 years, the NJSP has deeply valued the concepts of intelligence, devoting considerable resources to the cause.

As depicted in Figure 3, the keys to more effective policing include greater information sharing, improved communication, and enhanced coordination of effort and resource allocation.

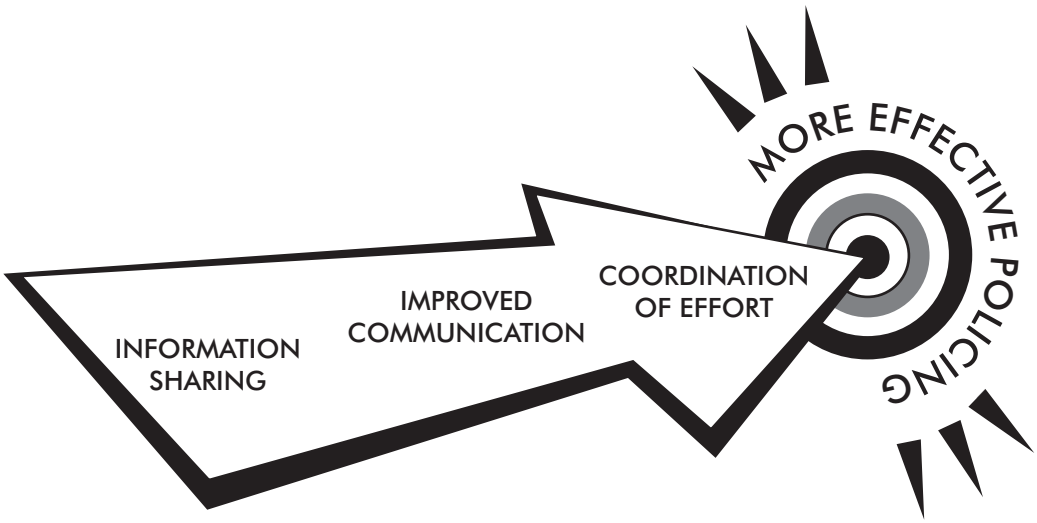

Figure 3. Keys to More Effective Policing

Yet today, as the State Police enters the new era of Homeland Security, its long-established intelligence construct cannot sustain the demands intrinsic to this new age. The intelligence processes of the past were aimed largely at organized criminal activities, creating a honed approach toward this end. Conversely, this focus also indirectly spawned information and operational silos that restricted the application of intelligence among select groups within the NJSP's former Intelligence Services Section. The threats the NJSP faces today have expanded beyond the criminal realm into terrorism and man-made and natural disasters. The hazards abound require the Superintendent to broaden the NJSP's scope and application of intelligence outside its traditional pathways and set a new direction to follow. Intelligence-led policing is the new intelligence course toward which the NJSP will set its sails.

Intelligence-Led Policing (ILP)

Intelligence-led policing is a management philosophy supporting optimal resource allocation based on fully understanding the operating environment. It is adapted from the United Kingdom's law enforcement community and has recently gained traction in the United States, particularly following the release of the National Criminal Intelligence Sharing Plan. ILP is a collaborative philosophy based on improved intelligence operations to aid in understanding changes in the operating environment to enable law enforcement to rapidly adjust to new circumstances. This philosophy supports decision makers who seek intelligence to improve their judgment and enable them to make the best possible decisions with respect to crime control strategies, allocation of resources, and tactical operations.

The key to ILP is to answer the need for targeted resource allocation to combat crime, terrorism and other law enforcement issues through improved situational awareness. For the trooper on the road, this requires feeding information into intelligence databases and receiving intelligence to assist patrol operations. At the detective and analysts' level, it refers to the broader understanding of issues that affect the NJSP throughout the state, as well

as in neighboring states. Finally, for the senior leadership it requires an awareness of events that affect the broader scope of all NJSP and partner activities.

Implementing ILP

The NJSP is aggressively changing its operational processes to bring improved structure to its near, mid and long-term planning and to optimize resource allocation decisions. This change requires a concerted effort by all parties – senior leaders, emergency management personnel, operators and analysts – in adopting an appropriate variant of the Intelligence-Led Policing model that is consistent with the mission, strategy, and core values of the NJSP. The tenets of the ILP process are defined by the simultaneous and ongoing implementation of four primary facets (see Figure 2 above): the reorganization of the NJSP to ensure an adaptable force construct for flexible deployment; adoption of the Intelligence Cycle for processing and analyzing data; development and integration of ROIC functions; and use of strategic planning and intelligence-driven analyses to set priorities and allocate resources.

NJSP Reorganization: an ILP Initiative

In 2005 the New Jersey State Police Investigations Branch Command began a careful review of its existing intelligence infrastructure to determine whether the organization had adapted to the challenges of policing in an era when both homeland security and traditional crime control place considerable demands on finite resources. After careful study, several barriers were identified and a strategic plan was crafted to transform the Investigations Branch into an agile investigative entity capable of tackling "all crimes, all hazards, all threats." The NJSP developed five strategies to ensure the success of this endeavor:

1. An architectural realignment of the organization to remove barriers and promote intelligence and information exchange.
2. A cultural shift to embrace intelligence-led policing philosophies and practices.
3. The re-tooling of the distribution and management of the Statewide Intelligence Management System (SIMS).
4. The creation of a "fusion center," known as the Regional Operations and Intelligence Center.
5. The implementation of regional accountability plans for managing intelligence and enforcement operations related to organized criminal activities[1].

In support of the structural changes outlined above, the decision was made to adapt intelligence-related NJSP policies and procedures to the contours of the intelligence cycle, which is a tried and true method of managing and promoting a constructive and orderly interface among data collectors, intelligence analysts, field operators, and intelligence product consumers.

ILP Role of Strategic Leadership

Adopting the ILP process requires senior leadership to actively engage the analysts and the operators to ensure the leadership has a sufficient picture of the operating environment and that it can act to distribute resources according to conclusions and priorities drawn from this understanding.

ILP Role of Operators (Troopers and Detectives)

For operators ILP requires becoming both better data collectors and better consumers of intelligence related products. This means shifting from emphasizing post-event evidence collection to constantly gathering all relevant data and ensuring it is provided for entry into appropriate databases, as well as drawing from the intelligence analysts and relevant databases all the information that is needed to support ongoing operations.

ILP Role of Analysts

For analysts the key components of the ILP process include the creation of tactical, operational and strategic intelligence products that support immediate needs, promote situational awareness, and provide the foundation for longer-term planning. The Intelligence Analyst also plays a vital role in the Intelligence Cycle. In addition to assisting in the creation of the Collection Intent, the Intelligence Officer is

[1]NJSP Investigations Branch. 2005. "Confronting the Investigative Challenges of the Homeland Security Era: Reorganizing the NJSP Investigations Branch."

responsible for making sure the Collection Plan remains a dynamic, living product.

ILP Role of the ROIC

The functions of the ROIC are three-fold: conducting watch floor operations (Watch Ops), real-time tactical intelligence analysis (Analysis), and tracking assets (Asset Management and Coordination). During daily operations, these functions are performed to create a complete picture of the current operating environment throughout the state of New Jersey, including external factors that may also present immediate concerns (terrorism, severe weather events, gang or drug problems in neighboring states, etc.) as well as the resources available to address them. During crisis operations these same functions remain paramount, albeit with much greater immediacy of information flow and expanded outreach to and integration with external agencies and federal partners. Drawing upon its resources and partners, the ROIC remains the center of gravity for the creation of a comprehensive common operating picture of relevant events and happenings within the state.

SECTION TWO: The Intelligence Cycle and the NJSP

Overview

The **Intelligence Cycle** is the process by which intelligence gaps are identified, relevant data/information are tasked and collected, then converted into finished intelligence for dissemination to consumers at the tactical, operational and strategic levels. These consumers, in due course, use that intelligence to make better-informed decisions. Consumers include policymakers, commanders, detectives, analysts, or troopers on patrol – anyone with the ***right to know*** and the ***need to know*** the intelligence.

Consumers, analysts, collectors, and other interested parties all have an opportunity to interact across multiple levels throughout the Intelligence Cycle. At its most basic level the intelligence cycle seeks to set appropriate tasking priorities for the collection of basic data, process that data into an easily useable format, analyze it to create situational awareness through intelligence products that support tactical, operational and strategic needs, then disseminate those products to customers who provide feedback on what additional or new intelligence requirements remain. The cycle begins anew as new requirements are again balanced against command guidance, operational needs, and resource constraints.

The NJSP intelligence cycle generally consists of five continuing phases: Planning and Direction, Collection, Analysis and Production, Dissemination, and Evaluation (see Figure 4).

Figure 4. Five phases of the intelligence cycle

Note, however, that while the Intelligence Cycle graphic is a useful framework for discussing the process of intelligence planning, collection, production, and dissemination, in practice this closed loop runs continuously and often involves simultaneous overlapping or parallel efforts. Because the threat environment is so dynamic certain process phases will at times require mid-cycle adjustments and overlap other related data collection and analysis cycles.

Phase I: Planning & Direction

Planning and Direction is the phase where intelligence consumers at all levels formulate questions about the operational environment and define their priorities for data collection and intelligence analysis efforts. These priorities are then coordinated through a formal tasking process that delineates each Branch's prioritized collection and analysis needs.

Planning and Direction is the most fundamental segment of the intelligence cycle because it identifies the specific focus areas with which the NJSP is concerned and therefore sets the boundaries of data collection, analysis and dissemination efforts. It is used to identify and codify focus areas that intelligence consumers have identified as their priorities so that collection assets can be assigned accordingly.

The Planning and Direction process represents a highly collaborative strategic practice, bringing together the NJSP's operational elements in order to develop annual *intelligence collection priorities* based on input from the NJSP Senior Leadership and regional commanders. The process, in effect, ensures that the Superintendent endorses the intelligence priorities deemed relevant by each Branch command. The Planning and Direction process is how the NJSP determines intelligence priorities and allocates assets to address those priorities through appropriate tasking guidance for data collection. It's designed to sharpen the focus of intelligence operations within the NJSP while remaining flexible to changes in the operational environment.

The diversity of the NJSP's mission requires that the Investigations, Homeland Security, and Operations Branches annually undergo an intelligence Planning and Direction process to produce their own *intelligence collection priorities* (due by November 15 of each year). Once Branch commanders complete their individual *intelligence collection priorities*, the Superintendent will convene a meeting in early December to discuss and approve each Branch's priorities. Each Branch is expected to defend their recommendations by using estimative analytical products (see Section Six) that identify intelligence gaps. The Administration Branch commander and the Director of the NJ ROIC Task Force will also attend this important meeting to ensure that the operations of their respective commands support the collection priorities of the other Branches. This support may include, for example, training, information and technology needs, tactical analytical support, etc.

Once the Superintendent endorses each Branch's respective *intelligence collection priorities*, the Branches are then required to codify these priorities and associated "Commander's Intent" within an internal publication for their membership to view (completed by the first week of January). The "Commander's Intent" ties together the vision, strategy, and mission of each Branch. This process ensures that resource allocations aimed at intelligence, investigative, and field operations are in line with the Superintendent's global vision for the NJSP.

After the Branch Commanders furnish their "Commander's Intent" to each of their subordinate Sections, it is the responsibility of each Section Commander to align their Section's strategic mission with the Branch commander's intent. In effect, Section Commanders will then undergo a similar process of developing a "Commander's Intent" for the section, identifying intelligence gaps and collections strategies. Depending on the mission and scope of the subordinate commands, this process of setting strategic course is then carried out at the Bureau or Region level to influence unit or station intelligence collection operations.

Note: This process is similar in principle to the NJSP's strategic planning process as outlined in Operations Instruction 6-17; however, this process focuses directly on intelligence collection objectives.

Phase II: Collection

Collection refers to the research and operations activities that fulfill the formal taskings created by the Planning and Direction phase. Collection involves both researching existing intelligence and conducting operations to gather **raw data** from a variety of potential sources. Once collected, this data must be fed back into the analytical cycle through appropriate channels so that it can be formally analyzed.

During the **collection** phase of the intelligence cycle, various NJSP and associated assets are tasked to collect data according to the intelligence planning and direction embodied in each Branch's Collection Intent, an annual document published by the Branch commanders from the Investigations, Operations, and Homeland Security Branches. Just as the Planning & Direction phase determined **what** to collect, the Collection phase addresses the **who**, **where** and **how** of the collection of information that fulfills commanders' needs.

The Collection Process is comprised of two main functions, research and operations:

- Research is the use of existing databases or other information repositories to search for information or previously processed intelligence that is relevant to the current investigation or other activity. It includes indices checks of federal, state, county and local law enforcement and other government databases, as well as open source information and subpoenaed documents.

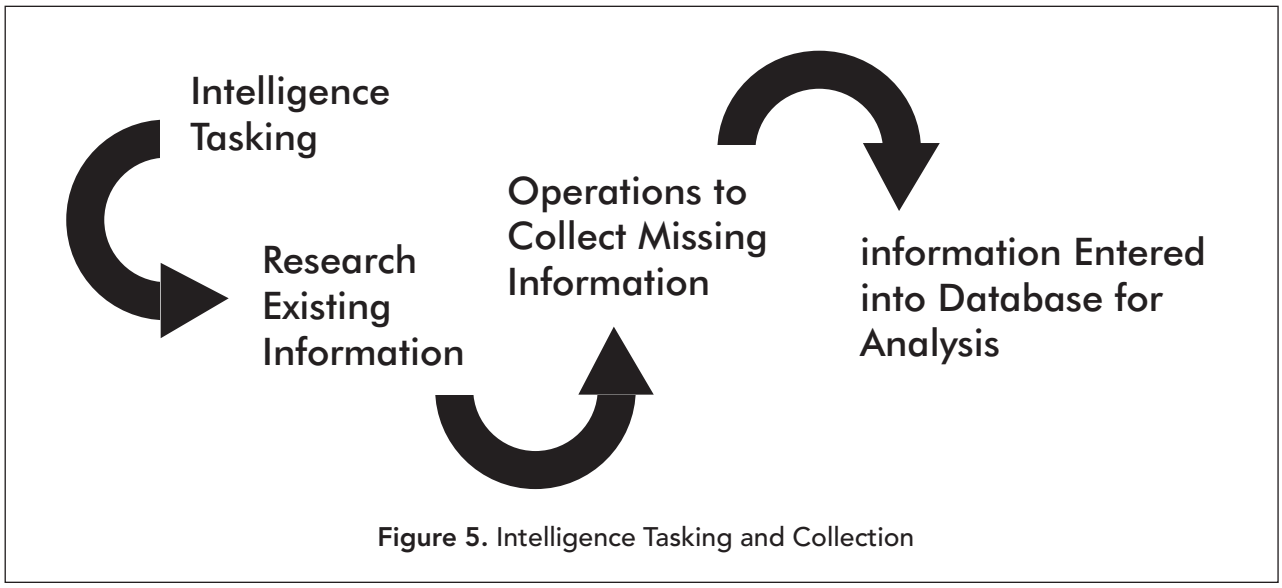

Figure 5. Intelligence Tasking and Collection

- Operations are the traditional police activities used to gain more data about a particular criminal environment or event. They include use of human sources (criminal and non-criminal), undercover operations, physical and electronic surveillance, and execution of search and/or arrest warrants. Under the Intelligence Cycle framework these collection activities are either tasked out or requested by the Regional Commanders in accordance with the Regional Collection Plans.

