U.S. DEPARTMENT OF ENERGY

PNNL-20314

Prepared for the U.S. Department of Energy

under Contract DE-AC05-76RL01830

Law Enforcement Technology Roadmap:

Lessons to Date from the Northwest Technology desk and the Northwest FADE Pilots

CL West
SJ Kreyling

April 2011

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandra, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/from.aspx>
Online ordering: http://www.ntis.gov

PNNL-20314

Law Enforcement Technology Roadmap:

Lessons to Date from the Northwest Technology desk and the Northwest FADE

CL West
SJ Kreyling

April 2011

Prepared for
The U.S. Department of Energy
Under Contract DE-AC05-76RL01830

Pacific Northwest Laboratory
Richland, Washington 99352

Contents

Acknowledgements

I would like to personally thank the following people and organizations for their support and trust in developing this program. They have provided me open access to their organizations and their inner workings on a daily basis, taken me on a host of ride-alongs and operations, endured an endless set of questions, and generally adopted me within their organizations as a trusted member of their profession. This report would not be possible without them, their professionalism, and their dedication to an often difficult and thankless job.

Seattle Police Department	King County Sheriff's Department
Seattle Police Criminal Intelligence Section	King County Sheriff Regional Intelligence Group
Seattle Police Vice and High Risk Victims Unit	Seattle Police Gang Unit
Auburn Police Department	Port of Seattle Police
Seattle Police ICAC Unit	King County, Department of Adult & Juvenile Detention
U.S. Marshals Service	Federal Bureau of Prisons
Kent Police Department	Federal Way Police Department
Washington State Fusion Center	US Dept. of Veterans Affairs Law Enforcement Division
U.S. Immigrations and Customs Enforcement – Homeland Security Investigations	Federal Bureau of Investigation
Bellevue Police Department	Tukwila Police Department
Washington State Patrol	

My special thanks to the following individuals:

Sgt. Steve Davis, King County Sheriff	Sgt. Ryan Long, Seattle Police Department	Lt. Eric Barden, Seattle Police Department
Sheila Hatch, King County Sheriff Gang Analyst	Sue Dailey, Seattle Police Department	Det. Monty Moss, Seattle Police Department
Sgt. Jim Dyment, Seattle Police Department	Det. Brian Palmer, King County Sheriff	Det. Malcolm Chang, King County Sheriff
Lt. Eric Sano, Seattle Police Department	Det. Laura Hoffenbacker, King County Sheriff	Crystal Byelick, Social Security Administration, Office of the Inspector General, Criminal Research Specialist
Officer Brian O'Neill, Auburn Police Department	Agent Aaron Reynolds, ICE HSI	Det. Tim Renihan, Seattle Police Department
Sgt. Tom Mahaffey, Seattle Police Department	Agent Todd Rignel, ICE HSI	Keith Evans, U.S. Bureau of Prisons
Raymond F. Fleck Supervisory Deputy United States Marshals Service	Sgt. Brad Thomas, Seattle Police Department	Sgt. Catey Hicks, King County, Department of Adult & Juvenile Detention *Special Investigations Unit*
Det. Josh Landers, Port of Seattle	Tim Ensley, ICE HSI SAC Seattle	Sgt. Barclay Pierson, King County, Department of Adult & Juvenile Detention *Special Investigations Unit*
Ye-Ting Woo, Assistant United States Attorney	Lt. Ron Leavell, Seattle Police Department	Jenifer Lopez ICAC Program Analyst
Det. Ian Polhemus, Seattle Police Department	Doug Larm, Washington State Fusion Center	Det. Garry Jackson, Seattle Police Department
King County Sheriff Sue Rahr	Seattle Police Assistant Chief Paul McDonagh	Sgt. Verner O'Quin, Seattle Police Department

A special thanks to all the Information Technology professionals at the Seattle Police Department and the King County Sheriff's Office.

Executive Summary

The goal of this report is to provide insight into the information technology needs of law enforcement based on first hand observations as an embedded and active participant over the course of two plus years. This report is intended as a preliminary roadmap for technology and project investment that will benefit the entire law enforcement community nationwide. Some recommendations are immediate and have more of an engineering flavor, while others are longer term and will require research and development to solve.

Some of the opinions in this report are controversial, indeed inflammatory in some circles both inside and outside of law enforcement. They are presented to provide context for technology investment, development, integration, and deployment projects – a roadmap to promote dialog. There are no simple solutions and no fingers need be pointed – but the issues are real. If you are developing technology for law enforcement, they must be considered.

Law enforcement is on the front lines of the war on terrorism; the ways and means of terrorism occur at the street level via the day-to-day activities of organized criminal entities. Money, supplies, transportation, weapons, and information are all available and actively facilitated by these organizations. Crime and terrorism are intertwined and sometimes hard to distinguish. Organized crime - street gangs, traditional mafia, outlaw motorcycle gangs, militias, human traffickers, drug cartels – each has a traditional criminal focus on making money accompanied with varying degrees of focus on ideological, social and political issues – the more ideological, the more terrorist-like. Many of these organizations have an international network and presence with cross-border capabilities in a number of domains. Like terrorist groups, they can act as state and non-state proxies in international conflicts where direct confrontation with stronger opponents is to be avoided[i]. Where these organizations dominate, regions of lawlessness are common. These "black spots" are defined as physical areas that are outside of effective governmental control. Black spots are dominated by alternative, mostly illicit, authority structures (criminals, warlords, terrorist organizations), and are capable of breeding and exporting insecurity (e.g., illicit drugs, conventional weapons, weapons of mass destruction, terrorist operatives, illicit financial flows, strategic/sensitive know-how) to faraway locations.[ii,iii] There are blacks spots within the continental United States. Organized criminal networks also require and are fully integrated within licit regions as part of their on-going activities.

Ideology is the key differentiator between organized crime and terrorism. Tools and techniques applied and successful with one will generally be effective against the other. Technology designed to address child pornography networks and their hidden communications or to analyze the overall market for prostitution based on open source data have direct analogues in the counter-terrorism world. Investment in this arena benefits both sectors and is consistent with four of the five DHS missions listed in the Quadrennial Homeland Security Review[iv]:

- Mission 1: Preventing Terrorism and Enhancing Security
    - Goal 1.1: Prevent Terrorist Attacks

    - Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
    - Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events
- Mission 2: Securing and Managing Our Borders
    - Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
    - Goal 2.2: Safeguard Lawful Trade and Travel
    - Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations
- Mission 3: Enforcing and Administering Our Immigration Laws
    - Goal 3.1: Strengthen and Effectively Administer the Immigration System
    - Goal 3.2: Prevent Unlawful Immigration
- Mission 4: Safeguarding and Securing Cyberspace
    - Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
    - Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Criminal intelligence is the law enforcement answer to organized crime. Much of the work of this program has been with criminal intelligence and its use within the law enforcement community. This is where many of the most difficult technical problems lie and this is where the nexus with terrorism is the strongest. This is where "the good stuff" shows up; raw data that can *make dots worth connecting* comes here first. In short, this is where technology can have the greatest leverage.

It is worth noting that most traditional law enforcement data is historical in nature. Only c*riminal intelligence has the ability to look forward at data that has not yet met the metric of reasonable suspicion*. For this reason, it is also primary to intelligence-led policing strategies.

The report is organized by technology themes and issues with observations, issues, and recommendations within each section. The major topics covered include:

- General and cultural
- Digital forensics and cyber
- Video
- Open Source and Social Media Data
- Federated search of existing law enforcement information sources
- Management and sharing of criminal intelligence
- Mobile devices
- Cross jurisdictional and large scale analysis
- Privacy

Each of these is an area of particular need – some represent whole families of potential projects. Many would be recognized by the community while others are observations based on emerging trends.

Why Focus on Law Enforcement?

This work is important to the DHS mission, because law enforcement is on the front lines of the war on terrorism. The ways and means of terrorism occur at the street level via the day-to-day activities of organized criminal entities. Money, supplies, transportation, weapons, and information are all available and actively facilitated by these organizations. Crime and terrorism are intertwined and sometimes hard to distinguish. Organized crime - street gangs, traditional mafia, outlaw motorcycle gangs, militias, human traffickers, drug cartels - each variant has a traditional criminal focus on making money with a varying focus on ideological, social and political issues – the more ideological, the more terrorist-like. Organized crime can be defined as having the following attributes[v]:

- Structure
- Restricted membership
- Continuity
- Violence or the threat of violence
- Illegal enterprises
- Legitimate business penetration
- Corruption

Given that ideology is the only critical differentiator between organized crime and terrorism, tools and techniques applied successfully with one will generally be effective against the other. Technology designed to address child pornography networks and their hidden communications or to analyze the overall market for prostitution based on open source data have direct analogues in the counter-terrorism world. Investment in this arena benefits both sectors and is consistent with four of the five DHS missions[vi].