Sources of Information: Overt and Covert

Sources of information are wide-ranging—however, they are generally regarded as either **open source information** or **covert sources of information**. Open source information is that which is readily available to the public at large. Information gathered from open sources must be evaluated for reliability, relevance, and validity, as with covert sources of information. Once information is evaluated and analyzed, it is transformed into intelligence.

Some examples of types of open source information include:

- Business directories
- Media reports (newspapers, magazines, television, other publications, radio)
- Internet searches, chat rooms, and internet websites
- Telephone Directories and People Finders
- Commercial information providers

However, some of the most critical information can only be obtained through covert means. The most frequently used covert source is the confidential source, or informant. Other covert sources of information include:

- Indices Checks: Agency Records; Other Law Enforcement Agency Records; Credit Bureaus; City, County, and State Agencies; Courts; Schools Public Utilities; Employment; Banking and Financial Institutions; Military records
- Undercover operatives
- Physical surveillance (either remotely via videotape, or in-person)
- Electronic surveillance

Note: Although the above text reflects data related to criminal intelligence, the breadth and diversity of the NJSP's mission requires that our personnel collect intelligence related to other domains. For instance, members assigned to the Homeland Security Branch are required to collect intelligence related to natural and man-made disasters, critical infrastructure, and health crises (pandemics). This type of intelligence, which does not associate people to criminal activity, is not required to adhere to the guidelines promulgated by Title 28 Code of Federal Regulations, Part 23 and the Attorney General Guidelines on the Collection, Handling, and Dissemination of Intelligence in New Jersey; however, it should be of course done in a legal and ethical manner. This type of intelligence is stored in appropriate databases that do not contain intelligence related to criminal activity. Future addendums of this guide will delineate in detail how collection related to non-criminal intelligence involving Homeland Security and Emergency Management preparedness is tasked and carried out.

Phase III: Intelligence Analysis and Production

Analysis and Production is the transformation of collected data into intelligence codified in intelligence products such as reports and briefings. First, the raw data is evaluated for its validity and reliability and then entered into SIMS, which requires assigning a security and handling code. Next, analysis is performed to derive meaning, make conclusions and propose recommendations. Finally, production encompasses the timely presentation of the analysis, conclusions and recommendations in a format suitable to the consumer for the purpose of fulfilling different intelligence needs.

Intelligence analysis is the process of producing intelligence products (briefings, reports, etc.) based on evaluation of data and inputs from multiple sources about a specific area of interest. It involves, but is not limited to the analysis of previously processed intelligence, for often it requires analysts to draw upon experiences, context, and other relevant data points that may not be codified in existing finished intelligence reports. Once analysts have reached conclusions and made appropriate determinations regarding the matter, they create specific products in order to effectively communicate their findings, conclusions and recommendations.

The New Jersey State Police analyzes information to better inform the NJSP's understanding of the operational environment and to prevent crime by better allocating resources.

The purpose of intelligence analysis products is to provide consumers with products that aid them in decision-making and resource allocation. Delivery of such products is the **backbone** of intelligence-led policing. The type of intelligence analysis product delivered (style, format, approximate length, etc.) will depend upon the consumer's requirements. The analysis and production portion of the intelligence cycle is designed to be flexible and can accommodate a variety of products for a range of customers.

The NJSP analyzes information to better inform the command of the operational environment and to prevent crime by better allocating resources. While intelligence analysts are the primary personnel responsible for analysis, the techniques described herein can be utilized by enlisted members as well, both to become better intelligence collectors and consumers, as well as to find ways to conduct useful intelligence analysis for their own needs. (**Note**: This section is in no way intended to limit the creativity of analysts and enlisted members, but rather to assist in creating useful and relevant finished intelligence products.)

Types of Finished Intelligence Products

Examples of intelligence products include written reports, verbal or written presentations, and broadly focused background papers or estimates. Intelligence products can vary in length depending upon the depth of the analysis, the time frame in which the product is needed and consumer preferences. These products can offer value at one or more of the following levels:

Tactical Intelligence Products are focused on specific targets. An example of Tactical Intelligence product is the analysis of a specific leadership of a street gang in a specific neighborhood. The product will be used in carrying out near-term operations against that leader and their senior lieutenants. Tactical Intelligence can be described as the view from the street level. A tactical intelligence product should include target profiles, why the targets are considered a criminal network, the frequency of their interaction, types of crimes in which the network engages, chain of command in the network, geographic range of the network, interaction with other criminal networks, duration of criminal operations and the likely impact of law enforcement activities on the area in which the network operates. Currently, the bulk of tactical intelligence analysis will be conducted by Troopers and Detectives.

Operational Intelligence Products are those required for planning at the unit level. An example of Operational Intelligence is the analysis of information on a specific set of a street gang in a city. The final product will be used to assist in planning how to proceed in a criminal investigation against the set in the city. It will be used to determine how to approach the overall problem of dealing with that one gang in relation to the overall gang problem in that region.

Strategic Intelligence Products are those required for policy formation and planning. For the NJSP, Strategic Analysis focuses on regional and statewide trends of crime and criminal

organizations, as well as potential terrorist threats. An example of Strategic Intelligence is a statewide analysis of a street gang to determine their areas of influence, likely criminal activity and probable future direction of the organization. Strategic Intelligence can be described as the view from 40,000 feet. NJSP intelligence analysts will be responsible for Strategic Intelligence Analysis on both a regional and statewide basis.

Phase IV: Dissemination

Dissemination is a critical process because the finished intelligence is of no value if it is not properly distributed to all relevant consumers and integrated into the appropriate intelligence database for use in future analyses. Given the sensitive nature of certain collection methods it is important to adhere to the guidelines that have been established by the federal and state governments with regard to the dissemination of intelligence. Nonetheless, whenever possible the analytical reports, briefings and other products should be disseminated as widely as possible to inform decisions by all relevant parties.

The dissemination phase refers to the need to ensure the widest practicable dissemination of the intelligence products that have been created by the NJSP, including both internal and external dissemination. The internal dissemination should include both directly presenting the products to interested parties and their entry into SIMS so that the intelligence products become part of the SIMS universe of data. External dissemination includes reaching out to share intelligence, whenever permitted, with both law enforcement and other public sector agencies as well as private sector entities. This is especially critical in an era of terrorism and globalization, wherein the ability of all to better understand the threat and operating environment can improve both the public and private sector's preparedness for dealing with whatever issues may arise.

Phase V: Intelligence Product Evaluation

Intelligence Product Evaluation is the final task and is a central and ongoing feature of the intelligence cycle. Responsible evaluation provides appropriate feedback by which analysts can determine if they are meeting the needs of their consumers with appropriate analysis and relevant products. It is also the best means for peer-to-peer analyst interaction, for the entire intelligence process is greatly enhanced when the sharing of information, understanding, and situational awareness amongst analysts is encouraged and promoted.

It is intuitively obvious that in order for the analytical community to better produce future products of maximum utility they need to receive feedback regarding previous products. However, one of the least precise functions of the intelligence cycle is the development of appropriate feedback mechanisms for analytical products. While many different people are involved in the intelligence cycle as both collectors and consumers, it is essential that these same participants, as well as fellow analysts, offer specific and constructive feedback regarding the utility of the analysts' products. Processes for this evaluation should include direct feedback from the end-users at the senior leadership (strategic), unit command (operational) and the operator (tactical) levels, as well as from analysts throughout the NJSP.

SECTION THREE: The New Jersey Regional Operations and Intelligence Center (ROIC) Task Force

As New Jersey's fusion center, the ROIC's intended benefits are to increase situational awareness of what is taking place in the operational environment, to provide a tactical intelligence analysis of how to best prevent or respond to changes in this environment, and to better manage asset allocation. Taken together, these ROIC's activities will enable the NJSP to maximize the utility of their resources, streamline operations, and improve their collective ability to fight crime and terrorism. With New Jersey's focus on an "all crimes - all hazards - all threats – all the time" preparedness strategy, it is imperative that the ROIC's analytical capacity be aligned with the NJSP's intelligence cycle in order to promote ongoing tactical situational awareness by the NJSP and relevant partners. This integration will evolve over time, and should be fostered by close interaction among the ROIC and the Investigations Branch's operational and strategic analysts. A central role is played by the ROIC's Watch Operations function, whereby NJSP personnel provide near-real-time situational awareness and coordinate with state and federal agencies to track issues of concern. Of equal importance is the performance of the analysts who, daily, are responsible for "connecting the dots" and producing finished intelligence products required for influencing decision-makers. Each function is carried out on a continual basis, though they are of course greatly energized and consume much greater attention during various crisis operations. At the same time, the ROIC must remain engaged in the management of emergency response assets.

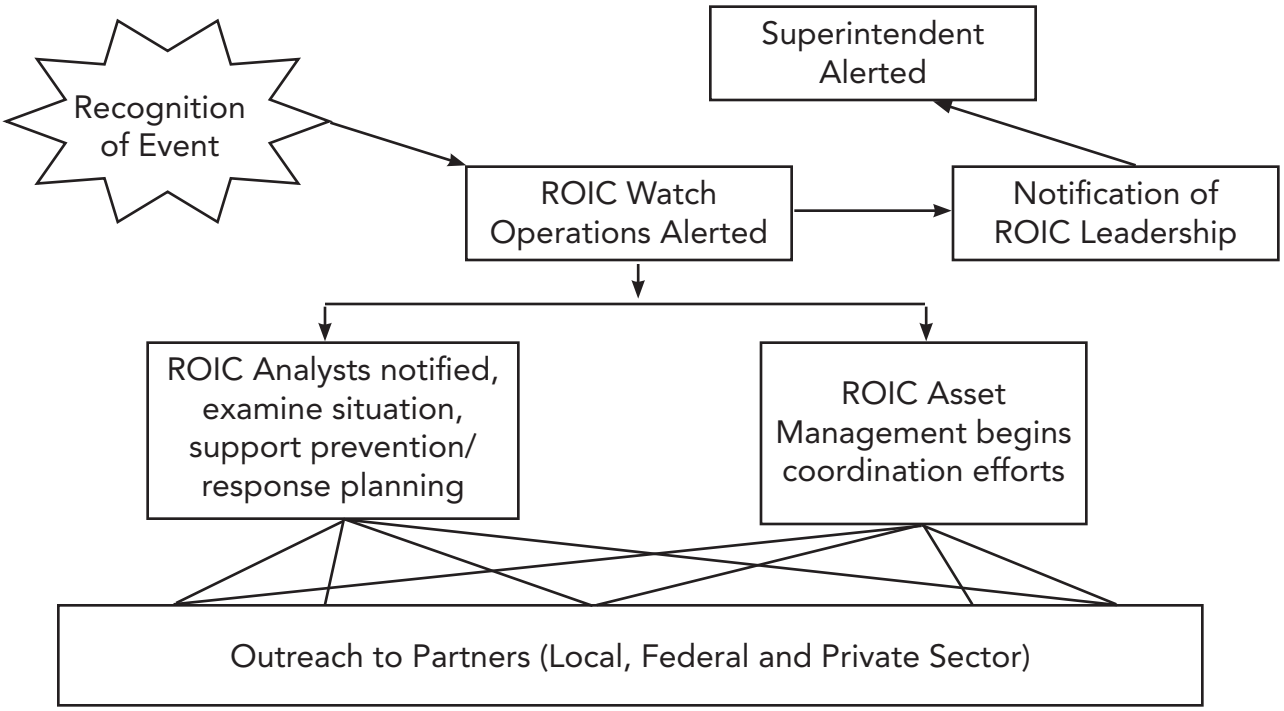

Figure 6. ROIC Alert Response Processes

New Jersey has established the ROIC Task Force to create intelligence and warning for a diverse customer base. The functions of the ROIC are threefold, including Watch Operations, Analysis, and Asset Management and Coordination.

The *Watch Operations* component is responsible for working with the ROIC intelligence analysts to develop the common picture of the NJSP's operational environment and for receiving and responding to alerts regarding changes to that environment. This function requires a variety of real-time operations such as answering phone-in tip lines and the 911 call center, providing operational de-confliction, and providing 24/7 "reach-back" support to investigators in the field such as conducting criminal background and intelligence checks. They are also the central authority responsible for notifying the command staff of significant events. *Watch Operations* personnel also answer requests for aviation, maritime, arson/bomb and K-9 assets, as well as facial recognition comparison analysis requests. They also maintain connectivity to the watch floors at other intelligence centers (Interpol, El Paso Intelligence Center, National Operations Center, National Joint Terrorism Task Force, etc.) to ensure NJSP personnel are aware of ongoing multi-agency issues.

> Watch Operations is responsible for real-time situational awareness of activities of interest across the state and beyond.

The *Analysis* component is responsible for creating tactical and operational intelligence products to service the NJSP and other consumers within the Homeland Security, Emergency Management, and Public Safety communities through daily, weekly, and monthly bulletins. In addition, this section of the ROIC is responsible for conducting rapid analytical support at the tactical level for ongoing operations to the following crime programs across the state's three regions (north, central, and south): street gangs and guns, counter terrorism, drug trafficking, organized crime and corruption, and general crime. The intelligence analysis portion of the ROIC also supports emergency responders, especially during a terrorist event. Moreover, the analysis

> The Analysis component provides intelligence support for immediate tactical needs.

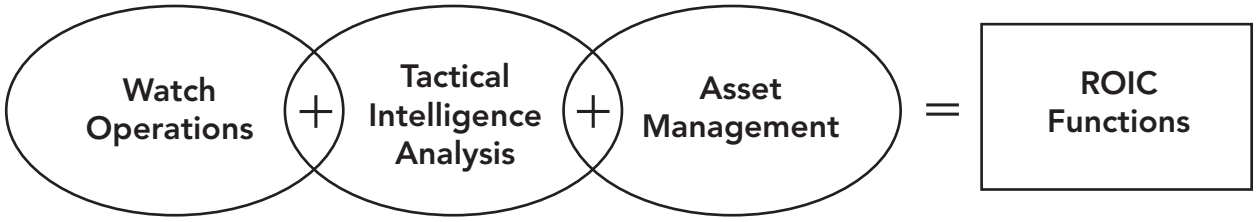

Figure 7. Functions of the ROIC

component is responsible for coordinating intelligence briefings and interfacing with analytical groups from other agencies on the Federal, state and local levels. The *analysis* component is also in charge of generating finished intelligence products to service the public safety community, which includes the fields of health, agriculture, transportation, and the fire service or any entity that can enhance and further New Jersey's prepardeness level. The ROIC's analysis component is responsible for producing assessments, briefings, and bulletins for the 23 key industry sectors that participate in the Critical Infrastructure Advisory Committee.

Asset Management enables better prevention and response by tracking asset status and supporting timely asset deployment.

Finally, the *Asset Management and Coordination* component of the ROIC is responsible for maintaining awareness of the disposition of NJSP and select partner assets for the purpose of coordinated response to threats and incidents. During Level 1, 2 and 3 of an emergency crisis, assets will be directly managed by the ROIC staff, while during Level 4 and 5 crisis and the corresponding need to stand up an Emergency Operations Center (EOC), the ROIC's role will be to provide the EOC with information on the status, location, and operational capabilities of NJSP assets. Through this function, the ROIC will also strive to ensure that all relevant information and intelligence that resides within its Watch Operations and Analysis functions are made available to the EOC, as necessary.

As part of this asset management and support to emergency operations the ROIC also needs to become the state's central repository for the hundreds of response plans, traffic diversion plans, emergency operations plans, evacuation plans, school plans, contingency action plans and risk management plans. In order to achieve this task and facilitate an emergency response, all of the existing plans (many of which have been developed, but have never been made accessible to the appropriate personnel in the ROIC) will be loaded into a computer database and made accessible through the Emergency Preparedness Information Network (EPINet).

The following is a partial list of ROIC functions and tasks with select functions defined in greater detail:

Watch Operations	Analysis	Asset Management
• The Superintendent's Daily Briefing • Command 'Blackberry' messages • Periodic weather and traffic updates • GIS mapping for Operations Ceasefire and Safe-Cities	• Intelligence support for Investigations • Threat assessments • Intelligence reports and briefings • Criminal financial analysis • Telephone-toll analysis • Association, link, and network analysis • Crime-pattern analysis • Criminal case correlation • Critical infrastructure analysis and reports on target hardening and threat advisories	• Asset availability • Asset deployment Tracking • Outreach to partner agencies to determine asset availability/status

SECTION FOUR: Roles and Functions of Key Players in Intelligence-led Policing

NJSP Leadership

All levels of the NJSP leadership must strive to implement the ILP framework by applying its precepts to their specific organizational role. This includes, most obviously, setting priorities based on the Commander's Intent, fulfilling the Intelligence Collection Tasking, and striving to support development of a highly accurate common operating picture through the analysis of events and other relevant intelligence. Three key tasks will define success for the efforts of the NJSP leadership:

1) Setting appropriate guidance for prioritized intelligence collection and operational focus;
2) Supporting full NJSP adoption of ILP and the Intel Cycle, to include allocation of necessary funding for equipment upgrades and training for analysts, operators, and other users;
3) Implementing promotional and other job performance standards based on group performance with respect to these priorities.

In particular, the unit level leadership will play a significant role in the success of ILP. It will require more management of resources in accordance with stated NJSP priorities as well as ensuring that squads properly collect and process requested information, including validation of SIMS entries. Unit leaders are also responsible for understanding the value that analysts can provide to their units regarding interpreting information collected from the field. They are expected to encourage the interface between operators including briefings, debriefings and updates. Finally, the analysts will play the key role in ensuring that crime prevention practices become paramount and that practices are implemented to reward team performance, and not individual efforts.

Operators (Troopers & Detectives)

One part of the ILP-relevant role of operators is in essence that of becoming Data Collectors. Because all Operators have always collected the kind of information being sought under ILP, be it consciously or unconsciously, this is not as much a departure from their historic roles as a necessary evolution of policing. For example, operators have always sought to identify the key leaders of organized crime families, or to determine when one gang was moving into another gang's territory, or to look for operational deviations within the practices of drug dealers that may presage a shift in distribution or a coming wave of violence. The differences under ILP are two-fold:

1) In addition to the information collected in the normal discharge of duties, under ILP specific collection priorities are identified and tasked out for collection so as to fill in critical gaps in the current understanding of the operational environment; and
2) Today the Operators need not only collect such information, but also ***record the information into the proper SIMS database*** to maximize utility through broader analysis and understanding of all relevant information.

In other words, through ILP the NJSP must now extract all relevant information from its "eyes-on-the-street" in order to provide the analysts with information to properly characterize the operating environment. This, in turn, will promote operations that address the primary challenges facing the law enforcement community in New Jersey.

Additional significant functions of operators include conducting operations and additional research/outreach to fellow operators to acquire relevant data for processing into intelligence products. They also must more regularly engage analysts and formally request appropriate analytical intelligence support for ongoing operations (including briefings/debriefings with the analysts). This latter role necessarily represents a more dynamic interaction between the operators and the analysts, but this is only logical given the need to better capture and represent the sum of the NJSP's understanding of its operating environment. Finally, operators will need to provide intelligence analysts with evaluations of products and other relevant feedback to ensure optimal future analysis in support of their tactical, operational, and strategic needs.

Intelligence Analysts[2]

The NJSP's adoption of ILP has perhaps its most profound impact upon analysts because their roles are now relatively

[2] The description of the intelligence analysts' role in ILP is somewhat lengthier than those of the other Key Players because the analysts' role in ILP is more of a departure from traditional NJSP practices, and therefore requires more detailed explanation, which is meant to inform both the analysts and all other ILP participants as to the types of roles the analysts are expected to fulfill.

more sharply defined and significantly more robust than under previous policing paradigms. The following section describes the basic roles and functions of analysts, whether they are assigned to the Investigation Branches' Regional Bureaus, the ROIC's Watch Operations or Analysis elements, or elsewhere within the organization. This is a critical aspect of ILP, because in order to provide maximum utility from somewhat limited resources, all NJSP analysts will need to find ways to collaborate, regardless of where they are assigned.

The primary role of intelligence analysts is to work with the operators, analysts, ROIC personnel, and external partners (public and private) to develop accurate situational awareness upon which the NJSP leadership can make appropriate resource allocation decisions. This is a significant function, and one that requires a concerted effort to develop and constantly update the overall understanding of the operational environment. It requires reaching out to analysts, both within and outside the NJSP to foster cooperation and compare notes, as well as ensuring all relevant external open-source information and other available intelligence products are included in SIMS or other appropriate databases. It also requires thinking across the tactical, operational and strategic levels in order to provide appropriate, relevant reports and other finished products to Troopers/Detectives, fellow analysts, and strategic leadership.

The primary functions of the analysts are to:

- Develop timely and relevant intelligence products that address the information needs of tactical, operational and strategic intelligence customers.
- Develop and maintain in-depth awareness of, and familiarity with evolutions in the criminal environment throughout New Jersey, and, as needed, throughout the world.
- Assist strategic and operational leaders with formulation and production of Section and Bureau collection intent, operating directives and collection requirements.

Achieving these ends requires maintaining contact with Troopers, Detectives, ROIC Watch Operations personnel, and fellow analysts in order to exchange information about relevant features of the operating environment. Because the Intelligence Cycle requires information flow to be a two-way street, the analysts will need to both provide briefings to intelligence consumers on various topics as well as debrief them to gather tactical and operational knowledge that can be fed into further analysis. Analysts will also need to blend a wide range of open source information with covert reporting when developing intelligence products in order to better describe the environment and context in which criminal activity is occurring. This in turn requires analysts to conduct ongoing critical evaluations of their own information sources, analytical assumptions and intelligence judgments, as well as to perform quality assurance/peer review of intelligence products to ensure that the effects of bias, groupthink or selective omission are eliminated. Finally, analysts will need to take the initiative in refining/defining/determining the information needs of intelligence consumers based on a balance of mission parameters, operating environment and consumer guidance, including regular consultation with the Section and Bureau Intelligence Officers to adapt intelligence collection requirements to changing conditions.

In addition, NJSP analysts play a role as a collator of information, meaning they are required to work with all new intelligence reports to review each report to determine the significant elements of the intelligence topic (who/ what/ where/ how/ when/ etc), and to validate the information through queries against the SIMS database to determine if previous intelligence confirms/conflicts/does not exist. They then need to ensure the report is appropriately annotated, and notify the appropriate Section/Regional analysts concerning the determination of supportive or contradictory information.

SECTION FIVE: The Intelligence Report

Intelligence reports are the principal method by which collectors (Troopers, Detectives, Analysts, and others) document and communicate criminal intelligence information. They are, in essence, the most fundamental component of any intelligence-led policing system.[3] However, the information they focus on is much more descriptive of the operating environment and its targets than the specifics of a criminal investigation, and therefore are somewhat different from the traditional reports filed by Troopers. Two key developments have changed the

[3] Use of the generic term intelligence report stems from the traditional use of such reports. With select exceptions, however, the information contained within intelligence reports in SIMS will actually be raw data or information, as opposed to processed intelligence. Notwithstanding this definitional discrepancy and in keeping with tradition, NJSP will use the term intelligence report in an effort to differentiate it from other reports used within the New Jersey State Police.

NJSP's reliance upon the intelligence report and the need to add clarification regarding its use: the adoption of Intelligence-led Policing (ILP) and the use of the Statewide Intelligence Management System (SIMS) database to collect and record information and intelligence.

Understanding the Intelligence Report

> The aim of intelligence reports is to provide lead information necessary for preventing crime, identifying and interdicting targets, influencing future operations and policy decisions, and guiding resource allocation.

A useful analogy for describing the information used in an intelligence report is the information contained in a Trooper's memo book.[4] When a Trooper receives information from a source (i.e. witness, victim, informant, etc.) they often note relevant nuggets of information in their memo book, even though much of this information may never appear in an Operations Report or Investigations Report. It is this information that, when compared and contrasted against other data sets, can paint a more detailed picture of the operating environment in which the NJSP has a vested interest. Unfortunately, this potentially significant information typically remains in the Trooper's notebook, and not in an NJSP database, which inherently limits its ability to be available for use in formal analysis. Under ILP, this paradigm must change by entering such information as an intelligence report in the SIMS database.

Unlike investigation reports, which are evidentiary in nature and must satisfy the elements of proof required for criminal prosecutions, the aim of intelligence reports is to provide lead information necessary for interpreting the environment, preventing crime, identifying and interdicting targets, influencing future operations and policy decisions, and guiding resource allocation. These specialized reports aid in understanding the operating environment and the actions of specific suspects and criminal enterprises who occupy this terrain. Information contained in intelligence reports may seem innocuous; however, when teamed or examined against other pieces of data they are nonetheless valuable to police operations.

Intelligence Reports and ILP

Intelligence-led policing requires that intelligence operators and analysts interpret the criminal environment and then influence decision-makers through finished intelligence products, who in turn impact the environment through appropriate resource allocation. This analytical interpreting of the criminal environment can only emerge when operators actively engage in criminal intelligence collection operations that "pull" information to support better understanding of their operating environment.

The SIMS intelligence report is the primary vehicle by which the trooper, detective, or analyst can add to the criminal intelligence component of the SIMS database. The implementation of SIMS has eliminated the need for the paper-based SP382, the former intelligence report for the NJSP. Today, SIMS, underpinned by the Memex™ Intelligence Manager software, has the capacity to digitally record information that collectors choose to input. The SIMS intelligence report not only captures text related to collection activity, but also affords contributors the ability to append other data, media, or information files to enhance the intelligence collected.

Understandably, much of the confusion over the proper use of the intelligence report stems from the traditional role that Troopers have played in the law enforcement realm - that of being first responders. From the time a Trooper graduates the Academy until he or she completes their final tour on the road, whether through an Accident Report, Operations Report, Investigations Report, or a Stop Report, with a few exceptions all of their experience writing police reports will have been 'post-incident.'

[4] **NOTE**: The above analogy merits qualification, adding that troopers should not to submit all their notebook entries as intelligence reports. "Title 28 CFR, Part 23," the "Attorney General Guidelines on the Collection, Handling, and Dissemination of Intelligence in New Jersey," and common sense will dictate and set parameters for such submissions. The analogy instead outlines the vehicle for use by members for documenting perishable lead information related to criminal activity. In the past, this information may have been lost to a member's notebook. Today, all members have the opportunity to document suspect information into an intelligence report for dissemination across the larger law enforcement community.

This confusion over the intelligence report is not limited to the NJSP. Twenty-five years ago, Frost and Morris outlined the primary differences between investigative and intelligence reporting to illuminate this issue.[5] They distilled the principal differences between the two reports into the meaning of two words: evidentiary and premonitory (meaning warning in advance).[6] Figure 8 below illustrates the divergence between the two reporting styles.

Investigative	Intelligence
• Report is evidentiary in nature. • Presents information that, when taken as a whole, satisfy the elements of proof of a past criminal offense. • Report must describe what is to be reported without opinion or amplification. • Manner in which information is gathered must conform to strict rules of criminal procedure if defendants are to be prosecuted.	• Reporting is premonitory (provides advance notice). • Prosecution is not the main objective. • Intended to direct organizations toward potential criminal activities that require focused investigations or alert them to future threats requiring tactical responses. • Cannot be expected to meet rigorous standards for formal investigative reporting.

Figure 8. Differences between reporting styles; adapted from the work of Frost, C. and J. Morris (1983) Police Intelligence Reports. Palmer Enterprises (Orangevale, CA)

Most Troopers are not familiar with writing for a premonitory purpose and might find this concept difficult to put into practice. However, once understood within its proper role and context, the intelligence report becomes as essential and manageable a tool for law enforcement as any other type of report.

To be of greatest value to its consumers, and to assist in protecting it from unintentional compromise, an intelligence report should adhere to the following guidelines:

- Each report should address only one subject or event when possible.
  This makes for easier understanding and it also tends to protect a second intelligence collection effort or open case should one or the other be brought on complaint to an "in camera" hearing with a judge.
- Each report should reflect the statements of one source. Usually a report will be obtained from a single source, although brief reports from several sources can be combined into one report on the same subject or event.
- Each report should be carefully sourced. Consumers must be able to distinguish information the source provides from that the source obtained from one or more sub-sources.
- Segregate background information from collected intelligence. What was history and now difficult to verify and validate should be carefully separated from current intelligence.
- All writing should be carefully phrased to guard against careless or inadvertent compromise of sensitive sources and collection methods and strategies.[7]

While the intelligence report should follow a distinctive format, it need not be a protracted chronological record similar to the format used in the investigations report. The aim of an intelligence report is to be timely. Rapidly communicating information gleaned from the fluid criminal environment to decision-makers requires that intelligence reports be brief, concise, and recognized to be perishable. Unlike an investigative report, contributors should not view the intelligence report as a completed account in which all pieces of the narrative story are already known. The intelligence report instead is useful only when it becomes part of a larger mosaic of information contained in an intelligence system.

The intelligence report is useful only when it becomes part of a larger mosaic of information contained in an intelligence system.