Many organized criminal groups have an international reach with cross-border capabilities in a number of domains. While their on-going activities are fully integrated into everyday American life, like terrorist groups, they can act as state and non-state proxies in international conflicts where direct confrontation with stronger opponents is to be avoided[vii]. Where these organizations dominate, regions of lawlessness are common. These "black spots" are defined as physical areas that are outside of effective governmental control. Black Spots are dominated by alternative, mostly illicit, authority structures (criminals, warlords, terrorist organizations), and are capable of breeding and exporting insecurity (e.g., illicit drugs, conventional weapons, weapons of mass destruction, terrorist operatives, illicit financial flows, strategic/sensitive know-how) to faraway locations.[viii,ix] There are blacks spots within the continental United States.

At the same time, organized criminal groups still operate in places where there is effective government control – not just in "black spots." In the context of examining either organized criminal groups or terrorist organizations, the nature and methods of illicit trafficking can be illustrative. The problem of trafficking is hardly a new one; illicit trade has always existed. What is new, however, is the ease and speed (due to global transportation, global communication and global awareness) in which this trade

can occur, and thus, its heightened profitability – particularly for organized criminal entities.[x] With globalization, there is increased tension between governments attempting to control their borders and those in search of amplified rewards who are prepared to break the rules. This creates opportunities and pressures for all of these agents (criminal, state, terrorist) to tolerate, co-opt, and in some cases support each other in pursuit of a wide variety of goals.[xi] We see both capability and motive driving agents to work together.

It is worth noting that illicit trade is not just about crime and money. "It is true that criminal activities surged and became global in the 1990s. But thinking about international illicit trade as just another manifestation of criminal behavior misses a larger, more consequential point. Global criminal activities are transforming the international system, upending the rules, creating new players, and reconfiguring power in international politics and economics."[xii] Terrorism, crime, and the state are not always so easy to discern. This makes the work of chasing organized crime all the more complex.

What is Criminal Intelligence?

Criminal intelligence is the law enforcement answer to organized crime. Driven by the rise of organized crime in America, criminal intelligence has been defined and regulated by a number of federal laws, including the Omnibus Crime Control and Safe Streets Act of 1968 and most importantly CFR 28 part 23 (*28 CFR Part 23 CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Executive Order 12291 1998 Policy Clarification 1993 Revision and Commentary*).

> § 23.1 Purpose. The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968 … are utilized in conformance with the privacy and constitutional rights of individuals.
>
> § 23.2 Background. It is recognized that certain criminal activities, including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for federally funded projects are required.

The Association of Law Enforcement Intelligence Units (LEIU) is the organization most closely aligned with criminal intelligence and promoting its proper use within law enforcement. Its mission is "*providing leadership and promoting professionalism in the criminal intelligence community in order to protect public safety and constitutional rights. LEIU was founded in 1956 and subsequently established criminal intelligence standards that are recognized by both law enforcement and civil libertarians as creating a proper balance between the needs of law enforcement and the constitutional privacy rights of individuals*." The LEIU guidelines for criminal intelligence along with the applicable federal laws provide a framework for using this class of data. LEIU's guidelines are widely supported outside of law enforcement as an essential balance between individual privacy and public need.

Our program focused on criminal intelligence and its use within the law enforcement community. This is where the most difficult technical problems lie and where the nexus with terrorism is the strongest. This is where "the good stuff" shows up; raw data that can *make dots worth connecting* comes here first. Often criminal intelligence is housed within a specific law enforcement unit, but this is not always the case, sometimes a specific unit or whole department has need for its own data that still have to be managed to the same standards. Criminal intelligence units also tend to house the "technical units" of police departments –supporting such activities as video surveillance, wire tapping, and other technical activities.

Overview of Criminal Intelligence file types/phases[xiii]:

- Pre-reasonable suspicion
  - Kept separate from normal intelligence files
  - Factual based profiling is ok to determine reasonable suspicion
  - LEIU Guidelines
  - Working/developmental file can be kept for 1 year
- Post Reasonable Suspicion
  - Kept separate from normal police files
  - Most often associated with individual privacy
  - This is where intelligence files on people are usually kept
  - Maintenance and dissemination issues
  - Destruction issues
  - 28 CFR key here – rules and regulations that govern the creation, maintenance, dissemination, and destruction of Intel files
- Normal police files

It is worth noting that most traditional law enforcement data is historical in nature – Computer aided dispatch (CAD - 911 calls), record management systems (police reports and investigations), etc. ***Only criminal intelligence has the ability to look forward at data that is not yet met the metric of reasonable suspicion***. Suspicious activity reports, hunches, oddities, "bad smells", can be factually investigated and data collected to assess reasonable suspicion. ***Criminal intelligence is also the place for non-case specific topical analysis***. Taking this step back and having a bigger picture view is the hallmark of good criminal intelligence and the basis for intelligence-lead policing. Without it, law enforcement is left in a continuously reactive state. Efforts to improve criminal intelligence have a direct and lasting impact on counter-terrorism efforts as well as supporting community specific needs.

Structure of the Program

Northwest Technology Desk

The Northwest Regional Technology Desk was set up to provide the following:

- Embedded observer (following our Human Centered Analytics approach)
  - Gather requirements and needs

    - Develop relationships working directly with law enforcement
    - Full access to data and inner workings
- Technology liaison and assistance
    - Reach-back to the laboratory system on specific topics
    - Unbiased advice on technology
    - Technical resource for case specific issues

The Technology Desk has been a primary means of gaining perspective on the needs of law enforcement. This program has allowed me to provide a unique persistent presence within the community – providing direct and immediate assistance on real technical issues. At the same time, the embedded nature of the work allows observations over time that a one-time meeting or ride-along cannot provide. Being a standard fixture of the daily routine provides a gateway to the real problems, opinions, and on-going needs of a team or unit.

Northwest FADE Pilots

The Northwest FADE Pilots were conceived as a method to evaluate the FADE tool suite (Fused Analytic Desktop Environment) for use in managing, sharing and analyzing criminal intelligence around selected organizations in the Puget Sound region.

The analysis of criminal intelligence is not so different than analysis within the intelligence community. FADE was originally designed for all source intelligence analysts working in the intelligence community. Ease of use, scalable, heterogeneous - mostly document centric data, ad hoc use of various analytical techniques and tools – these are the requirements the FADE suite of tools was designed to address. It was built specifically with an architecture that could be customized, added to and otherwise tailored to a specific domain. Traditional visualization and analytical tools have often proven unpopular with analysts due to their steep learning curves and rigidity in daily use on common real world data. FADE was designed specifically to address these concerns and provide an environment to ease both data and analyst into more productive states.

The initial goal was to deploy the software and get it up and running for use within the community. Training of key users and development of minor enhancements were also targeted for the first 18 months. On-going feedback was to be collected and fed back to this report and to the development teams for product enhancement. Subsequent years are planned to expand the pilot to more agencies in the region and develop the technical means to share criminal intelligence with a regional focus.

Feedback from the FADE Pilots

We deployed FADE within three local agencies to get feedback on its usefulness and what kinds of changes would be desired to make it more applicable to their mission. Currently it is running within the Seattle Police Department's Criminal Intelligence Section, the King County Sheriff's Regional Intelligence Group (RIG), and the Auburn Police Department's Gang/Intelligence Unit.

FADE has allowed these agencies to manage, access, and search their criminal intelligence separate from their regular police data. Street gang, outlaw motorcycle gang, traditional organized crime, and counter

terrorism are the most common topics stored in the system. Street gang data in particular has been popular and consistent across all the organizations – having a locally focused database of regional criminals is proving useful.

The biggest request from FADE users is to have a system that empowers the local entity to manage its own criminal intelligence to its policies and standards while allowing sharing when appropriate. The system documents when and with whom a given file was shared.

We have added the following changes to FADE based on on-going feedback:

- Gang database – this is a structured database within the FADE system which allows the user to store "gang card" information alongside traditional unstructured information - documents such as bulletins, pictures, surveillance recordings, etc. The entire database can be quickly exported to an MS Excel format to facilitate statistics, export to other systems, or analysis via another tool. This is in the process of being rolled out.

- Tag and timer for criminal intelligence – any file within the FADE system can be tagged as criminal intelligence. This visually marks the file and also begins a timer based on the category of the file. The categories and time frames can be configured for each organization. When the time frame is almost up, a notification is sent to a set of designated users allowing them to either reset the timer based on new information or delete the file. This makes it easier to actually implement the LEIU guidelines and provides stronger documentation.

- Miscellaneous bug fixes and minor changes

The next step is to develop a mechanism to allow individual files or gang member records to be shared from one FADE implementation to another in a secured manner. There is also interest in the ability to export elements of the gang database information to existing gang information systems. The gang database is not meant to replace any existing system; rather, it augments and formalizes an agency's local records while still allowing them to share/feed other regional databases.