In the past, NJSP intelligence detectives were required to submit paper-based intelligence reports that

[5] Frost, C. and J. Morris (1983) Police Intelligence Reports. Palmer Enterprises (Orangevale, CA),
[6] Ibid, p. II-4.
[7] Frost and Morris, p. III - 1

would undergo a process of review before clerical staff would enter summaries of such reports into an antiquated database. The review process could take weeks and the submission into the database could take months. Although the intelligence detectives were adept at writing intelligence reports, they often dismissed reporting on issues that were timely in nature and instead favored reporting on information that could appeal to the reader in the future. This style of reporting seemed to fit the practices of investigating traditional organized crime, where criminal relationships that evolve over time were central to the association-in-fact conspiracy investigations intelligence detectives investigated. However, these practices, limited by an antiquated intelligence system, could not process reporting on the rapid-paced activities of non-traditional organized crime networks dealing in drugs and violence. For instance, if an intelligence detective received information that a trafficker was delivering a bulk load of cocaine to New Jersey in a few days, it could take at least a month before that information would make it into an intelligence system viewable to others. Of course, by that time the information would have become outdated and of little value.

Today, with the inception of SIMS, the intelligence report has climbed to new heights within the NJSP and law enforcement community within New Jersey. Once receiving lead information that meets system submission criteria, a contributor can enter an intelligence report into SIMS that is available to other users across the network. Timely access to this new digital intelligence report can sustain consumers, at all levels, the capacity to assess changes in the criminal environment that effect strategic deployments and targeted operations.

Intelligence Reporting Procedures for the Statewide Intelligence Management System

Situational awareness of the environment begins with the process of collecting timely, relevant, and accurate information. However, in order for collected information to be of any value, it must first be reported. Although members enjoy a sundry of reports for reporting police information, each carrying established systems, protocols, and specific guidelines to govern the type and flow of information, the NJSP recognizes only one report for capturing criminal intelligence. This report is contained within SIMS. SIMS affords its trained users a magnetic medium for reporting collected criminal intelligence that satisfies the guidelines promulgated in Title 28, Code of Federal Regulations, Part 23 (28 CFR, part 23).

28 CFR, part 23 governs the basic requirements of the processes inherent to an intelligence management system. The processes include: a) information submission or collection, b) secure storage, c) inquiry and search capability, d) controlled dissemination, and e) the purge and review process. Although SIMS administers its entire operation in accordance with each of the above elements, for purposes of this chapter, we are only concerned with the first process. The format for capturing information reflective of criminal intelligence collected from the field, which has been evaluated for reasonable suspicion and which meets all submission criteria that makes it eligible to be inputted into a criminal intelligence database, will be outlined ahead.

In keeping with 28 CFR, part 23, "operators shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. In addition, an operator shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. Reasonable suspicion or criminal predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise."[8]

The following types of information, associated with criminal activity, constitute valid examples of criminal intelligence that collectors should report in SIMS. Each information type is followed by a brief description of WHY it constitutes valid criminal intelligence.

[8] Title 28, Code of Federal Regulations, Part 23.

a) Credible allegations (from whatever source) of criminal activity on the part of individuals or organizational entities

WHY: If the reporting SIMS user has a reasonable belief that the allegation may be true, information concerning past, present or future criminal activity provides criminal justice agencies with leads that may solve or prevent crimes.

VALID SCENARIO: "On July 14, 2005 confidential informant NJSP2005-08-267 informed me that William Carter and his wife Betty Carter are currently operating an out-call escort service from their residence in Eatontown, Monmouth County, NJ. A relative of NJSP2005-08-267 has been approached to work for this escort service. The Carters reside at 138 Glendora Rd, Eatontown." The source believes that this business is used to facilitate prostitution. [partial report excerpt]

INVALID SCENARIO: "A concerned citizen who wishes to remain anonymous called the dispatcher to report a suspicious male on her street this morning, lurking around her garbage cans as they sat on the curb waiting for pickup." [no allegation of criminal activity, just vague suspicions]

b) Fully articulated suspicions of criminal activity described and/or substantiated by trained employees of a criminal justice agency

WHY: If the reporting SIMS user properly articulates his/her suspicions, this information concerning past, present or potential future criminal activity provides other SIMS users with leads that may solve or prevent crimes.

c) Descriptions of modus operandi employed in the conduct of criminal activity, either by specific suspects or by persons unknown

WHY: Description of a criminal modus operandi can permit other investigators to more rapidly develop a reasonable suspicion of similar criminal activity, and to articulate that suspicion in a subsequent SIMS report. Descriptions of modus operandi also contribute to commanders' awareness of the criminal environment in their own or neighboring jurisdictions.

d) Associations between known or suspected criminals

WHY: Identification of associations between criminals permits other SIMS users to learn the scope and membership of criminal networks engaged in specific types of crimes.

e) Associations between known or suspected criminals and organizational entities

WHY: Describing associations between criminals and organizations increases the number of investigative avenues that can be explored by other SIMS users who may have access to additional information concerning suspected criminal activity involving those organizations.

f) Locations frequented by known or suspected criminals

WHY: Establishing the locations frequented by criminal suspects allows other SIMS users to more quickly identify places where these suspects can be found, and can also contribute to the development of reasonable suspicion of criminal activity on the part of others who are repeatedly present at those locations at the same times.

g) Ownership of property and/or other assets used or controlled by known or suspected criminals

WHY: Establishing ownership of property and other assets can assist civil forfeiture proceedings initiated in conjunction with a criminal prosecution.

h) Estimates of revenue generated by criminal activities and enterprises

WHY: Providing estimates of criminal revenue can assist commanders in setting enforcement priorities, and (under state statute) can also determine the degree of the crime suspected.

i) Surveillance of individuals known to be connected to or suspected of criminal activity

WHY: Surveillance reports describe vehicles used by criminal suspects, the locations frequented and their personal interactions, and often include descriptions of the suspects' actions and behavior. This information can form the basis for describing a criminal modus operandi in SIMS, or serve as substantiation for claims of criminal associations between individuals.

Understanding the SIMS Intelligence Report

The SIMS intelligence report is divided into two pages, titled Main Details and Text/Narrative (See Figure 9). Overall the report consists of a range of fields (Evaluation, URN,

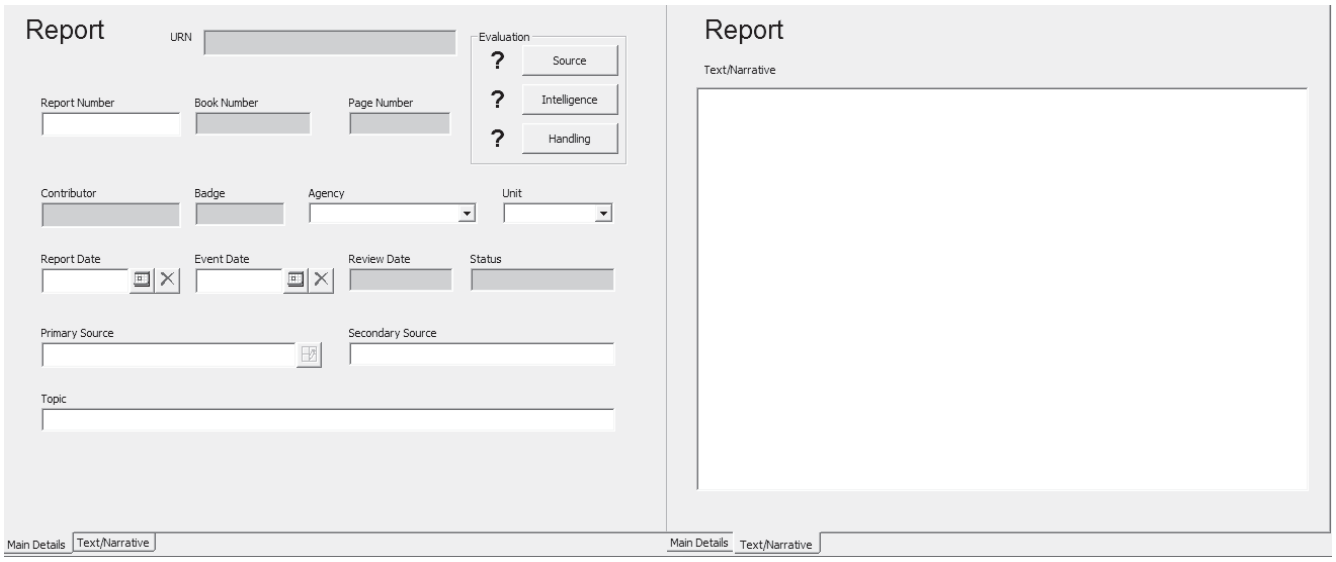

Figure 9. Two page SIMS Intelligence Report

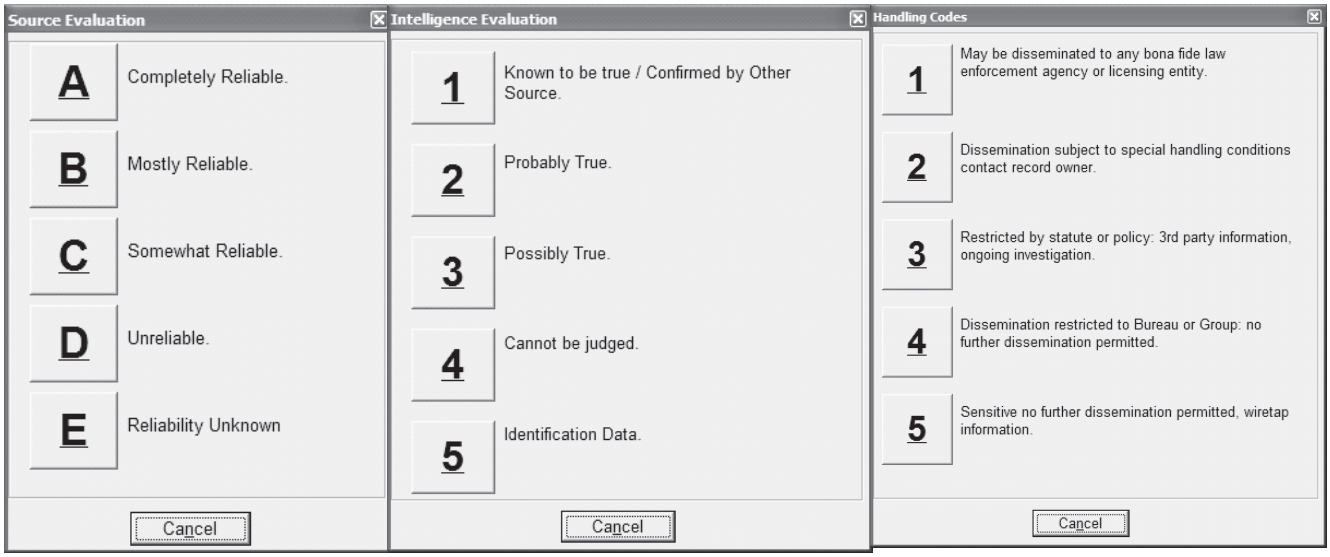

Figure 10. Evaluation Section of SIMS Intelligence Report

Figure 11. Topic Field from a SIMS Intelligence Report

Contributor, Agency, Unit, Report Date, Event Date, Review Date, Status, Primary Source, Secondary Source, Topic, and Text/Narrative) that are intended to satisfy the elements (who, what, why, when, how) of an effective intelligence report. The majority of these fields are self-explanatory and do not require much effort. However, three fields; Evaluation, Topic, and Text/Narrative, in particular, warrant special attention.

The **Evaluation** field (See Figure 10) requires contributors to assess three evaluation components involving the intelligence submission. They include an evaluation of the credibility of the source, the veracity of reported intelligence, and recommendations for handling the completed intelligence report. Contributors should pay particular attention to the ratings they provide in each of these three fields in order to ensure an accurate portrayal of collected information while balancing the need to protect the source and method of collection.

The second unique field requiring particular attention by the contributor is the Topic field (Figure 11), which denotes the title and subject of the intelligence report. Often times, when users conduct queries through SIMS they are confronted with a long list of search results. A properly titled report will speed the decision-making required of users who must sift through numerous reports when looking for a specific subject or result. This element of the intelligence report will be of great

value to those who may access the report in the future. To determine whether the title chosen is an adequate descriptor of an intelligence report the writer should look ahead to how it will be later displayed and ask the following questions: is the title a) unnecessarily wordy?, b) too cryptic?, or c) not specific enough?[9]

The final field warranting extra attention is the Text/Narrative field (Figure 12) of the SIMS intelligence report. Report writing skills are a premium on all state police reports and the intelligence report is no different. At a minimum, contributors should seek to detail the who, what, why, where, when, and perhaps the how of the event.[10] Although there is currently no absolute format for the narrative portion of the SIMS intelligence report it is a good practice to provide the reader some context of the reporting to follow and may possibly provide a description of the criminal predicate. This also serves as a bridge for linking the current report with past and future reports. The remainder of the report should depict the current event being reported, vigilantly paying attention to the guidelines and recommendations mentioned above.

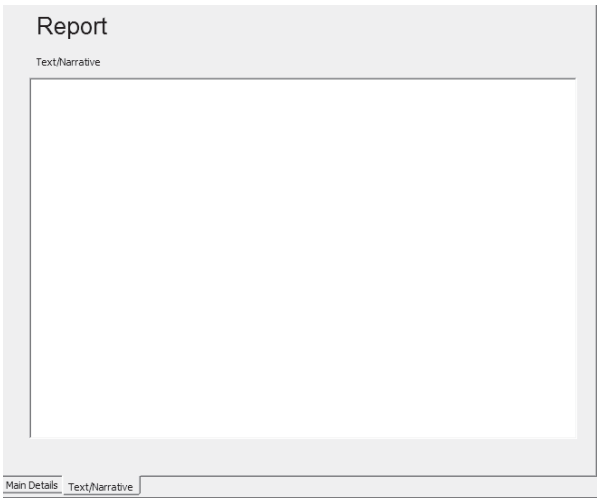

Figure 12. The Text/Narrative field from the SIMS intelligence report

Suggested Format for the Text/Narrative field of the SIMS Intelligence Report

Unfortunately, many SIMS contributors will "cut and paste" information from other police reports directly into their intelligence reports. Although the inserted information may satisfy the elements of reasonable suspicion outlined in 28 CFR, part 23, this format may decrease the intelligence report's utility in terms of value and efficiency and therefore is discouraged. As previously stated, in order for intelligence reports to be useful they should address only one subject or event, should reflect the statements of one source, be carefully sourced, segregate background information from collected intelligence, and guard against careless or inadvertent compromise of sensitive sources and collection methods and strategies. "Cutting and pasting" text from the narrative of other types of police reports inevitably violates these simple rules. Instead, intelligence reports should follow a standardized format that allows for efficient and judicious reporting.

To assist SIMS contributors with presenting information in a format suitable for sharing and analysis, the following format is recommended for use in the **Text/Narrative** field (see Figure 12) of the SIMS intelligence report. This text/narrative format requires contributors to submit brief intelligence entries that involve breaking information into basic elements which allows for efficient reporting, while providing analysts and investigators the ability to scan multiple reports rapidly to find specific information. Formatting a police report into basic elements is not new to the NJSP. Troopers who submit Driving While Under the Influence (DWI) reports also follow a specific format that enables them to better articulate the factors needed to prove a DWI case.

The first element of the text/narrative format is **Activity Type**. Police activities that result in criminal intelligence collection opportunities include, but are not limited to:

- Affidavits/Written Statements/Reports
- Analysis of Evidence
- Field Observations
- Financial Investigation
- Incident/Investigative Review
- Interview/Interrogation
- Police Operation - (ex. Arrest Sweeps, Search Warrant, Arrest Warrant Execution, Deployments, etc.)
- Other - describe
- Physical Surveillance
- Records Checks - (ex. Agency Record Checks; Other Law Enforcement Agency Records; Credit Bureaus; City, County, and State Agencies; Court; Schools; Public Utilities; Employment; Banking and Financial Institutions; telephone; Military; Newspapers, Magazines, and Other Publications; Directories; and Internet Searches)

[9] Frost and Morris, p. III - 5
[10] Ibid., p. III - 10

- Search of a Person/Document Exploitation
- Technical Surveillance
- Witness/Informant Debriefing
- Undercover Operation

(**Note**: Maintaining a standardized format requires that the above activity types be used when reporting criminal intelligence into SIMS)

Figure 13. Reporting format for a SIMS Intelligence Report

The second element of the text/narrative format is **Topic**. Although this field is duplicated from the Topic field in the Main Details section of the SIMS Intelligence Report, it provides analysts and investigators a quick reference to the title of the report they are currently reviewing in the context of the details of the report without having to switch back to the screen with the Main/Details section.

The third element of the text/narrative format is **Event Synopsis**. This field is a summary of the report details. By summarizing historical details that may have preceded the event being reported on, the contributor provides the reader some context of the reporting to follow and may provide a clearer description of the criminal predicate. The Event Synopsis also serves as a bridge for linking the current report with past or future intelligence reports.

The fourth element of the text/narrative format is **Investigators**. This field identifies all operators or analysts that were involved in acquiring the intelligence. At times, this field will only reflect the author of the report; however, there are some activities where intelligence may have been acquired by multiple investigators. For instance, during a physical surveillance or a large operation there may be multiple investigators involved in obtaining the information. As primary investigators transfer or retire it may be useful to speak with others that were involved in acquiring the information. This field assists analysts and investigators with tracking down those who may possess additional knowledge of the event or subjects listed in the report. The field should not be confused with the source of the information, which is documented in the Main Details section of the SIMS Intelligence Report.

The final element of the text/narrative format is **Details**. This field should depict the event being reported, paying attention to the who, what, why, when, and how of the information collected. The details should be presented, carefully paying attention to the perspective of the reader, so the report stands on its own. Again, the narrative should address only one subject or event, should reflect the statements of one source, be carefully sourced, segregate background information from collected intelligence, and guard against careless or inadvertent compromise of sensitive sources and collection methods and strategies.

The intelligence report is the single most important element required for constructing a robust intelligence system. However, the tradecraft involved with mastering intelligence reporting is a learned skill, success at which is dependent on knowledge, experience, and willingness to constantly improve your own efforts. NJSP members who expend the time and effort can hasten this process while developing their own style for meeting the objective of the intelligence report - complete with their own added nuances. Accelerating the pace of learning requires a blend of mentoring and instruction from skilled personnel. Ultimately, the efforts of these dedicated contributors will pay dividends by contributing to a comprehensive strategy aimed at interpreting and thus impacting upon the criminal environment.

Sample Reports using the Text/Narrative Format

The following are sample reports using the text/narrative format for the corresponding activity types that result in criminal intelligence collection opportunities. It is important to note that *reasonable suspicion* is clearly stated in each of the following examples and any information that reflects non-criminal information is marked to reflect identification only data. Also, remember that the following reports outline only the text/narrative field of the SIMS report and do not address other fields or the protocols for creating entities, linking, handling, supervision, or security.

The following example reports are for guidance and are not meant as a strict requirement. However, standardization of the format of the narrative section of the intelligence reports will benefit all members of the NJSP since ILP is a NJSP-wide endeavor, and will result in many more personnel relying upon the use of easily understandable intelligence reports.

*** IMPORTANT ***

a) To satisfy the requirements promulgated by 28 CFR, Part 23, non–criminal identifying information can only be reported in a criminal intelligence database when it is related to the criminal activity of the subject of file. Any non-criminal identifying information that is reflected in a SIMS intelligence report should be clearly marked with the abbreviation (ID only). The contributor need only list the abbreviation once after the first time the entity is mentioned in the narrative of the report. This applies to the names of persons and businesses. For example: JOHN SMITH (ID only), INTERSTATE ENTERPRISES (ID only).

b) To assist the supervisor, investigator or analyst with their interpretation of the intelligence report, respective of the scope of their assignments, all entities that have already been identified within the SIMS criminal intelligence database, because of their association to suspected criminal activity, should be followed with the initials IF, signifying the entity is already "in file." The contributor need only list the abbreviation once after the first time the entity is mentioned in the narrative of the report. For example: JOE SMITH (IF), TWILIGHT ENTERPRISES (IF).

c) It is also helpful to the reader to list a subject's date of birth once he or she is mentioned in the intelligence report. It provides the reader with an additional reference to the subject's identity outside of name only. This can be extremely useful to investigators and analysts that are trying to match a suspect to additional information. For example: JOHN SMITH (DOB: 10/15/1968).

EXAMPLE REPORT 1

Activity Type: Affidavits/Written Statements/Reports
Topic: Marijuana trafficking activities of HAROLD MASON (DOB 00/00/0000).

Event Synopsis: This report provides summary information on an affidavit seeking a Communications Data Warrant to intercept telephone facility number (201) XXX-XXXX, belonging to HAROLD MASON (IF). MASON is suspected of trafficking marijuana from Texas to New Jersey.

Investigators: Det. John Smith and Det. George Jones (NJSP)

Details: HAROLD MASON (IF) is suspected of coordinating the movement of bulk shipments of marijuana between Texas and New Jersey. He is suspected of using his cellular phone (number 201-XXX-XXXX) to manage operations. The attached affidavit is seeking a Communications Data Warrant to intercept MASON's telephone.

EXAMPLE REPORT 2

Activity Type: Analysis of Evidence

Topic: Fetanyl recovered from HUGH JACOBS (DOB: 00/00/0000) linked to US Drug Sales, Cherryhill, NJ.

Event Synopsis: This report provides information received from Forensic Scientist Dean White of the NJSP South Lab related to a recent analysis of heroin seized.

Investigators: N/A

Details: Forensic Scientist Dean White reported that a test of heroin seized from HUGH JACOBS of Gloucester City, NJ, contains derivatives with the same molecular signature as the Fetanyl diverted from US DRUG SALES (ID only) in Cherry Hill, NJ. [partial excerpt from report]

EXAMPLE REPORT 3

Activity Type: Field Observation

Topic: Identification of PETE RICCO (DOB 00/00/0000) as member of THE DISCIPLES motorcycle gang.

Event Synopsis: This report contains information gleaned from a motor vehicle stop that identifies PETE RICCO as a member of the outlaw motorcycle club, THE DISCIPLES (IF). THE DISCIPLES are known to engage in various criminal activities including Murder, Aggravated Assault, Weapons Trafficking, CDS Distribution and Extortion.

Investigators: Tpr. John Smith and Tpr. George Jones

Details: On May 5, 2006, PETE RICCO was stopped on U.S. 206 in Bordentown, NJ, after committing a motor vehicle violation on his Harley Davidson motorcycle, bearing NJ registration AB1234. RICCO was wearing a vest displaying THE DISCIPLES insignia and a 1% logo. While speaking to RICCO about his violation, he admitted that he was en route to Trenton, NJ, to meet a friend he identified as HENRY RIVERS (IF) (DOB: 00/00/0000).

HENRY RIVERS is a known member of THE DISCIPLES motorcycle gang and was last believed to be incarcerated in Florida on state charges related to methamphetamine distribution. RICCO explained that he and RIVERS had opened up a car delivery business out of 126 Burke Street, Trenton, NJ. In the past, THE DISCIPLES motorcycle gang has used this address as their clubhouse.

EXAMPLE REPORT 4

Activity Type: Financial Investigation

Topic: Suspicious activity on PETE JONES (DOB 00/00/0000) related to money laundering and drug trafficking.

Event Synopsis: This report provides information from George Hill (ID only), the Bank Security Officer of National Bank (ID only), Trenton, NJ, regarding the questionable financial activity of PETE JONES.

Investigators: Det. John Smith (NJSP)

Details: On 03/01/2006, PETE JONES of New York, New York, made a cash deposit of $22,970.00, followed by a large cash deposit of $150,000.00 on 03/04/2006 at National Bank in Pennington, New Jersey. Also on 03/04/2006, JONES made payment to an outstanding loan in the amount of $250,000.00. Additional information revealed that the cash deposits smelled like raw marijuana.

The name of the account is:

JONES TEXTILES CO.
775 Walsh Avenue
Trenton, NJ
Work Tel: (609) 882-0000
Residence Tel: (609) 233-0000

EXAMPLE REPORT 5

Activity Type: Incident/Investigative Review

Topic: Armed Robbery of IRVINGTON FRUIT & VEGETABLE WEST INDIAN GROCERY; Irvington, NJ.

Event Synopsis: This report contains information related to an investigation into a robbery/shooting at the IRVINGTON FRUIT & VEGETABLE WEST INDIAN GROCERY (ID only) in Irvington, NJ.

Investigators: Det. John Smith and Tpr. George Jones (NJSP), Det. Connors (Irvington Police)

Details: On January 22, 2005, several suspects robbed the IRVINGTON FRUIT & VEGETABLE WEST INDIAN GROCERY located at 890 18th Avenue, Irvington, New Jersey. Witnesses at the scene stated that five males, three with handguns, and all wearing black ski masks and black army jackets, were the perpetrators. Two patrons in the store sustained gunshot wounds and an additional subject sustained a laceration.

The three injured victims were:
ALDUS BEDEAUX (ID only) (DOB: 00/00/0000)
RONALD BETHANE (ID only) (DOB: 00/00/0000)
MICHAEL ROSCOE (IF) (DOB: 00/00/0000)

During the robbery investigation, detectives observed small glassine envelopes as well as loose marijuana droppings at the scene. The victims all denied any knowledge of marijuana or drug paraphernalia.

The location of the shooting is familiar to the Street Gang North Unit from a past search warrant that was executed at the location on December 23, 2004. The search yielded 78 baggies of cocaine. In addition, the location has been the target of multiple search warrants from other agencies.

(**NOTE**: According to Det. Connors of Irvington Police a confidential source has provided information to the Irvington Police that this location is still being used to distribute cocaine. The source has stated that after being robbed in September 2004, the store installed a buzzer with a locking mechanism on the front door. In addition, the Irvington source revealed that the store's front door and the rear door, which leads to a back room, was reinforced by the storeowners).

EXAMPLE REPORT 6

Activity Type: Interview/Interrogation

Topic: Interview of SAMUAL ADAMS (DOB: 00/00/0000) ref. Paramus car theft;

Event Synopsis: This report contains information related to the interview of SAMUEL ADAMS (IF), a known car thief.

Investigators: Det. John Smith (NJSP) and Det. George Jones (Paramus Police)

Details: On 04/25/2006, SAMUEL ADAMS (IF) was interviewed at the Paramus Police Headquarters, Paramus, NJ, for his suspected role in the theft of a 2006 Toyota Land Cruiser on 04/21/2006.

During the interview, ADAMS implicated FRANK CARICCI (IF) (DOB: 00/00/0000) as leader of a car theft network responsible for stealing cars from northern New Jersey and placing them on cargo ships bound for Dubai. ADAMS claimed that CARICCI employs a network of associates in Port Newark to help facilitate his operations. ADAMS identified CARICCI as the owner of FRANK'S IMPORT/EXPORT 113 Ferry Street, Newark, NJ.

ADAMS admitted to stealing the Toyota Land Cruiser and delivering it to CARICCI's subordinate, a subject named JOHN (no further information).

(Optional) See attached statement.

EXAMPLE REPORT 7

Activity Type: Police Operation

Topic: Arrests of numerous LATIN KINGS street gang members at Meadowbrook Apartments, Paterson, NJ.
Event Synopsis: This report provides information received from Lt. Steve Jacobs, Paterson Police, regarding recent arrests conducted at MEADOWBROOK APARTMENTS (ID only), 11 Main Avenue, Paterson, NJ, an area known to be frequented by the street gang LATIN KINGS (IF).

Investigators: Paterson Police Special Investigations Unit, Det. John Smith (NJSP)

Details: On July 3, 2006, the Paterson Police Special Investigations Unit coordinated a raid of the courtyard of the Meadowbrook Apartments after receiving information that gang members were arming themselves and planning an assault on a rival gang. Lt. Jacobs advised that this area is a known meeting location for the street gang known as the LATIN KINGS (IF). The LATIN KINGS are known to engage in criminal activity including murder, aggravated assault, weapons possession and CDS distribution.

During the raid, several LATIN KING members were identified from their tattoos and statements to the Paterson Police. Among the 20 subjects arrested on weapons, drug, and warrant charges were GEORGE RIVAS (IF) and MARK SMITH (IF), two ranking members of the LATIN KINGS in Paterson.

Attached is a list of subjects who were identified and/or arrested during the police operation.

EXAMPLE REPORT 8

Activity Type: Physical Surveillance

Topic: Surveillance of Genovese associate JOE BLACK (DOB: 00/00/0000).

Event Synopsis: This report contains information regarding a March 15, 2006 surveillance of Genovese Crime Family associate JOE BLACK (IF) meeting with PETE SULLIVAN (DOB: 00/00/0000) to settle on a gambling debt.

Investigators: Det. John Smith (NJSP), Inv. George Jones (Bergen County Prosecutor's Office)

Details: Information was received from the Rockland County District Attorney's Office that Genovese Crime Family associate JOE BLACK (IF) had arranged to meet with PETE SULLIVAN to settle up a $30,000 debt incurred from activities related to an illicit sports betting ring. The meeting took place at the Dunkin Donuts (ID only), 101 Midland Ave., Hackensack, NJ.

A surveillance was conducted at the Dunkin Donuts. BLACK was observed in the parking lot in a 1992 Cadillac bearing NJ registration XXX123, which is registered to BLACK at 123 Mockingbird Rd., River Edge, NJ. SULLIVAN was observed entering the parking lot operating a 2003 Volkswagen bearing

NY registration AAA345 that is registered to SULLIVAN'S wife, MARYANN SULLIVAN (ID only), 32 Ping Rd., Harriman, NY. BLACK entered SULLIVAN'S vehicle where he remained for several minutes, then both BLACK and SULLIVAN departed.