Other requested features for FADE:

- Easier installation and management process for the server – lessen the need for lab personnel to be involved

- More extensive and improved user documentation

- Retain the ability to scale from a laptop up to an enterprise implementation. This allows small agencies and departments to access and use the technology with only a single laptop

- While the existing rich client (installed on desktop) has many advantages for analysts, having a web based client to the same information would be cheaper for many departments.

- The analysis tools are useful in some situations, but they need more maturity or specificity to the law enforcement domain to be truly useful
- Additional analysis tools including, enhanced link analysis, basic intelligence tools, timeline, etc. (see the section on criminal intelligence for more details)

Observations, Issues, and Recommendations

Each section is scored for its scope, impact, and maturity. Scope is a measure of its potential to assist a range of law enforcement activities – the more scope, the more agencies or divisions affected (narrow, medium, wide). Impact is a measure of its potential effectiveness within its scope (low, medium, high). Maturity is a measure of how technologically or legally mature the idea is, i.e. in need of basic research (low), primarily an engineering problem (high), or somewhere in the middle (medium).

Example:

Scope	Wide
Impact	Medium
Maturity	Low

This would indicate an idea that affects a wide range of organizations/topics, is medium in its impact on those areas, and is in need of basic research.

General and Cultural

Some of the opinions in this section (undeniably in this report) are controversial, indeed inflammatory in some circles both inside and outside of law enforcement. They are presented to provide context for technology investment, development, integration, and deployment projects – a roadmap to promote dialog. There are no simple solutions and no fingers need be pointed – but these issues are real. If you are developing technology for law enforcement, the following must be considered.

General

- Commercial tools (analytical, forensic, visualization, etc.), even when they exist, are often too expensive for state, county, and local law enforcement. Even federal field offices are often limited in their capabilities. This cannot be over emphasized. Information on the tools' utility is usually limited to vendor presentations and testimonials of other officers you happen to know personally. There is a need for unbiased technology reviews. The "Analyst Toolbox"[xiv] and "Fusion Center Technology Guide"[xv] do not provide enough specifics to enable organizations to select tools, even if they can afford them. Further, technologies often considered "solved problems" within research and commercial communities are still not implemented in a useful

manner within law enforcement. There is a general market failure concerning technology and law enforcement.

- Criminal intelligence is not well known or regarded in all agencies or departments despite its potential. The rules around it are very different from normal police work, which creates a barrier for medium and smaller departments. LEIU still has a great deal of out-reach to do to make sure law enforcement is aware of the potential and the guidelines surrounding this work.

- There is a huge gap between the tools and data sources that are available for law enforcement and what law enforcement is aware of and can actually access and use in daily work. There is a need for continued outreach on technical capabilities and to widen communication of this information. This is especially true with shrinking state, county, and city budgets; efficiency is at a premium and departments can use any assistance or leverage they can find. Many officers or departments are simply not aware of the resources available to them.

- Communication silos within law enforcement organizations can be very strong. Groups do not always share with other groups, even within the same agency. Part of the reason for this is political, as in any organization; however, much of it is also cultural – it just does not always occur to folks that sharing is important in any given situation – particularly if it does not directly involve the case at hand.

- Each department has its own interpretation of how "things" work, much like the communities they represent vary in their opinions on any given topic. Each has its own unique culture as well. This can vary quite widely.

- Coordination across jurisdictional boundaries is a huge issue. Not so much at patrol level, but on an investigative, analysis, and intelligence level. Criminals routinely take advantage of this fact (Native American reservations, borders, multiple municipalities, etc). Meaningful cross-jurisdictional information sharing can be difficult and time consuming. The proliferation of taskforces and regional intelligence groups has helped, but they need tools to extend their manpower. Also, as the number of jurisdictions increase – either through incorporation in a region (regions of a county incorporating into many smaller cities) or as the problem scope is broadened geographically (broader areas including many jurisdictions) – this issue becomes even more important.

- Time for analysis/intelligence creation that is outside of specific case work is limited or non-existent in most organizations. With ever tightening budgets, command-staff need to be shown how good intelligence can directly affect their communities and decisions in a positive way. Broad understanding of particular issues could provide more comprehensive approaches which are more effective and efficient. This understanding is a key tenant of intelligence-led policing. Understanding also lends itself to the involvement of policy/political actors in a region.

- Local law enforcement is generally good about sharing data when asked. However, as in the intelligence community, people are far less likely to share with people they do not know. *An individual's information is limited by the depth and width of their personal network*. Information sharing is excellent when a specific need arises, but is not as nearly as good for routine information. Time pressures are a factor here, as well as perceived importance of sharing vs. other tasks at hand.

- Conversely, some agencies and officers tend to share too broadly – sending out sensitive information to broad distribution lists. This can and has leaked information to inappropriate audiences. Criminal intelligence guidelines are critical to managing this issue.

- Federal law enforcement agencies are far less likely to share information with anyone, even other feds. This is a cultural artifact of the organizations and has little or nothing to do with the individual agents/officers. Even on federal task forces there are sometimes two levels of information, one for "feds" and one for "locals". Some of this is driven by classification issues, but most of it is cultural mistrust driven at an organizational level. Even when classification issues are removed, the sharing issues often remain. This is often a continuing source of friction between various agencies at all levels. In some cases, this leads to a backlash where "locals" do not share with "feds", but it is rare.

- Not enough state and local personnel have clearances to access classified information where appropriate. Even those who do, may not be considered to have a "need to know", with the result that information is not shared.

- There are perceived and real barriers between doing analytical work and doing police work. Analysts are sometimes seen as less than police officers. Consequently many police officers do not want to see themselves as "analysts". The workload of detectives is becoming increasingly analytical to keep up with the criminal element; yet, these biases have slowed the adoption of any kind of toolset or approach. Analysis is often considered synonymous with "statistics" or "comp stats". A hybrid team of experienced street cops and analysts seems to provide a better product than either alone. Policing is inherently a "high-touch", people oriented job. Doing it well involves a great deal of skill in dealing with humanity. Analysis is more abstract in its thinking and its tools. Hybrid teams bring out the strengths of each. It is difficult to move people between these skill sets, pointing to the notion of two professional career tracks. There is a continued need for professional analytical training and parallel careers within the law enforcement community.

- Many analysts get their start in the military. While the training is adequate, the jargon they bring with them is not helpful to the law enforcement mission. There is a language barrier between ex-military intelligence and police officers. Military analysis is not the same as police work.

- Nearly all areas of law enforcement need cheaper and more pervasive geospatial data and tools. Existing tools are too expensive and difficult to use. The software typically ends up on a single physical computer used by a very small number of personnel with specialized skills. The turn-around on geospatial work is often much too long to be truly useful to the organization. A government run, *law enforcement only*, central Google Earth server would be ideal. This could also serve as a data sharing mechanism for a variety of other data. It is well understood by most officers and is an established standard. DHS Earth is a very similar concept, only not focused on and exclusive to law enforcement.

Gangs, War Games and COIN

Scope	Wide
Impact	Medium
Maturity	High

Gangs are complex social and cultural phenomena that are ubiquitous in the American landscape. Despite numerous efforts to reduce their influence and growth, they are thriving. What is needed is a new approach to understanding the complex nature of the problem and a means to understand the consequences of policy and law enforcement choices[xvi]. Law enforcement and suppression alone cannot stem the tide – only a consistent multifaceted approach seems to have a chance. In the context of military counter insurgency (COIN) doctrine this is referred to as the "whole of government".

A whole of government approach, translated into a domestic context, is an approach that integrates the collaborative efforts of the departments and agencies of a city or county to achieve unity of effort toward a shared goal. A whole of government approach is vital to achieving the balance of resources, capabilities, and activities that reinforce progress made by one of the instruments of national power while enabling success among the others. It relies on interagency coordination among the agencies of local government, including the Law Enforcement community, to ensure that the full range of available capabilities are leveraged, synchronized, and applied toward addressing the drivers of gang violence and reinforcing local institutions to facilitate achieving sustainable peace in a community. Success in this approach depends upon the ability of civilians and law enforcement to plan jointly and respond quickly and effectively through an integrated, interagency approach to a fundamentally dynamic situation. Accomplishing this requires a willingness and ability to share resources among municipal, county, or state agencies and organizations while working toward a common goal. These resources—financial, law enforcement, policy, developmental, and strategic communications—are often limited in availability and cannot be restricted to use by a single department, agency or level of government.[xvii]

Insurgency is a similarly complex social phenomenon. Both war and organized criminal activity seem to be ubiquitous to the human condition and resistant to efforts to curb its existence. Managing an insurgent problem is directly analogous to the gang problem. Most of the same actors and forces come to bear. The U.S. military attempts to manage threats in complex social environments by undertaking actions to "ensure a stable and lasting peace, [in order to] capitalize on coordination, cooperation, integration, and synchronization among military and civilian organizations. These complementary civil-military efforts aim to strengthen legitimate governance, restore or maintain rule of law, provide a safe and secure environment, support economic and infrastructure development, and foster social well-being."[xviii]

To assist their efforts, the military uses "war games" to train personnel in the complexities of this environment, including:

- What are the consequences of different actions (course of action analysis)?
- What are the implications of a policy or action at a strategic, theatre, or tactical level?
- How does a "doctrine" or "policy" play out in the light of uncertainty or the "fog of war"?
- What are the consequences of mistakes within a given framework?