(Optional) See attached surveillance report.

EXAMPLE REPORT 9

Activity Type: Records Checks

Topic: Follow-up report providing ID data on GEORGE TORRES (IF) (DOB 00/00/0000).

Event Synopsis: The following report contains identification data concerning GEORGE TORRES (ID only), son of ANGELO TORRES (IF) (DOB 00/00/0000), a subject suspected of trafficking large quantities of cocaine from Texas to New Jersey.

Investigators: Det. John Smith (NJSP)

Details: A check of the Accurint public record database service conducted on July 16, 2006 revealed a listing for:

George Torres
DOB: 00/00/0000 SSN: 123-45-6789

Associated addresses:
—1234 Blue Way, Lake Worth FL 33467,
Palm Beach County (Apr 2006)
—134 Sun Cir, Wantage Twp NJ 07461,
Sussex County (Sep 2004 – Apr 2006)
—135 Hunters Dock Rd, Yonkers NY 10704,
Westchester Co. (Aug 1998 – Sep 2004)

Torres has a NJ driver's license: T0000 00000 00000
Torres has a New Jersey criminal history, SBI # 000000

EXAMPLE REPORT 10

Activity Type: Search of Person/Document Exploitation

Topic: Documentation found on Anita Robbins (DOB: 00/00/0000) after CDS arrest.

Event Synopsis: This report contains information retrieved from the "pocket litter" of ANITA ROBBINS after she was arrested for trafficking 30 kilograms heroin at the Days Inn (ID only), Newark, NJ.

Investigators: Det. John Smith and Det. George Jones (NJSP)

Details: On June 5, 2006, ANITA ROBBINS was arrested by the Drug Trafficking North Unit for trafficking a significant quantity of heroin. While she was being processed at Newark Station, her personal effects were searched. Numerous business cards and scraps of paper noting names, business names, addresses, and phone numbers were discovered.

Attached is a listing of noteworthy associations she maintained at the time of her arrest.

EXAMPLE REPORT 11

Activity Type: Technical Surveillance

Topic: Telephone conversation of GEORGE BLUE (IF) (DOB 00/00/0000) regarding weapons possession.

Event Synopsis: This report contains information gleaned from a telephone conversation captured during Operation Nine Connect, which is a current ongoing investigation into the criminal activities of the NINE-TREY GANGSTER BLOODS (IF) street gang.

Investigators: Det. John Smith (NJSP). Det. George Brown (NJSP)

Details: On Monday, August 21, 2004, the following conversation between GEORGE BLUE (IF) and an unidentified male was captured during a wire intercept. During the conversation, BLUE refers to the unidentified male as BLACK. BLACK is believed to be MICHAEL CARTER (IF) (DOB 00/00/0000), but this has not been confirmed.

The subject of the conversation was retaliation for a shooting that took place on Saturday, August 19, 2004 at 18th Avenue and Columbia Avenue in Irvington, NJ. In that incident, an unknown assailant shot JACOB ARRINGTON (IF) (DOB: 00/00/0000).

During the conversation between BLUE and BLACK, BLACK stated that he has three "burners" (believe to be code for

guns) stashed at the "Treetop". BLUE stated they would need them by the end of the week. At this time, the location of the "Treetop" is unknown.

EXAMPLE REPORT 12

Activity Type: Undercover Operation

Topic: Drug dealing activities of FESTER DOWD (DOB: 00/00/0000).

Event Synopsis: This report contains information related to the criminal activities of FESTER DOWD (IF), a member of the CRIPS (IF) street gang in Irvington, NJ. The information was received during an undercover operation and is extremely sensitive in nature.

Investigators: Det. John Smith (NJSP)

Details: On July 1, 2006, I met with FESTER DOWD (IF) at the corner of Springfield Avenue and Ellis Avenue, in the City of Irvington. I had contacted DOWD on his cellular phone (908-555-5555, registered to ANNETTE JONES (ID only), Newark, NJ) to arrange a purchase of "crack" cocaine. While meeting with DOWD, we conversed for at least an hour on insignificant issues related to the CRIPS; however, DOWD did express an interest in shooting a subject he named as ANTHONY PEACOCK. DOWD claimed that PEACOCK had been trafficking firearms for him between Georgia and New Jersey. According to DOWD, PEACOCK recently kept five guns for himself after telling DOWD they had been stolen in a rest area on Interstate 95.

No further information was provided by DOWD on the identity of PEACOCK.

EXAMPLE REPORT 13

Activity Type: Witness/Informant Debriefing

Topic: Cocaine distribution by SCOTT JOHNSON (DOB 00/00/0000).

Event Synopsis: This report provides information received from NJSP confidential source I######### regarding the illegal activities of SCOTT JOHNSON (IF).

Investigators: Det. John Smith (NJSP)

Details: On December 1, 2006, NJSP source I######### provided information that SCOTT JOHNSON (IF) is currently soliciting buyers to purchase five kilograms of cocaine. The source alleges that JOHNSON is storing the cocaine in an unknown storage facility in Atlantic City, NJ. The source also alleges that JOHNSON has an additional 16 kilograms of cocaine ordered but could not elaborate on the delivery date. Allegedly, JOHNSON works as an electrician for the television show, *Law and Order*, which is currently filming in New York City. JOHNSON's employment could not be corroborated at this time.

SECTION SIX: Analytical Intelligence Products[11]

A principal feature of intelligence-led policing involves the collection and analysis of information to produce intelligence products necessary for influencing decision-making at the tactical, operational and strategic levels. The NJSP, modeling the Central Intelligence Agency in interpreting its intelligence products, will produce finished intelligence products within the following four categories that relate to a specific temporal framework:

- **Current Intelligence** – addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potentially dangerous situations in the near future. Current intelligence is presented in daily, weekly, and some monthly publications, and frequently in ad hoc memorandums and oral briefings to senior officials.

- **Estimative Intelligence** – deals with what might be or what might happen. Like all types of intelligence, estimative intelligence starts with the available facts, but

[11] Portions of this section are based upon the US Marine Corps' MCWP 2-12 (MAGTF Intelligence Production and Analysis, 2001) and MCWP 2-13 (MAGTF Intelligence Dissemination, 2000) and the Central Intelligence Agency Office of Public Affairs' A Consumer's Guide to Intelligence (Washington, DC: Central Intelligence Agency, 1999).

then migrates into the unknown, even the unknowable. The main roles of estimative intelligence are to help policymakers navigate the gaps between available facts by suggesting alternative patterns into which those facts might fit and to provide informed assessments of the range and likelihood of possible outcomes.

- **Warning Intelligence** – sounds an alarm or gives notice to policymakers. It connotes urgency and implies the potential need for policy action in response.

- **Research Intelligence** – is presented in monographs and in-depth studies. Research underpins both current and estimative intelligence; there are also two specialized subcategories of research intelligence: basic intelligence and intelligence for operational support.

Analytical intelligence products are designed to provide an accurate and useful representation of information that has been analyzed and which represents the analyst's best understanding of the situation. They may be in graphic, written, or oral form and may be as simple as an answer to a question or as complex as an intricate and highly detailed threat assessment that takes into account criminal, demographic, social, and political factors. Although they may be used to produce warnings or to identify opportunities, intelligence products are intended to facilitate planning and decision-making.

Analytical personnel will use finished intelligence products – formal and informal – to disseminate intelligence to their organization's leadership, fellow analysts and operators. The ability to prepare and convey relevant intelligence in a clear, concise manner is an essential skill for analytical personnel.

Regardless of the format, the following considerations should be taken into account when developing any intelligence product:

- **Know your audience.** Is the product for the commander, their staff, or their subordinate commanders? What is their level of knowledge concerning the subject? Does the commander have any personal preferences as to how they receive information?

- **Be sure of the purpose and intent of the product.** Is the product an update on critical events in the last couple of hours (tactical), or is it intended to describe in detail the threat and area of operations prior to planning for an

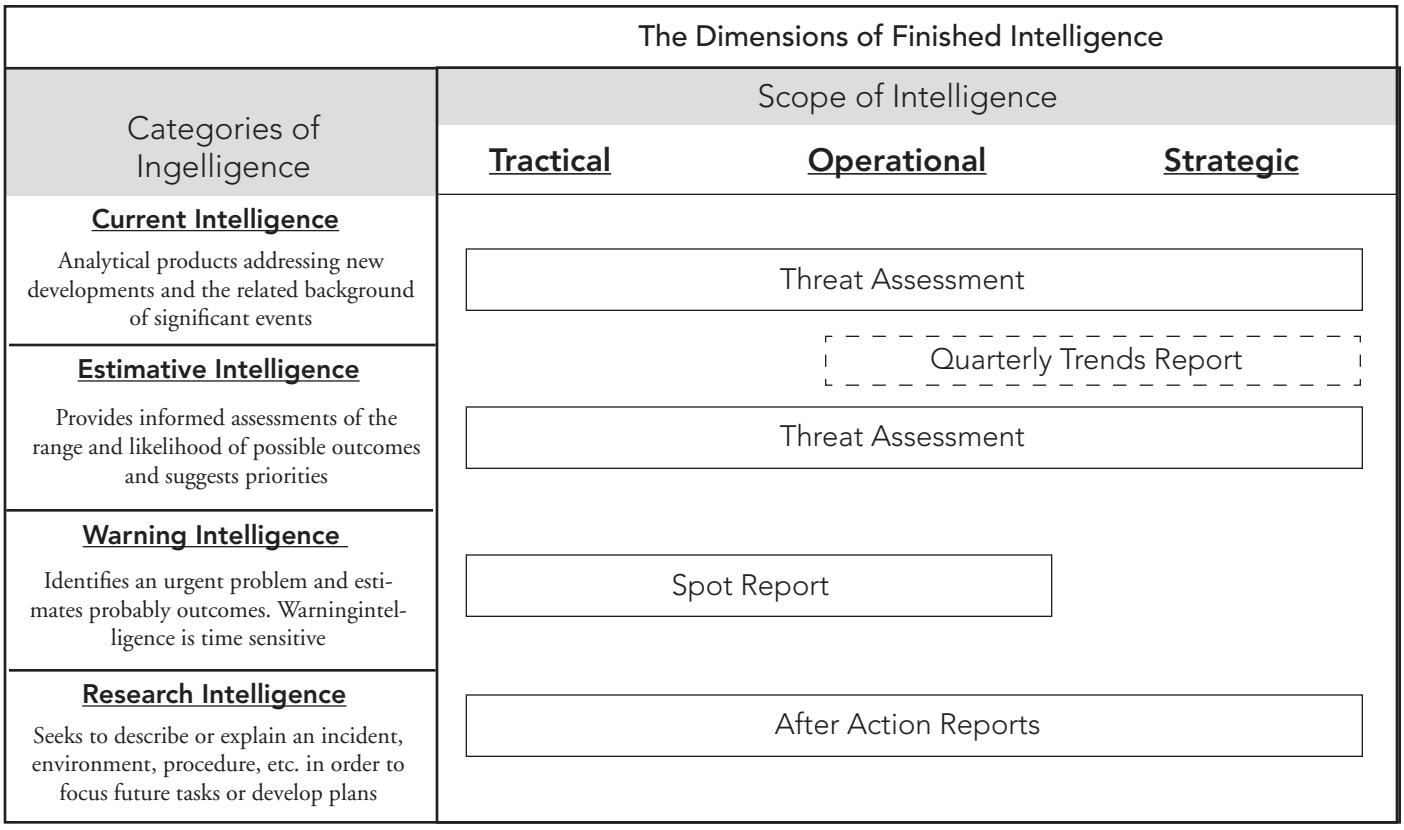

Figure 14. Dimensions of Finished Intelligence

operation (operational), or is it designed to review the state of threat from an overall long-term view (strategic)?

- **Concentrate on essential information and intelligence**, but be prepared to provide details or expanded intelligence should questions arise.

- **Use clear, concise, readable graphics.**

- **Know your information.** If you anticipate questions on subjects where you have little depth, either arrange to collaborate with someone that has that knowledge or take the question for follow-up research. Admit when you do not know something; never make up an answer.

- **Beliefs are not facts.** Always distinguish between what you know (facts), what you do not know (gaps), and what you believe but cannot prove (estimates).

- **Every product should delineate or at least infer its Latest Time Information of Value (LTIV).** This is the time beyond which the information is no longer relevant for NJSP needs.

The types of finished analytical intelligence products include:
- Briefings
- Spot Reports
- Quarterly Trends Reports
- Threat Assessments
- After-Action Reports (AARs)

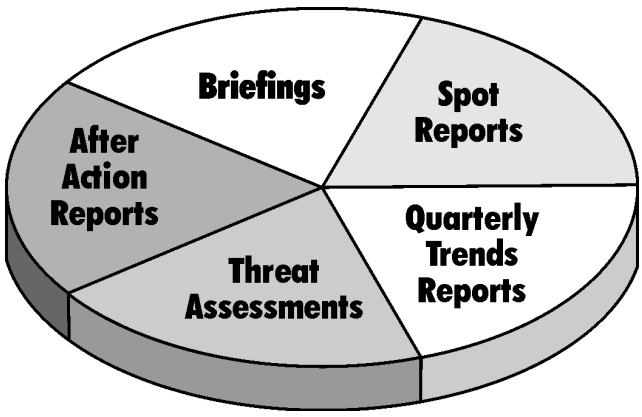

Figure 15. Types of Intelligence Products

Briefings

Briefings are an effective way to disseminate intelligence quickly. They permit direct interaction with the intended audience, and the audience can provide instant feedback to the briefer concerning content, conclusions, and questions or new Operating Directives and Collection Requirements. Briefings are used to convey specific intelligence and intelligence operations details to a select audience in a concise format. Depending on available preparation time, briefing styles can range from formal presentations with detailed handouts and graphics to oral updates. Even in the absence of formal tasking to prepare an intelligence briefing, intelligence personnel informally disseminate intelligence at every opportunity through coordination with staff counterparts and other commands.

Preparation for briefings can be time-consuming in an already time-constrained situation. To convey a large amount of intelligence, supplemental data (in electronic or 'hard-copy' formats) covering key briefing points should accompany the oral presentation. Time constraints, however, may preclude this. Further, briefings usually reach only a limited audience — such as the commander's staff. To compensate for this, analytical personnel are encouraged to prepare concise intelligence summaries in order to more widely disseminate and record critical intelligence presented at the time of briefing.

Types of Briefings

Information Brief - The primary purpose of the information brief is to provide a situation orientation for initial planning and to enhance situational awareness and understanding. Common examples would be a briefing about new trends in criminal activity or a criminal organization that is being considered for investigative targeting.

Decision Brief - A decision brief has the intended purpose of getting a decision from the commander. One example would be a briefing describing the conclusions of an analytical project and requesting a decision from command regarding which, if any, of the recommendations should be carried out.

Confirmation Brief - A confirmation brief is conducted as a final review of a planned action to ensure those participating are certain of the objectives and synchronized with each other. Any significant project or event should generate, at a minimum, a confirmation brief after the work is assigned but before work begins in earnest to ensure confusion and ambiguities are resolved early in the process. Ideally, additional

confirmation briefs should occur periodically to insure all parties involved remain "on track."

Spot Report

A Spot report is used to disseminate important, time critical intelligence without regard to a specific schedule. Spot reports should be prepared and disseminated as rapidly as possible. Generally, each report will concern only a single item. A Spot Report is generally required whenever an event occurs that is likely to result in a change in the disposition of NJSP resources or when a change to the current or future analytical assessment is made. A spot report is also generated when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. Spot reports are focused on priority topics defined by the Commander's Intent. The Spot Report should include an estimate of likely outcomes as well as a source reliability and accuracy evaluation.

FORMAT: SPOT REPORT

Dissemination Restrictions

Date:
Subject:

1) Significant Event(s): Summarize the significant event(s) or developments that initiated the Spot Report. Generally follow the 5Ws (i.e., who, what, where, when, and why) format.

2) Assessment: Estimate the effect of the current activity on threat capabilities or courses of action.

3) Evaluation of Source: State the original information source, and evaluate the accuracy and reliability of that source.

Dissemination Restrictions

Quarterly Trends Report

Quarterly Trends Reports should be produced for areas of emphasis designated by Commander's Intent (such as focus on official corruption, violent street gangs, wholesale narcotics trafficking, or counter-terrorism). Within the NJSP, the Regional Intelligence Groups should produce briefs for each of their regions while the Statewide Intelligence Group will combine the reports and add additional trends or information from the state/national/international perspective. The Quarterly Trends Report (QTR) should include predictions of future activity, identification of intelligence gaps and recommendations (or prioritization) of collection assets. Analysts should consider information not only from their own commander's intent but also the intent of their next higher level of command (i.e. analysts at the bureau level should also look to provide information that would address the intent at the section level).

The Quarterly Trends Report should highlight new information (including Open Source material) that has been collected since the last report. QTRs serve as a quick and effective way to keep Threat Assessments current (see below). The information contained in the QTR should not focus on investigative activities or be construed to be any sort of "case summary." Rather, the QTR should strive to answer previously identified intelligence gaps, describe significant changes to the operating environment and identify and describe events and trends that are applicable to more than a specific group or target(s). For example, is a recent change in legislation going to make it more difficult for criminals to launder money? How are criminal groups moving to adapt and compensate? Is a criminal group branching into new types of criminal activity? The QTR should encompass information gathered from a wide variety of sources including other agencies and open source materials.

FORMAT: QUARTERLY TRENDS REPORT

Dissemination Restrictions

Date:
Subject:
Relevant Commander's Intent:

1) Executive Summary: Brief bullet-point statement of key conclusions.

2) Threat Activities: This section focuses on the characteristics of the criminal organization.

   a. Criminal activities: What new criminal activities have been identified and how are they conducted (modus operandi, or M.O.)? Is there a change in the intensity of previously identified criminal activity?
   b. Changes in M.O.: Is there a change in how previously identified activities are conducted?
   c. Changes in Capabilities: What new skills or resources do the subjects possess? Have law enforcement

activities curbed the subject(s) ability to conduct criminal activity?

d. Changes in Intent: Have the goals of the organization changed or priorities shifted?

e. Other: Any additional information of value could be included here to include rivalries or alliances with other groups, internal power struggles, etc.

3) Operating Environment: The operating environment, by definition, covers a large area. It is therefore impossible to identify every factor that an analyst should include in this section. This section, more than any other, will require the analyst to rely on their tradecraft in identifying factors that may not, at first glance, directly impact upon the actions of criminal groups, yet which may in fact wield significant influence upon them. This section is likely to be the most difficult to complete but is also one of the most important. Analysts will probably find it necessary to get significant input from other analysts and operators in order to complete this.

a. Physical environment: Have there been any changes to the physical environment where the subject(s) operate? Are they expanding to new territory?

b. Social/demographic factors: Is there a change in attitude among the population towards the organization and its members? How is an influx/exodus of a population affecting the criminal environment?

c. Governmental: Is new legislation being enacted that affects a crime type or criminal organization? Are law enforcement agencies using new tactics or strategies?

d. Other: Are the activities of other agencies, Non-Governmental Organizations (NGOs) or other actors affecting the operating environment?

4) Analysis and Discussion

a. Most likely courses of action for criminal group over the next quarter (in order of probability). Also identify any indicators of activity that would confirm or deny specific courses of action among the subject(s).

b. Intelligence Gaps: What is not known? In what area(s) is more information needed? Of what kind?

c. Conclusion: Opportunities for disruption of the organization's activities and recommendations for further intelligence collection.

Dissemination Restrictions

Threat Assessment

A man-made threat is defined as a criminal, criminal organization or crime type which has the potential to do harm to the citizens, institutions, environment or infrastructure of New Jersey. When discussing criminal activities, threat is a combination of the intent and the capability to do harm. Threat assessments dealing with natural hazards are coordinated through the R.O.I.C. and the Emergency Preparedness Bureau.

A threat assessment is essentially a collection of what is known about a specific threat. While most people think of a threat assessment as a profile of a specific criminal group, the term here would also include a description of the threat posed by a type of crime. For example, a threat assessment could describe the production and distribution of methamphetamine. The focus of the assessment would be the dangers posed by methamphetamine distribution, how it is distributed and what future distribution trends are expected instead of focusing on who is conducting the activity. Both types of threat assessment have value depending on what the intended use of the product is. It can be relatively brief (describing the potential threats to a sporting event, for example) or quite lengthy (a detailed description about a specific criminal organization or a regional criminal environment).

FORMAT: THREAT ASSESSMENT

Dissemination Restrictions

Date:
Subject:

1) Origin: Identification of the person who specifically directed the creation of the document, and a statement of the reasons for its production. This explains to "secondary readers" (who don't know the background) why the assessment was undertaken.

2) Scope: Identifies the Bureau/Section Operating Directive that the assessment addresses (how does it tie into the commander's intent?). The boundaries of geographic area, time period, and specific criminal activities covered by the assessment.

3) Key Findings: Brief bullet-point statement of key conclusions that directly address the purposes of the assessment as described in the Origin section. These Key

Findings are drawn from the Threat Characteristics and Outlook sections (described below).

4) Context: A brief description of the current situation that identifies the particular relevance of the threat assessment: why it is being provided at this time.

5) Threat Characteristics: Information organized point-by-point around the key findings, briefly citing the relevant sources. Information from open sources should be blended into this section where appropriate, rather than provided as a separate attachment – divided into descriptions of **Intent** and **Capabilities**. When writing a threat assessment that's focusing on a specific criminal group the following sections should be included:

A. Threat Activities: This section focuses on the characteristics of the criminal organization.
   i. Criminal activities: What new criminal activities are the subject(s) involved in and how do they conduct those activities (their M.O.)? Is there a change in the intensity of previously identified criminal activity?
   ii. Changes in M.O.: Have the subject(s) changed how they conduct previously identified activities?
   iii. Changes in Capabilities: What new skills or resources do the subjects possess? Have law enforcement activities curbed the subject(s) ability to conduct criminal activity?
   iv. Changes in Intent: Have the goals of the organization changed or priorities shifted?
   v. Other: Any additional information of value could be included here to include: rivalries or alliances with other groups, internal power struggles, etc.

B. Targets: This section focuses on specific individuals that make up the organization.
   i. Personal data: Biographical data on new members or new information on existing members.
   ii. Resources: Logistical, Financial, Operational.
   iii. Miscellaneous Data: Any other information of value such as individual priorities that may conflict or support those of the organization.

When writing a threat assessment on a specific crime type, the following sections should be included:

A. Crime context and description
   i. How is the crime typically carried out?
   ii. Who are the primary targets of the crime?
   iii. What are the estimated costs of the crime (in monetary, social and human scales)?
   iv. What vulnerabilities exist that allow the crime to occur/flourish?
   v. What tactics have been used to address the crime and how successful have they been?

B. What criminal groups are involved in this criminal activity?
   i. To what extent are they involved (do they engage in different phases of the criminal process?
   ii. Are there any differences in how criminal groups engage in this criminal activity?

6) Outlook: What future developments are anticipated? Depending on the scope of the assessment, these can be either near-term or longer term developments.

7) Intelligence Gaps: What don't we know? Where do we need more information? Of what kind?

8) Alternate Hypothesis: What other possible explanations/ alternative scenarios should be considered?

9) Information Sources: A brief listing of the information sources used in the assessment.

Dissemination Restrictions

After Action Report (AAR)

The After Action Report provides detailed background about specific events with the intention of highlighting lessons learned that can be applied to future intelligence operations. This is done by describing the events that occurred, their causes and their effects, and by identifying indicators that might be relevant in the future. For example, an examination of the spate of gang shootings that took place in Trenton in April of 2006 could examine: 1) the chain of events that precipitated the shootings, 2) the causes of the eventual ceasefire, 3) the social relationships between the groups and individuals involved, 4) the effects of various responses by law enforcement, civilian community, etc., and 5) physical characteristics of the environment and their effect on events.

It is unlikely that any one individual will have a complete, detailed grasp of all aspects of a specific event. Therefore, a comprehensive AAR should strive to include individuals who were able to observe and participate in the event from many

different perspectives. This can be done either through a group exercise, similar to a brainstorming session, or by individuals preparing comments separately and submitting them to a single point of contact.

FORMAT: AFTER ACTION REPORT

Dissemination Restrictions

Date:
Subject:

1) Origin: Identification of the person who specifically directed the creation of the document, and a statement of the reasons for its production. This explains to "secondary readers" (who don't know the background) why the assessment was undertaken.

2) Scope: The boundaries of geographic area, time period, and specific criminal activities covered by the assessment.

3) Key Findings: Brief bullet-point statement of key conclusions.

4) Description of the event: What was supposed (or expected) to happen and what actually happened?

5) Lessons Learned:
   a. Issue statement: A brief statement of a specific problem or issue that warrants discussion.
   b. Narrative: Brief background of the issue and its significance.
   c. Recommendation: Specific recommendations for future operations.

Dissemination Restrictions

Intelligence Product Review[12]

The term Intelligence Products refers to the finished formal documents, briefings, and other NJSP products that contain finished intelligence analysis and are produced and disseminated by NJSP analysts. These products represent the entire NJSP, and therefore must meet high standards of analytical quality combined with thoughtful presentation. To ensure this goal, all intelligence products should undergo a review process at the level of the analysts' commander or above, although for select products multiple levels of review may be beneficial as it allows for greater insight into issues not readily visible to the intelligence producer. Reviewers must be cognizant that intelligence products are perishable and the review process should be conducted in an expeditious manner. Therefore, both the writers and reviewers of NJSP intelligence products should examine products for the following issues:

Descriptions of the sources and what the reporting says precisely: It matters a great deal whether the source states that an organization is associated with criminal groups or whether the organization has actually committed criminal activities. The analysis must reflect this distinction, even if the analyst believes that the organization is involved with criminal activities. This is so because if intelligence officers are called to explain the analysis, the evidence will only reflect the association, not actual criminal activity, resulting in diminished credibility. It also matters—at least to the audience—whether the source has direct knowledge or indirect knowledge. The rule is simple: the more politically sensitive the subject matter, the greater the requirement for absolute precision, because on a politically charged issue a single piece of uncorroborated information could be used to discredit all analytic work.

Characterizations of the body of evidence: A "majority of the reporting" means a majority, and 60 percent is not "almost every." Furthermore, the review must incorporate a broad range of inputs in order to avoid being too closely tied to any single specific interpretation of the facts.

Analysis of alternate explanations or interpretations of the evidence: An author owes it to the reader to inform him or her when another view exists, especially if that view has a measure of acceptance by other experts. However, the author is not obligated to walk the reader through all of the various interpretations or permutations of the evidence, and there ought to be a presumption that the analyst considered alternate interpretations before arriving at the interpretation presented. Whatever assertions follow the term "intelligence suggests" or "intelligence indicates" is actually often a lead-in for that analyst's favorite pet theory for which there is generally some but not compelling evidence. One of the first questions the reviewer should ask is what else might this development suggest or indicate and why is this theory put forth as the best possibility?

[12] Much of this section is adapted from the article "Making the Analytic Review Process Work" by Martin Petersen and available at http://www.cia.gov/csi/studies/vol49no1/html_files/analytic_review_7.html.

Assertions: The statement that Trenton is the capital of New Jersey is a fact, while a statement that leaders of one criminal organization take a harder line on police informants than another is an assertion — a judgment based on earlier analytic work and evidence not cited. Assertions are necessary; intelligence is not geometry, and analysts have neither the time nor the space to prove every point. However, assertions can be dangerous, too, because too often they are mistaken for facts. Assertions need to be questioned periodically, especially if long held and based on earlier analysis, for they have a tendency to become subconscious assumptions over time.

Definition of assumptions that underpin the analysis: There is no tougher issue to get at, nor one with graver consequences if left unexamined, than identifying key underlying assumptions. Assumptions are different from assertions — assertions are explicit statements, whereas assumptions tend to be implicitly buried within the analysis. The CIA Directorate of Intelligence's work on the fall of the Shah of Iran in the 1970s and Iraq's weapons of mass destruction in the early 2000s share a common characteristic: each was premised on a strong, widely held assumption. In the case of Iran, it was assumed that the Shah was strong and the opposition weak and divided; in the case of Iraq, it was assumed that Saddam Hussein would not allow his stockpiles of chemical and biological weapons to erode. In both instances, the assumptions led analysts to interpret "could be" behavior as "is" behavior. If the analyst and the reviewer cannot articulate the assumptions on which the analysis rests, then they are flying blind. As the results of these examples demonstrate, the consequences can be dire.

Consistency with previous analysis: Often analysis sheds new light on topics, and from time to time analysis based on new facts conflicts with previous analysis. For clarity's sake, if the analysis being put forth is a departure from prior analysis then that must be explicitly acknowledged and explained. Also, if it has been some time since the subject was addressed, caution dictates a quick review of previous work. Over time, caveats and qualifiers are at risk of being dropped or forgotten, especially as different analysts or reviewers become involved.

Identification of key facts and assumptions, changes in which would alter the assessment: For example, variables are the drivers and the causal links in analysis, the "if A, then B" part of the analysis. They are closely tied to the assumptions but generally are more evident. The easiest way to get at the variables is to ask "what if." A change in one of these variables should alter the analysis, and indeed, should help the analyst think through how it might change. Spelling out, discussing, and periodically revisiting what the analyst believes to be the key drivers and shapers of the issue are also the best ways to identify the underlying assumptions.The September 23, 2004 transmittal message to the Duelfer Report on Iraq's weapons of mass destruction discusses hidden assumptions and Saddam Hussein's views and perceptions at length. The report argues that Saddam saw his situation with the United States and Iran very differently than his adversaries did—a different set of causal links, variables, assumptions, and what-ifs. Sometimes the key variable is a strategic perspective, as it may have been in the Saddam case; at other times, it may be more mundane, like whether the railroad system can get the contraband to a port in time to make a sailing date.