Games can be defined as a goal-oriented means of grappling with a problem. They are both instructional and exploratory. They are excellent vehicles for exploring trade-off optimization strategies in complex systems where there is no single "right" answer. A complex system is a system composed of interconnected parts that as a whole exhibit one or more properties not obvious from the properties of the individual parts.[xix] Strategies often emerge that not even the game creators envisioned. There are also elements of simulation and decision support; however, **it is the process of playing games that produces ideas and lessons in the players – not that the games necessarily produce "correct" answers.**

"With US gang policy development at an impasse, there is a pressing need for new paradigms and additional frameworks for confronting the modern street gang phenomenon. For authorities reliant on traditional notions of organized crime, the decentralized and loosely aligned nature of these extralegal social networks poses a serious conceptual challenge. Fortunately, insights can be gleaned from another type of extralegal network …the modern insurgency."[xx]

This makes COIN doctrine interesting as it provides a framework for viewing a domestic problem through a very different lens or context. However, the choices and actions required for its implementation are not easy. Choosing these tradeoffs within a geographic and social context is non-trivial and even more complex in a thriving democratic society.

Pulling these three ideas together, there is a need for a game and process that would provide a means to explore a multifaceted, whole of government approach to the gang problem. Players from law enforcement, political actors, service providers, and community members could work through the implications of this type of approach – gaining awareness of the true complexity of the problem,

grappling with tradeoffs that would allow more successful strategies in dealing with gangs, and insight to the type of consequences which might emerge as a result of their decisions.

Ad Hoc Information Sharing

Scope	Wide
Impact	High
Maturity	High

Across all the agencies there is a continued need for tools to support ad-hoc information sharing. Weekly or monthly meetings to share information are popular and useful; however, there is a need for *more immediate and specific data*. Information needs to be both geographically and topically specific, yet have the informal feel of a marketplace of ideas that are editable by an individual and available with only a browser. Craigslist embodies the topical and geographic themes – you can pick what city and what category you are interested in. Intellipedia, the classified wiki, has the editable qualities. What is needed is a mix of the two, a "**CopsList**" - editable by a law enforcement officer, yet with fixed geographic and categorical sections to focus on their specific interests (human trafficking, icac, gangs, narcotics, etc.). This would work to both extend an individual officers network of contacts in a specialty and also allow for querying and sharing of information on an as needed basis. The communication is cop-to-cop and is also strengthening regional connections between departments. Formal sharing of information and related systems are necessary and useful, but they do not allow for the flexibility and timeliness on a case-by-case basis that a system like this would offer. Types of queries and information might be, have you seen this person before, here is a trend we are seeing in X type of activity, have you seen this tattoo, etc. Some topic sites exist; however, they are often organized by discussion threads which make finding information much more difficult and time consuming. Also, the use of specific COI's (communities of interest) is too rigid and limiting for the nature of day-to-day police work. An officer should not have to specifically sign up and be approved for only a specific topic.

Civil Identification

Scope	Wide
Impact	High
Maturity	Low

Are you who you say you are? How do I know that? There is a growing need for a means to quickly identify someone in variety of situations. This is a pressing officer safety issue. What is needed is a rapid, highly accurate, minimally invasive, non-obvious, secure, and portable means to id someone – *above all*

someone who has already been in the correctional system and has been known for violence. Just as we have seen sex offenders held by civil containment, it seems an exploration of mandated civil identification for violent offenders would begin to address the most pressing issue. There is a great deal of research and commercial investment into biometrics of various kinds and the technology to implement it – fingerprints, facial recognition, retinal scans, voice, dna, etc. However, the real issue will be the laws to compel violent offenders to be "tagged" and the cost of getting the equipment into the hands of law enforcement. There is a need for legal and policy exploration as well as a survey of available biometric technologies.

Technical

General

- There is an ongoing need for unbiased tool and technique evaluation with continued outreach across the community. Vendors are currently often the sole source of information.

- Many departments have nothing more than their Records Management System (RMS) and Computer Aided Dispatch (CAD) systems to provide them information. These are usually focused on cases and reports, documentation to feed the court system, not intelligence to fight crime. All of these documents are past tense – what has happened.

- Tracking systems/GPS locators run into mixed reactions among officers. There are cultural and operational reasons at work here. There is the "big brother" mistrust of someone knowing where you are all the time, as well as operational security concerns with who has access to this information. On the flip side there are big pluses to knowing where all your undercover assets/blue force members are at any given time. The best compromise is to make this an option that can be turned off in any particular project.

- There will never be a single all encompassing system for law enforcement information either at a local, state, or federal level – *nor should there be*. We see a continuing proliferation of systems. However, the risk of a single system, especially if it contains criminal intelligence, is its fragility to both legal gaming and inappropriate use by any one agency/individual (in or outside of the law enforcement community). One wrong use can poison the well for everyone – with nothing left to replace it. The downside of the proliferation is a growing need to visit multiple sites to gain information for any given case. Any single officer/analyst only has access to a small set of these systems. Officers need assistance in gaining awareness about new systems and obtaining access to them; this is a time consuming and non-trivial endeavor that they do not have time for.

- Many of law enforcement information systems are difficult to use and thus their use is limited in practice even if folks have access. NCIC is particularly complex with little or no way to get information out of it and into other systems. The information is also very brittle and it is often

hard to find what you are looking for. Features such as batch submissions of search candidates are often missing.

Open Source Data and Social Media

Situation Awareness

Scope	Wide
Impact	Med
Maturity	High

Maintaining regional situation awareness is an everyday need for most law enforcement personnel and agencies. Shared resources and cross-jurisdictional problems make keeping aware of a region's issues important. However, other than the standard news channel running in an operations center this can be difficult to do. What is needed is a multiple source, internet based, situational awareness tool that continuously aggregates information about events and presents them in an easy to digest format. Pulling in such sources as traditional news, selected topical websites, and various social media (blogs, chats, tweets, Facebook, mySpace, etc.) would allow a broad view of current and potentially upcoming issues that directly affect staffing and preparedness. The tool needs multiple levels of "zoom" so that world, national, state, or regional events can be examined as needed. While there are some commercial sites available, their biases, ownership, availability, and focus are not ideal for law enforcement. They are also fixed, with no means for law enforcement to "steer" focus towards a given topic. A government based and managed program would provide a cost efficient and re-useable tool which could be used throughout the country.

Profile individuals and groups based on open source information

Scope	Wide
Impact	High
Maturity	High

Commonly in investigations you start with only a name. Filling out the details of a person's life is a time consuming and error prone process. Which sites to visit? Are there on-line alias's discovered that need to be added into the search as it progresses? Is this the same person? The ultimate goal is a report that gives an officer a sense of who this person is, what their involvements are, and who are they connected with. This information can then be merged with existing police records and case data to provide a broader perspective on an individual leading to more arrests, prosecutions, and solved cases. What is needed is a tool that can generate this type of report in a semi-autonomous fashion – presenting decisions to the searcher for them to guide, but relieving them of grinding through each and every

website by hand. Extending this idea to groups is the concept of monitoring the trends and actions of known criminal organizations. This is where proactive criminal intelligence can really begin to get ahead of the curve. There is an ongoing need to track trends, ideas, opinions, etc. within hate groups, organized crime, gangs, outlaw motorcycle gangs, etc. Many of these groups have public facing websites, and virtual social gathering places ideal for this type of analysis. The concept would have elements of a web harvester, a federated search engine, a web mashup/programmable web interface, and decision support engine that enables it to progressively add information as discovered.

Federation of existing law enforcement information sources

Scope	Wide
Impact	High
Maturity	Low

As presented elsewhere in the report, there continues to be an ongoing proliferation of official law enforcement information sources. This provides an excellent source of growing information for cases, but also a host of issues for the individual officer:

- Source discovery – How do I know this even exists?
- Credential management – How do I keep track of so many different passwords? How do I get access? How do I get a machine "certified" or obtain the proper tokens?
- Training – What are the rules for the system's use? How do I access it? How do I install it?

However, the number one request heard over and over again is, "how can I search all of these at once?" There is a real need to federate to all of these for finding information. The Global Justice Extensible Markup Language (XML) and Data Model (Global JXDM) are a good start at defining an interchange standard when this is appropriate, but there is a need to go further. The place to start is to identify an emerging industry standard for federated search (OpenSearch or CMIS as examples) and begin to slowly move existing and new systems to support it. This is a more flexible integration approach – instead of sharing data (in effect connecting systems) with a common data interchange, we allow them to search each other. There is a further need to connect these systems in a progressively intelligent way – if I search for a name, can the system also connect up a driver's license number or a social security number as it discovers them? This is a well known and very difficult problem. Continued research funding for connecting ontologies, ontological based search, and related areas is needed. A visual metaphor and tool for exploring data in this type of multi-database environment is also an area for exploration.

Management, Analysis, and Sharing of Criminal Intelligence

Scope	Medium
Impact	High
Maturity	High

There has been a great deal written about this topic[xxi,xxii] in the aftermath of Sept 11, 2001. However, there are still many needs that have not been addressed. As I have noted elsewhere, there is a continuing need for outreach and education in this area at a "boots on ground" level.

The National Criminal Intelligence Sharing Plan (2004) identifies six sensitive but unclassified systems with a national presence:

- Regional Information Sharing Systems' secure intranet (RISSNET), funded by the U.S. Department of Justice (DOJ), Office of Justice Programs, and membership fees of participating local and state law enforcement departments and agencies and also some federal law enforcement agencies' field divisions and field offices; The RISS Program is a secure nationwide communications and information sharing network that serves over 7,000 law enforcement member agencies from all government levels, with members in 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. Internet technology and virtual private network (VPN) software provide an encrypted, secure intranet that is able to connect member agencies to the databases of six regional RISS centers and five other intelligence systems from a single query via RISSNET.

- Law Enforcement Online (LEO), funded by DOJ; OJP provided funding for the interconnection of the RISS and LEO systems which was accomplished in September 2002. The RISS and LEO systems were recommended as the initial communications backbone for the National Criminal Intelligence Sharing Plan, given that no other system has been identified that can provide local, state, tribal, and federal nationwide communication connectivity.

- International Justice and Public Safety Information Sharing Network (NLETS). NLETS primary focus is at the state level. What services/information you have or do not, depends upon your individual state's connections to NLET's.

- Anti-Drug Network-Unclassified (ADNET-U), provided to law enforcement agencies primarily along the Southwest Border by the U.S. Department of Defense (DoD), Defense Information Systems Agency (DISA);

- Open Source Information System (OSIS), provided to the intelligence community, military, law enforcement, and diplomatic community agencies by the Intelligence Community Chief Information Officer through the Intelink Program Management Office; in mid 2006, the name OSIS and the network and content to which it referred were decoupled. The network piece is now named DNI-U while the content piece is named Intelink-U. The DNI-U network is maintained by the DNI-CIO Intelligence Community Enterprise Services office (ICES).

- OpenNet Plus, provided by the U.S. Department of State (DOS) to the 40-plus U.S. government agencies' representatives at 250 embassy sites internationally and the DOS headquarters.

The plan also notes a significant number of regional systems, examples include:

- Automated Regional Justice Information System (ARJIS)—a complex criminal justice enterprise network utilized by 38 local, state, and federal agencies in the San Diego, California, region. The ARJISNet secure intranet contains data on the region's crime cases, arrests, citations, field interviews, traffic accidents, fraudulent documents, photographs, gang information, and stolen property

- CriMNet, an enterprise architecture that puts in place a statewide framework of people, processes, data, standards, and technology focused on providing accurate and comprehensive data to the criminal justice community in the state of Minnesota.

- Law Enforcement Information Exchange (LInX), a regional information sharing system developed by the United States Naval Criminal Investigative Service (NCIS). Deployed in several regions throughout the country.

Although the report lists these systems as part of the plan for "criminal intelligence" there exists a central issue: Not all of these systems are actually designed to hold criminal intelligence – i.e. data that must be managed to the CFR 28 Part 23/LEIU Guidelines standard. Indeed, all these systems do not necessarily have actual criminal intelligence in them. Issues such as co-mingling of public and criminal intelligence data, protections against inappropriate FOIA release, appropriate timelines for maintenance and destruction, information dissemination guidelines, etc. ; all of these are issues for these systems. This is a confusing web for an operational organization to navigate.

There are also legitimate trust issues in sharing true criminal intelligence outside of its home organization without any explicit record of who received it and when. Currently information that is shared widely is often redacted of key or significant data. A solid solution will need to dynamically create trust networks for particular data across organizations, but also be able to un-trust and wall off other data that is not appropriate to share.

There is a need for a locally managed criminal intelligence system with the ability to share when appropriate.

Enhanced Link Analysis

Scope	Medium
Impact	High
Maturity	Medium

Link analysis is a common tool for law enforcement. However, existing tools are commonly used for no more than static picture making. The real promise of this type of analysis has yet to be realized. What is needed is the following:

- The ability to use a simple, visual, domain specific language to build queries for use against both graphs and other data sources.
- The ability to browse and connect structured and unstructured sources of data.
- The ability to quickly and easily make a meaningful graph of related entities starting from a set of unstructured documents or structured data sources.
- The ability to share these enhanced graphs with other commercial tools – ingest and save common file formats

Basic Intelligence Tools

Scope	Wide
Impact	High
Maturity	High

LEIU runs a Foundations of Intelligence Analysis Training (FIAT) class considered the baseline for law enforcement, which covers the following basic analytical techniques:

- Crime pattern analysis
    - Geospatial
    - Frequency
    - Pattern – time of day, day of week, time between, etc.
- Indicator development – what has happened historically
- Link analysis charts of relationships
- Communication analysis – phone, text, and other communication patterns
- Flow analysis – sequence of events

Despite the training, most of these techniques are only useful to those who have tools to implement them. Some can be done manually, but time constraints limit this approach to very select cases. Commercial tools exist for some of these but there is a need for a solid no-cost basic tool kit. Feedback suggests that adding this capability to FADE would be useful, but it could easily stand on its own as well. The highest priority items would be:

- A timeline tool for building arbitrary timelines using a drag and drop interface

- A phone call analysis tool that reads in standard record types (phone company records and forensic extracted files) and allows this data to be fed to a timeline and/or a link analysis tool.
- A geospatial tool that is easy to use and allows arbitrary data to be easily put on it – mostly as visualization and not a true GIS. A government run, *law enforcement only*, central Google Earth server would be ideal. This could also serve as a data sharing mechanism for a variety of other data. It is well understood by most officers and is an established standard. DHS Earth is a very similar concept, only not focused on and exclusive to law enforcement.
- Analysis of persistent automated license plate reader (ALPR) databases to cross reference with other data and aid in pattern recognition.

Fusion of Data Types

Scope	Medium
Impact	Medium
Maturity	Low

There is a growing need for law enforcement to have a means to pull together and make sense of a wide variety of data in a single tool – video, audio, geographic, structured, and unstructured text. This is similar problem to what we have seen in the intelligence community and certainly an unsolved problem. The wave is really just getting to law enforcement now. On larger cases where there may be multiple surveillance activities (videos, geo-tracks, and on-going data exchanges – text messages, phone calls, VoIP); it can be difficult to pull the information into a coherent picture. Some exploratory approaches are needed to see how this might be accomplished.

Mobile Devices

Scope	Wide
Impact	Medium
Maturity	High

There is a general trend away from laptops and towards mobile devices for the general population. CPU's are powerful enough that common daily tasks do not require a laptop. This same trend is emerging in law enforcement. Departments that cannot afford laptops can afford mobile phones. Bicycle officers and others with mobility needs are looking for easier ways to do their work. Existing police radios have a significant issue with cost. Small numbers of vendors have kept the costs very high for departments and this has driven an aggressive search for alternatives. Mobile devices are high on this list as a primary communication tool.

Mobile devices (phones and tablets) give us a platform for communication, data sharing, and analysis/computation. In general, they can be tools for widening the bandwidth of communication between the field and the precinct or station. Common requests are for:

- Undercover officer tool
    - Blue force ("good guy") tracking when appropriate
    - Low profile communication device – everyone has one now so they do not draw attention like a common police radio
    - Inexpensive surveillance platform (camera and microphone)
    - Access to general applications that are useful
        - Bar code readers for drivers license verification
        - WIFI network scanners
        - Packet sniffers
- Primary communication tool
    - With the aggressive use of templates and integration into core systems, use as a primary report writing tool and laptop replacement
    - What barriers really exist to making this leap?
    - Review of mesh networks for large areas that are robust and flexible enough to support this type of use
    - What are the costs and benefits?
- Bringing the field and the station closer – data conduit
    - Confirming identity based on field photography
    - Biometric sensor platform – iris, voice, image, fingerprint, etc.
    - Access to vetted criminal intelligence data – mug shots, gang membership, etc.
    - Rapid field data capture and push back for analysis – graffiti, gang members, crime scene, etc.
    - Geo-located and vetted data pushed to phone for officer safety issues

Regardless of the intended use, applications must look and work extremely "slick" for widespread adoption. There is little margin for "average" or "just ok" – if it is not a perfect fit, then people will not use it. We see this time and time again in the commercial market – expectations for mobile applications are very high.

Cross Jurisdictional, Large Scale Analysis

Scope	Wide
Impact	High
Maturity	Medium

Some of the most difficult crimes can only be understood when viewed from across multiple jurisdictions. This type of large scale analytical effort was impossible only a few years ago and is rarely seen today as it is expensive and not always directly tied to prosecutions. However, understanding can go a long way toward addressing crime in a proactive manner and drawing attention to issues otherwise hard to visualize.