In making sure that the all-important review process works, analysts and reviewers share two obligations: do all that they can to create an environment that facilitates an exchange of views and keep the discussion professional and not personalize the issues or get emotional. Beyond these common responsibilities, they each have their own set of responsibilities as delineated in the next section.

SECTION SEVEN: Key NJSP Intelligence Resources

Emergency Preparedness Information Network (EPINet)

The EPINet program features a statewide information-sharing strategy, common information architecture and standards-based technology platform. Collectively these position EPINet to leverage existing systems, develop new capabilities, and to respond quickly to existing and emerging near and long term operational objectives. It is focused on achieving significant advances in information sharing and collaboration. EPINet views communities of interest (COI) throughout the State as members of an extended enterprise. This enterprise perspective is captured in the EPINet Enterprise Architecture (EA) Framework and positions EPINet to effectively foster collaboration and integrate processes, information, systems, and technologies across agencies/jurisdictions at all levels.

An overarching set of operations and systems principles form the basis for the EPINet EA Framework. The framework is designed to unify and govern the four related EPINet architectures:·

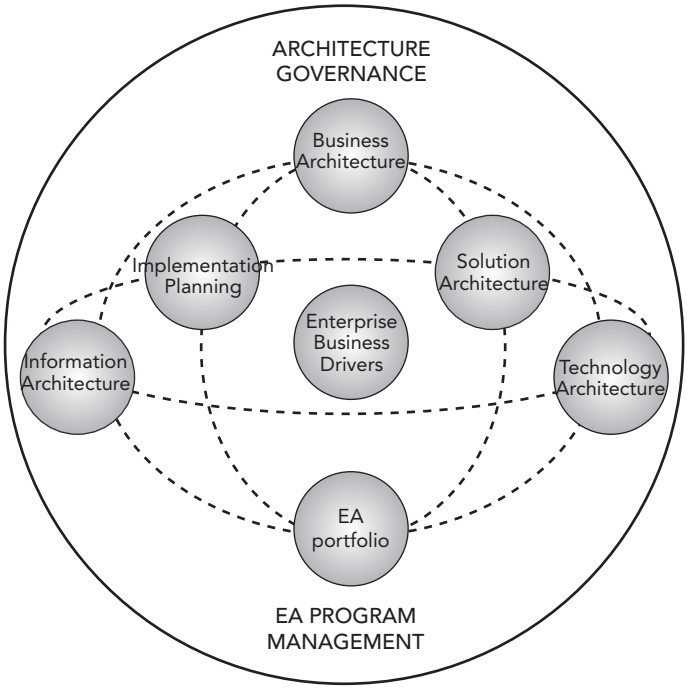

Figure 16. Enterprise Architecture Framework

- Business Architecture·
- Information Architecture·
- Technology Architecture·
- Solution Architecture.

It is important to recognize and manage the inter-dependencies between these four architectures. As the EPINet program matures and EPINet is enhanced in response to internal and external forces, these architectures will likewise evolve through a process of Architecture Governance.

The EPINet Information Architecture fuses data from multiple, disparate sources into a single cohesive system. EPINet's "build it once – use it many times" philosophy, enabled by an enterprise commitment to service-oriented architecture and role-based delivery of services, will help eliminate information and technology silos.

The EPINet program leverages the maximum potential from existing systems and initiatives while leaving the basic purpose and structure of each component system intact. EPINet also promotes and sponsors an evolutionary, rather than revolutionary, approach that provides incremental improvements to the system and its component subsystems, within a greater enterprise strategy. In systems engineering terms, this is referred to as spiral development. Existing capabilities are improved and new capabilities are realized without having to wait months or years for traditional engineering processes to be executed. Incremental improvements are implemented based on defined requirements. Lessons are learned, new requirements identified, and further improvements are made to the system.

The Statewide Intelligence Management System (SIMS)

The Statewide Intelligence Management System (SIMS) is a state-of-the-art computerized intelligence/information management system currently offered to every law enforcement agency in New Jersey as a means to provide timely access to criminal intelligence and other law enforcement sensitive information. SIMS consists of several distinct components: an intelligence repository, a terrorism tips/leads management system, and an information gateway to law enforcement sensitive resources or systems which are not governed by federal guidelines pertaining to the collection, storage, maintenance and dissemination of intelligence systems. The NJSP SIMS Unit administers SIMS, and is the official custodian of all State Police intelligence reports and the database that stores them. It also markets, trains, audits, and ensures compliance within SIMS. The unit ensures the physical security and overall integrity of the criminal intelligence files and enforces current access and dissemination policies. It enforces the policies and procedures for the entry, modification, purge, and audit of the data contained in the intelligence repository in accordance with established agency, state, and federal guidelines. SIMS users and their corresponding agencies are provided with training, system protocols, policies and user agreements, all of which ensure compliance with *Title 28 Code of Federal Regulations, Part 23 and Attorney General Guidelines on the Collection, Handling, and Dissemination of Intelligence in New Jersey.*

Criminal Intelligence Component

With regard to the criminal intelligence repository component, SIMS permits law enforcement personnel throughout New Jersey to store and share criminal intelligence concerning the identities, operating methods, and distinguishing characteristics of criminal suspects active in the region. Trained SIMS users can query and contribute information on suspected involvement in all types of organized criminal activity, including street gangs, outlaw motorcycle gangs, narcotics sets, terrorists, and traditional and non-traditional organized crime groups. Intelligence related to organized criminal groups operating in New Jersey, or information relating to criminal activity that is

serial or multi-jurisdictional, may be entered into the criminal intelligence component of SIMS.

SIMS serves as a vital hub for sharing criminal intelligence, because each piece of intelligence in SIMS can be made available to users from outside law enforcement agencies. SIMS allows agencies to store intelligence for their own use or for the benefit of the broader law enforcement community. Security features in SIMS enable the user agency to decide who can view the information they contribute. Highly-sensitive intelligence can be concealed from general view, for example, and restricted to those whose roles and assignments require it, while criminal intelligence that is not sensitive can be shared with users who have the need and right to know the information.

The New Jersey Department of Law & Public Safety has adopted SIMS as the criminal intelligence management database for all investigative personnel assigned to the Department, thereby creating a central repository for criminal intelligence that is available to local, county, state and federal law enforcement agencies that are participants in the SIMS initiative.

Tips/Leads

In 2002, SIMS incorporated a tip reporting and lead management process that tracks the progress of a terrorist-related tip or lead from its initial entry into the system to its final disposition. In November 2003, Attorney General Peter Harvey issued a mandate requiring all local, county and state agencies to enter terrorist related tips and leads into this section of SIMS. The process of tracking tips and leads related to potential terrorist activity serves as an early warning system to protect New Jersey from potential terrorist activity. Planning is underway to expand the tips/leads component of SIMS to manage lead information related to crime and man-made and natural disasters.

Information Gateway

At the time of this writing, the information gateway portion of SIMS is still under development, with several resources being considered for inclusion in SIMS that are non criminal intelligence systems, and therefore not governed by the requirements of Title 28 Code of Federal Regulation, Part 23. These resources, such as the State Police Records Management System and State Police initiatives (corporate outreach and maritime security), are valuable sources of information. The benefit of incorporating these systems into the SIMS platform is that the query technology can essentially link all databases for the user.

SECTION EIGHT: Conclusion

In the era of Homeland Security, data collection and intelligence analysis are vital components for ensuring appropriate planning and resource allocation that supports the police, emergency responders, and private sector as they collectively strive to prevent, deter and respond to crime, terrorist attacks, and man-made or natural disasters. The National Strategy of Homeland Security lists "Intelligence and Warning" as a critical mission area that focuses mainly on preventing terrorist attacks.[13] Significantly, for domestic law enforcement, reducing the scourge of violent crime in areas across the State requires the same forewarning dedicated to counter-terrorism operations.

In the era of Homeland Security, data collection and intelligence analysis are vital components for ensuring appropriate planning and resource allocation that supports the police, emergency responders, and private sector.

Intelligence-led Policing is a management philosophy supporting optimal resource allocation based on improved awareness and understanding of the operating environment. The New Jersey State Police is aggressively implementing Intelligence-led Policing in order to create better situational awareness at all levels – tactical, operational and strategic – and to enable optimum representation of the immediate and longer-term operational environment through analytical products capable of being immediately used by its consumers: the law enforcement, public safety and the private sector communities. Historically, in the United States only the military, the national security Intelligence Community, and certain specialized law enforcement units have applied intelligence operations to their strategic planning and daily operations. However,

[13] George W. Bush, National Strategy for Homeland Security (Washington, DC: Office of the White House, 2002).

with the increasing sophistication of those who operate outside the law, all participants in today's Homeland Security efforts must use intelligence to create situational awareness and drive appropriate activities. By adapting data collection and intelligence control systems employed by traditional practitioners while ensuring all legitimate citizen privacy issues are addressed, NJSP members can leverage all the information that is learned before, during, and after an event in meeting the challenges facing the NJSP.

This practical guide provides a reference manual defining ILP within the NJSP. It is aimed at achieving better situational awareness through the collection of data and the creation, dissemination, and cataloguing of intelligence products. These products will drive strategic decision-making and structured resource allocation to enable the NJSP to appropriately meet current and future challenges. This guide also defines the processes associated with intelligence that will be incorporated into NJSP-wide crime prevention and emergency management strategies. The primary aspect of this process is bounded by the need to achieve a common understanding of the operating environment, a task that is achieved through the combined efforts of the NJSP's formal Intelligence Cycle and the ROIC's real-time situational awareness efforts.

The adoption of ILP requires sustained effort by NJSP senior leaders, operators, and analysts. For the senior leadership it means actively engaging operators and analysts to ensure the leadership has a sufficient picture of the operating environment and that it can act to distribute resources according to conclusions and priorities drawn from this understanding. For operators, it requires becoming both better data collectors and better consumers of intelligence related products. This means shifting from emphasizing post-event evidence collection to constantly gathering all relevant data and ensuring it is provided for entry into appropriate databases, as well as drawing from the intelligence analysts and relevant databases all the information that is needed to support ongoing operations. For analysts, the key components of this process include the creation of tactical, operational and strategic intelligence products that support immediate needs, promote situational awareness, and provide the foundation for longer-term planning.

The process of implementing ILP is well under way, but it will not succeed without the dedicated participation of all members of the NJSP. The realignment of existing command structures in order to be able to respond more rapidly to emerging operational requirements has in large measure been completed. The process for adopting a formalized information and intelligence cycle has been laid out in the pages of this manual and work has begun to craft the initial series of products to support focused intelligence collection by all members of the NJSP, especially Troopers, Detectives and Analysts. Finally, the new Regional Operations and Intelligence Center has opened its doors and aligned its processes in order to better address watch operations, tactical intelligence analysis, and asset management and coordination. Together, these three facets of the NJSP's ILP implementation mark the tipping point in a new era of law enforcement, one in which the law enforcement community adopts a more advanced approach to not just being first responders for crime and terrorism, but instead becoming *first preventers*.

BIBLIOGRAPHY

Audit Commission. *Helping with Enquiries: Tackling Crime Effectively.* London: Audit Commission, 1993.

Central Intelligence Agency (Office of Public Affairs). *A Consumer's Guide To Intelligence, Gaining Knowledge and Foreknowledge of the World Around Us*. Washington, D.C.: Central Intelligence Agency, 1999.

Clark, RM. "Intelligence Analysis: A Target-Centric Approach." CQ Press, 2004.

Dannels, David, and Heather Smith. "Implementation Challenges of Intelligence Led Policing in a Quasi-Rural County." *Journal of Crime & Justice* 24, no. 2 (2001): 103.

Frost, Charles and Jack Morris. *Police Intelligence Reports: A Compendium on Police Intelligence Reporting Formats and Procedures*. Orangevale, California: Palmer Enterprises, 1983.

Guidetti, R. *Policing the Homeland: Choosing the Intelligent Option*. Master's of Arts in Security Studies ed. Monterey, CA: Naval Postgraduate School, 2006.

Heaton, Robert. "The Prospects for Intelligence-Led Policing: Some Historical and Quantitative Considerations." *Policing and Society* 9, no. 4 (2000): 337-356.

Heuer, R. "The Psychology of Intelligence Analysis." in Center for the study of intelligence, Central Intelligence Agency [database online]. Washington, D.C. [cited 2006]. Available from https://www.cia.gov/csi/books/19104/index.html.

Kedzior, Richard. "A Modern Management Tool for Police Administrators: Strategic Intelligence Analysis." *Criminal Intelligence Service Ontario* (January 1995): 1-13.

Maguire, M., and T. John. "Intelligence, Surveillance, and Informants: Integrated Approaches." *Police Research Group Crime and Prevention Seriesno*. Paper No. 64 (1995).

Maguire, Mike. "Policing by Risks and Targets: Some Dimensions and Implications of Intelligence-Led Crime Control." *Policing and Society*, 9 (1999): 315-336.

National Commission on Terrorist Attacks Upon the United States. *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York, NY: W.W. Norton & Company, 2004.

NJSP Investigations Branch. *Confronting the Investigative Challenges of the Homeland Security Era: Reorganizing the NJSP Investigations Branch*, 2005.

Patterson, ES, et.al. *Aiding the Intelligence Analyst in Situations of Data Overload: A Simulation Study of Computer-Supported Inferential Analysis Under Data Overload*. Ohio State University: Institute for Ergonomics/Cognitive Systems Engineering Laboratory, 1999.

Perry, Simon. *Police Intelligence Lecture Presented at the Suicide Bomber Seminar*. Princeton University, Princeton, NJ ed. Princeton, NJ: Jewish Institute of National Security Affairs, 2004.

Peterson, Marilyn. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, 2005.

Peterson, Martin. "Making the Analytic Review Process Work." *CIA Studies in Intelligence*, 49(1), 2005.

Ratcliffe, J., ed. *Strategic Thinking in Criminal Intelligence*. Sydney, Australia: The Federation Press, 2004.

Ratcliffe, J. H. "The Effectiveness of Police Intelligence Management: A New Zealand Case Study." *Police Practice and Research*, in Press.

Ratcliffe, Jerry H. "Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice." *Policing and Society* 12, (2002): 53-66.

United States Department of Justice. "28 CFR Part 23, Criminal Intelligence Operating Policies." Washington, D.C. [cited 2006]. Available from www.it.ojp.gov/process_links.jsp?link_id=5377.

White, Nathan R. *Defending the Homeland Domestic Intelligence*, Law Enforcement, and Security. Edited by Sabra Horne and Dawn Mesa. Belmont, CA: Wadsworth/Thomson Learning, 2004.

MANHATTAN INSTITUTE FOR POLICY RESEARCH

52 Vanderbilt Avenue • New York, N.Y. 10017

www.cpt-mi.org