The ability to explore all of the police data in a state, region, or even the country for patterns could yield incredible results. Computers and storage are now cheap and plenty enough make this feasible. Examples suggested include:

- Regional (multiple states and multiple cities) examination of underage prostitution and human trafficking patterns
- Nationwide analysis of cold cases (murder and missing persons) for cross-jurisdictional serial killers
- Narcotics, weapons, and human smuggling patterns
- Emerging patterns and ideas within the world of hate groups, outlaw motorcycle gangs, and other extreme criminal elements at a national scale
- Large scale analysis of ICAC (Internet Crimes Against Children)
    - Prevalence of material in cyberspace – scale of problem
    - Emergence of new material – i.e. new victims to find
- Search every available video recorded this morning (in the state, region or even the entire nation) for a missing child based on an amber alert. While this sounds fantastic, we are at the point where serious research could be done looking into this scale of problem.

- ID victims of human trafficking by analyzing all B1, H2A and H2B visas nation-wide looking for people at risk and then taking proactive action

As stated above, many of these applications have strong cross-cutting uses within the counter-terrorism world, but I have used other examples simply to show the broad utility of such approaches.

Secure Cloud computing will be an emerging theme in this type of work. Ideas here include:

- Rapid deployment major case toolkit – a suite of tools based in the cloud that is instantly deployable for small and otherwise over-whelmed departments dealing with high profile cases on short time frames. No need to deploy hardware or software for lead analysis – as in the FBI's RapidStart program. Public websites can be generated in minutes to capture input or to allow limited access for volunteer call-takers. Easily scalable to allow influx of mixed jurisdictions (Federal and local) to interact on a specific case. Support the rapid influx of heterogeneous data with need to track follow up and assign tasks to resources. There are few barriers to implementing this type of system now and it could yield great results – particularly for smaller departments.

- Ultimately, we will see individual systems moved into the cloud so that criminal intelligence and standard police data can be shared and analyzed on a routine basis at whatever scale is appropriate to the problem at hand. The better we plan for this, the easier integration will be. Research into standards, best practices, and security issues will be key areas to make this move successful.

Video

Scope	Wide
Impact	Medium
Maturity	Low

As we have already seen in the DOD and Intelligence community, law enforcement is being overwhelmed with video. The proliferation of cameras (public and private), public juries demand for "high tech" evidence (this is often referred to as the "24" or "CSI" effect after the respective television shows), the emergence and ultimate proliferation of UAV's as low cost alternatives to helicopters, growth in undercover surveillance footage are all forces at work here. There is no sign of this trend slowing. Indeed, the really large growth is likely still ahead of us. A medium size department I work with already has a 40 TB capacity and is planning on doubling this within three years. It is easy to see an average American city with 100 TB or more in less than five years.

Departments will need assistance choosing commercial systems for storage and management of such large data repositories. They will also need enhanced analytical and forensic capabilities which do not exist today.

Some coming issues:

- Video analysis
    - Search for an individual within a video based on a still photo or video clip
    - Search for an specific object (white pickup truck) within a video based on a still photo or video clip
    - Organize large sets of videos based on content (image and sound track)
    - Organize and search video footage based on metadata
    - Search videos for objects within them using text
    - Tag surveillance videos with significant events to triage review efforts
- Video forensics
    - Enhance surveillance footage in a semi-automatic fashion and thus reduce the time for analysis and the need for specialists in some cases.
    - Tools to access and work with all known video formats - proprietary and open source
    - Geo-locate a given unknown video or still photo based on sets of known locations already filmed and accessible on the web. This is particularly useful when attempting to identify the location in which a crime has been committed based on the surrounding objects and background of the footage. The idea is to tease out the location by using a large set of known images and known parameters of common items (cabinets, standard electrical plugs, brands of food and clothing, etc.). This is similar to what we have seen Microsoft Research do with Photosynth, but taking it much further than simply stitching disparate photos together.

Digital Forensics and Cyber

Scope	Wide
Impact	High
Maturity	Medium

Audio Forensics and Analysis

Audio forensics is still as much an art form as a science. Cleaning up surveillance audio is time consuming and is often a hit or miss process. Although, there are excellent and affordable tools

available, the time requirements are too high to allow its application in any except the most important cases. Semi-autonomous tools that can be operated by the non-technical people doing transcriptions should be our initial goal. This would cover a vast majority of the recordings, leaving special cases for specialists. Ultimately, we want to close this loop and remove the human transcriber, having a forensic algorithm feed a transcription algorithm which provides a feedback loop for improvement. Speech to text at this quality level is still an unsolved problem that needs basic research.

Speech to text is also an issue in radio transcription. Many have expressed interest in a tool to transcribe on-going radio traffic across multiple channels. This would provide a record of conversations for later review and also for quick reference. Radio transmissions are often difficult to hear requiring repetition of key information. This is especially true in large public crowd situations. Having a near real-time transcription of what is being said would be extremely useful in a variety of scenarios.

This same technology could be applied to the massive volume of jail and prison audio recordings. Many organized crime organizations are routinely run from prison. There are also a host of witness tampering, murders, and other miscellaneous criminal activities which are discussed and planned on a daily basis. Much, if not all, of this audio is recorded with no privacy concerns whatsoever; however, there is no good way to use it. Manual review is common and hence only applied in special cases. The county jail I have worked in alone has 100k calls per month which are recorded. A tool is needed to scan the audio for key words and triage particular calls for human review and also provide manual simple search. This will require a robust speech to text capability across a wide vocabulary and ultimately multiple languages.

Voice Biometrics

In the context of all this prison audio is also the need for fast and accurate biometrics for the human voice. Organized crime leaders and other incarcerated individuals could easily be identified both on prison recordings and from surveillance recordings done for, up to then, un-related cases. With sufficient accuracy this would be boon to law enforcement working to disrupt a variety of criminal networks. Voice prints could be taken when someone is booked into jail or prison and then shared across the community. This is related to the idea of civil identification discussed elsewhere in this report.

ICAC and Innocence Lost

Internet Crimes against Children (ICAC) and Innocence Lost (a program run by the FBI directed at underage prostitution) are particularly heinous crimes and yet these cases are underserved from a technology perspective. Many would prefer not to acknowledge the problem's existence; hence there is a great deal of potential in this area. The scope of the impact is also large; there are 61 ICAC and 39 Innocence Lost federal taskforces across the United States. Even small changes in efficiency would impact the workload and more importantly the lives of untold numbers of children.

- **Age Determination via Image**

Being able to have a machine accurately identify a minor from an image would provide a huge advantage to many Innocence Lost and ICAC officers. As a triage tool, a myriad of websites which routinely advertise underage prostitution could be scanned daily to identify new victims and make contact with victims who are already known to police but back on the street. There has been research in this area, but it is not a solved problem. Machines have yet to beat a human at the task, and humans are not very good at it.

- **Robust Image Signatures**

Currently the ICAC officer uses a hash as the common means to id a known child pornography image. A hash is a numerical signature for a specific image generated by a mathematical algorithm. There are tens of thousands of these hashes, each one matched exactly to a single image. The problem is that they are a brittle solution; a single pixel change will change the hash completely. This means there are a nearly infinite number of hashes for even the existing images on the internet – too many to ever really manage. What is needed is a robust signature for a given image, one that degrades slowly with changes and gives a low number for false positives. This would provide a host of benefits:

- Immediately determine if an image is new or already known even though an attempt has been made to obscure it. A new image means a new victim that needs assistance. This new signature can then be shared with other agencies, including NCMEC (National Center for Missing and Exploited Children) so it becomes a known image.

- Better detection of modified older images on networks and during forensic review of digital devices. This would make it more difficult to move this material around on the internet and force more of it to the physical world.

- Reduce the number of hashes to be managed and shared

- Ultimately, given sufficient accuracy, this type of signature would allow the creation of network sensors that could be given to private industry to allow them to monitor their own networks. While this data would not necessarily be useful for prosecution, it would give us the ability to accurately report on the problem's size and overall trend – for better or worse. The same data would allow a heat map to be drawn to bring attention to the problem.

A related idea is to be able to use these same signatures to identify or cluster families of images. Triaging images in this fashion might allow officers to better determine if they were made at the same time, via the same process, or at the same location based on similarities. A common problem is to have an image and have no idea where it was made, how, when, or who is in it.

Microsoft Research and other organizations have done work in this area; however, it is not clear how effective it is as a technique or how well it is fitting the grassroots needs of organizations.

What we see everyday locally and at a national level is the continued use of brittle hashes based on commonly known techniques. It is time to address this problem with a broader set of solutions and a continued effort to see it implemented.

Breaking Encryption – finding known images in encrypted volumes

It is a very hard problem to break encryption if you don't have any idea what is in the file. But what if you actually had 80% of the file? Could you use this knowledge to break the encryption? Often we know that an encrypted volume contains child pornography based on a suspect's on-line activities or other information. With this pre-knowledge of the suspect's interests, could you use a subset of the relatively finite set of child porn focused in this area to brute force and break the encryption? True Crypt and other strong encryption are becoming far more common in this world and it is a very difficult problem. This is a theoretical notion that has been bounced around and definitely worth some exploration.

Victim Identification

A key problem in this work is victim identification. Often we have a picture and have no idea of the identities of the victim (or the criminals). Using a variety of approaches there are a few areas to explore:

- Use of existing facial recognition algorithms to triage images via comparing them to known missing persons, previously incarcerated individuals, or other known image sets. This would assist both ICAC and Innocence Lost officers. Indeed it could have wide applicability.
- Tying this work into the civil identification database (see section on civil identification within general and cultural themes) to find known offenders who might have appeared in any of the found images.
- Surveying existing biometric research and tools to determine suitable candidates for use

Ethical hacking for law enforcement

There is a growing need for Law Enforcement to lawfully break into networks and computers in search of evidence and during long running surveillance. As the criminal world embraces technology for its ends, law enforcement will need to become more expert in it as well. This is particularly true in the ICAC arena. Tools and personnel will be needed to lawfully browse, penetrate, compromise, and otherwise capture information from the following:

- Local networks and general computers (windows, mac, linux)

- Wireless networks and technologies
- Peer-to-peer sharing networks and protocols such as:
    - IRC protocol networks
    - Gigatribe
    - Gnutella protocol networks
    - eDonkey, Kad
    - BitTorrent
    - Ares Galaxy
    - Direct Connect and Advanced Direct Connect
    - Freenet
    - StegoShare
    - Many others

Some of these tools exist, but many do not. More critical are the skills to use them. The Seattle Police Department estimates it takes a year and approximately $100K to train a new ICAC detective – that is only on the basics. While this area of need is most relevant to the ICAC world, there are direct benefits for any case that has a serious cyber component.

Cyber Crime Investigation

Scope	Wide
Impact	High
Maturity	Medium

Cyber issues are fast becoming a part of nearly every criminal investigation. The need for tools, techniques, best practices, training, and research is growing across the board. Most departments are not staffed deeply enough with skills locally. Regional centers are often backed up for months. This is a great deterrent to the use of this evidence in all kinds of cases. Yet everyone has these devices and they provide a telling story of activities when examined in depth.

Digital Device Forensics

There are a host of tools in the marketplace to assist in this arena. However, it can be hard to select the right one for your particular need. Unbiased advice is difficult to find.

Mobile Device Forensics

This is a particularly difficult area as the landscape (hardware and software) changes very fast. New devices are constantly on the market with the need for specialized techniques and equipment. There is need for an organization to assist in keeping up with the change as well as the internal contacts and policies of individual hardware and provider companies.

There is a need for faster in-field analysis of these devices. Sending them back to a specialist is not always possible. Tools are needed to quickly pull all the data out, put it together with multiple other devices' data, and create a visualization of all the content so analysis can happen sooner and not later. Numbers called, who called them, text messages, known VoIP application data, voice messages, pictures, dates and times, recent locations, etc. – all of this is needed in the combined analysis.

Image Forensics and Analysis

All of what has been said in the video section is also applicable here. The same general problems apply with a few additions.

- Image analysis
    - Search for an individual within a set of images based on a still photo or video clip
    - Organize large sets of images based on content
    - Organize and search images based on metadata
    - Search image sets for objects within them using text
- Image forensics
    - Enhance specific frames of surveillance footage in a semi-automatic fashion and thus reduce the time for analysis and the need for specialists in all cases.
    - Tools to access and work with all known image formats - proprietary and open source
    - Geo-locate a given unknown image based on sets of known images and locations
    - Graffiti identification and search
    - Tattoo identification and search

Privacy

Scope	Wide
Impact	High

Maturity	Low

With the scope and power of emerging technologies in law enforcement, it is both prudent and timely to consider overarching privacy concerns. Technology will soon allow us to do amazing, wonderful, and potentially appalling "things" – it is going to increasingly fall to individuals and organizations to make the right choices as to what "things" are appropriate in a given situation. There is a real need for reasoned policy discussion as to the appropriate limits without hampering law enforcement; this will not be an easy balance to reach. It is often said that "only the dumb criminals are caught", sadly this may be true in many cases. We find ourselves chasing an increasingly savvy criminal element willing to use technology to often heinous ends. Existing law provides an excellent guideline, but increasingly law enforcement will need coaching in the myriad grey areas. Different communities are going to face difficult choices:

- When is it appropriate to crack encryption?
- If I can search public video for a criminal act – should I? For a missing child? What about a missing car? Vandalized wall? Is it dollar amount driven?
- How do I craft a legal instrument to legitimately capture phone, VoIP, cell, and computer traffic? What about hacking that computer and taking control without the owner's knowledge? What if that "computer" is in the cloud along with legitimate users?
- How do you verify, store, and protect biometric data that identifies criminals?
- What are the legitimate uses for a UAV in law enforcement inside the borders?

This is of course nothing new from a moral or legal perspective. It is just that these issues are going to arise more often with many of the technologies explored in this report. Proactive measures to ensure community support will need to be considered and rolled out. Research into privacy policy should be considered an on-going priority.

Appendix

CFR 28 Part 23

28 CFR Part 23
CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES
Executive Order 12291
1998 Policy Clarification
1993 Revision and Commentary

28 CFR Part 23

Executive Order 12291 These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises. Regulatory Flexibility Act These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act. Paperwork Reduction Act There are no collection of information requirements contained in the proposed regulation. List of Subjects in 28 CFR Part 23 Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement. For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows: PART 23-CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec. 23.1 Purpose. 23.2 Background. 23.3 Applicability. 23.20 Operating principles. 23.30 Funding guidelines. 23.40 Monitoring and auditing of grants for the funding of intelligence systems. Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c). § 23.1 Purpose. The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals. § 23.2 Background. It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required. § 23.3 Applicability. (a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647). (b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy. § 23.20 Operating principles. (a) A project 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. (b) A project 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. (c) 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. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. (d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. (e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity. (f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles. (2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property. (g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained

participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented: (1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system; (2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project; (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization; (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster; (5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and (6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements. (h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years. (i) If funds awarded under the Act are used to support the operation of an intelligence system, then: (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and (2) A project shall undertake no major modifications to system design without prior grantor agency approval. (j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award. (k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance. (l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation. (m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system. (n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law. § 23.30 Funding guidelines. The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria: (a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity. (b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and: (1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and (2) Involve a significant degree of permanent criminal organization; or (3) Are not limited to one jurisdiction. (c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20. (d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency: (1) assume official responsibility and accountability for actions taken in the name of the joint entity, and (2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system. (e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation. § 23.40 Monitoring and auditing of grants for the funding of intelligence systems. (a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.
(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson Acting Assistant Attorney General Office of Justice Programs (FR Doc. 93-22614 Filed 9-15-93; 8:45 am) Criminal Intelligence Sharing Systems; Policy Clarification [Federal Register: December 30, 1998 (Volume 63, Number 250)] [Page 71752-71753] From the Federal Register Online via GPO Access [wais.access.gpo.gov] DEPARTMENT OF JUSTICE 28 CFR Part 23 [OJP(BJA)-1177B] RIN 1121-ZB40

- 6 -

1993 Revision and Commentary

28 CFR Part 23 Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies

---

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule **SUMMARY:** The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines. **EFFECTIVE DATE: September 16, 1993 FOR FURTHER INFORMATION CONTACT:** Paul Kendall, Esquire, General Counsel, **Office of Justice Programs**, 633 Indiana Ave., NW., Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235. **SUPPLEMENTARY INFORMATION:** The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691). The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows: **Confidentiality of Information**

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

This statutory provision and its implementing regulation apply to intelligence systems funded under title I of the Act, whether the system is operated by a single law enforcement agency, is an interjurisdictional intelligence system, is funded with discretionary grant funds, or is funded by a State with formula grant funds awarded under the Act's Drug Control and System Improvement Grant Program pursuant to part E, subpart 1 of the Act, 42 U.S.C. 3751-3759. The need for change to 28 CFR part 23 grew out of the program experience of the Office of Justice Programs (OJP) and its component agency, the Bureau of Justice Assistance (BJA), with the regulation and the changing and expanding law enforcement agency need to respond to criminal mobility, the National drug program, the increased complexity of criminal networks and conspiracies, and the limited funding available to State and local law enforcement agencies. In addition, law enforcement's capability to perform intelligence data base and analytical functions has been enhanced by technological advancements and sophisticated analytical techniques.

28 CFR part 23 governs the basic requirements of the intelligence system process. The process includes:

1. Information submission or collection 2. Secure storage 3. Inquiry and search capability 4. Controlled dissemination 5. Purge and review process

Information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation. The definition includes both systems that store detailed intelligence or investigative information on the suspected criminal activities of subjects and those which store only information designed to identify individuals or organizations that are the subject of an inquiry or analysis (a so-called "pointer system"). It does not include criminal history record information or identification (fingerprint) systems. There are nine significant areas of change to the regulation:

(1) Nomenclature changes (authority citations, organizational names) are included to bring the regulation up to date.

(2) Definitions of terms (28 CFR 23.3(b)) are modified or added as appropriate. The term "intelligence system" is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation; the terms "interjurisdictional intelligence system", "criminal intelligence information", "participating agency", "intelligence project", and "validation of information" are key terms that are defined in the regulation for the first time.

(3) The operating principles for intelligence systems (28 CFR 23.20) are modified to define the term "reasonable suspicion" or "criminal predicate". The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence data base (28 CFR 23.20(c)). This determination, as well as determinations that information was legally obtained (28 CFR 23.20(d)) and that a recipient of the information has a need to know and a right to know the information in the performance of a law enforcement function (28 CFR 23.20(e)), are established as the responsibility of the project for an interjurisdictional intelligence system. However, the regulation permits these responsibilities to be delegated to a properly trained participating agency which is subject to project inspection and audit (28 CFR 23.20(c),(d),(g)).

(4) Security requirements are established to protect the integrity of the intelligence data base and the information stored in the data base (28 CFR 23.20(g)(1)(i)-(vi)).

(5) The regulation provides that information retained in the system must be reviewed and validated for continuing compliance with system submission criteria within a 5-year retention period. Any information not validated within that period must be purged from the system (28 CFR 23.20(h)).

(6) Another change continues the general prohibition of direct remote terminal access to intelligence information in a funded intelligence system but provides an exception for systems which obtain express OJP approval based on a determination that the system has adequate policies and procedures in place to insure that access to system intelligence information is limited to authorized system users (28 CFR 23.20(i)(1)). OJP will carefully review all requests for exception to assure that a need exists and that system integrity will be provided and maintained (28 CFR 23.20(i)(1)).

(7) The regulation requires participating agencies to maintain back-up files for information submitted to an interjurisdictional intelligence system and provide for inspection and audit by project staff (28 CFR 23.20(h)).

(8) The final rule also includes a provision allowing the Attorney General or the Attorney General's designee to authorize a departure from the specific requirements of this part, in those cases where it is clearly shown that such waiver would promote the purposes and effectiveness of a criminal intelligence system while at the same time ensuring compliance with all applicable laws and protection for the privacy and constitutional

rights of individuals. The Department recognizes that other provisions of federal law may be applicable to (or may be adopted in the future with respect to) certain submitters or users of information in criminal intelligence systems. Moreover, as technological developments unfold over time in this area, experience may show that particular aspects of the requirements in this part may no longer be needed to serve their intended purpose or may even prevent desirable technological advances. Accordingly, this provision grants the flexibility to make such beneficial adaptations in particular cases or classes without the necessity to undertake a new rulemaking process. This waiver authority could only be exercised by the Attorney General or designee, in writing, upon a clear and convincing showing (28 CFR 23.20 (o)).

(9) The funding guidelines (28 CFR 23.30) are revised to permit funded intelligence systems to collect information either on organized criminal activity that represents a significant and recognized threat to the population or on criminal activity that is multi-jurisdictional in nature. **Rulemaking History** On February 27, 1992, the Department of Justice, Office of Justice Programs, published a notice of proposed rulemaking in the Federal Register (57 FR 6691). The Office of Justice Programs received a total of eleven comments on the proposed regulation, seven from State agencies, two from Regional Information Sharing Systems (RISS) program fund recipients, one from a Federal agency, and one from the RISS Project Directors Association. Comments will be discussed in the order in which they address the substance of the proposed regulation. **Discussion of Comments** Title - Part 23 Comment: One commentor suggested reinserting the word "Operating" in the title of the regulation to read "Criminal Intelligence Systems Operating Policies" to reflect that the regulation applies only to policies governing system operations. Response: Agreed. The title has been changed. APPLICABILITY - SECTION 23.3(a) Comment: A question was raised by one respondent as to whether the applicability of the regulation under Section 23.3(a) to systems "operating through support" under the Crime Control Act included agencies receiving any assistance funds and who operated an intelligence system or only those who received assistance funds for the specific purpose of funding the operation of an intelligence system. Response: The regulation applies to grantees and subgrantees who receive and use Crime Control Act funds to fund the operation of an intelligence system. Comment: Another commentor asked whether the purchase of software, office equipment, or the payment of staff salaries for a criminal intelligence system would constitute "operating through support" under the Crime Control Act. Response: Any direct Crime Control Act fund support that contributes to the operation of a criminal intelligence system would subject the system to the operation of the policy standards during the period of fund support. Comment: A third commentor inquired whether an agency's purchase of a telephone pen register or computer equipment to store and analyze pen register information would subject the agency or its information systems to the regulation. Response: No, neither a pen register nor equipment to analyze telephone toll information fall under the definition of a criminal intelligence system even though they may assist an agency to produce investigative or other information for an intelligence system. APPLICABILITY - SECTION 23.3(b) Comment: Several commentors questioned whether information systems that are designed to collect information on criminal suspects for purposes of inquiry and analysis, and which provide for dissemination of such information, qualify as "criminal intelligence systems." One pointed out that the information qualifying for system submission could not be "unconfirmed" or "soft" intelligence. Rather, it would generally have to be

: One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems. investigative file-based information to meet the "reasonable suspicion" test. Response: The character of an information system as a criminal intelligence system does not depend upon the source or categorization of the underlying information as "raw" or "soft" intelligence, preliminary investigation information, or investigative information, findings or determinations. It depends upon the purpose for which the information system exists and the type of information it contains. If the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity, and the information is identifying or descriptive information about the individual and the suspected criminal activity, then the system is a criminal intelligence system for purposes of the regulation. Only those criminal intelligence systems that receive, store and provide for the interagency exchange and analysis of criminal intelligence information in a manner consistent with this regulation are eligible for funding support with Crime Control Act funds. Comment

Response: No. A CHRI system contains information collected on arrests, detention, indictments, informations or other charges, dispositions, sentencing, correctional supervision, and release. It encompasses systems designed to collect, process, preserve, or disseminate such information. CHRI is factual, historical and objective information which provides a criminal justice system "profile" of an individual's past and present involvement in the criminal justice system. A fugitive file is designed to provide factual information to assist in the arrest of individuals for whom there is an outstanding want or warrant. Criminal intelligence information, by contrast, is both factual and conjectural (reasonable suspicion), current and subjective. It is intended for law enforcement use only, to provide law enforcement officers and agencies with useful information on criminal suspects and to foster interagency coordination and cooperation. A criminal intelligence system can have criminal history record information in it as an identifier but a CHRI system would not contain the suspected criminal activity information contained in a criminal intelligence system. This distinction provides the basis for the limitations on criminal intelligence systems set forth in the operating policies. Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system. Comment: Another commentor asked whether a law enforcement agency's criminal intelligence information unit, located at headquarters, which authorizes no outside access to information in its intelligence system, would be subject to the regulation. Response: No. The sharing of investigative or general file information on criminal subjects within an agency is a practice that takes place on a daily basis and is necessary for the efficient and effective operation of a law enforcement agency. Consequently, whether such a system is described as a case management or intelligence system, the regulation is not intended to apply to the exchange or sharing of such information when it takes place within a single law enforcement agency or organizational entity. For these purposes, an operational multi-jurisdictional task force would be considered a single organizational entity provided that it is established by and operates under a written memorandum of understanding or interagency agreement. The definition of "Criminal Intelligence System" has been modified to clarify this point. However, if a single agency or entity system provides access to system information to outside agencies on an inquiry or request basis, as a matter of either policy or practice, the system would qualify as a criminal intelligence system and be subject to the regulation. Comment: A commentor questioned whether the proposed exclusion of "analytical information and work products" from the definition of "Intelligence System" was intended to exclude all dissemination of analytical results from coverage under the regulation. Response: No. The exceptions in the proposed definition of "Intelligence System" of modus operandi files, historical telephone toll files and analytical information and work products are potentially confusing. The exceptions reflect types of data that may or may not qualify as "Criminal Intelligence Information" depending on particular facts and circumstances. Consequently, these exceptions have been deleted from the definition

: One commentor requested clarification of the role of the "Project" in the operation of an intelligence system, i.e. is the project required to have physical control (possession) of the information in an intelligence system or will authority over the system (operational control) suffice? : Operational control over an intelligence system's intelligence information is sufficient. The regulation seeks to establish a single locus of authority and responsibility for system information. Once that principle is established, the regulation permits, for example, the establishment of remote (off premises) data bases that meet applicable security requirements. of "Intelligence System" in the final rule. For example, analytical information and work products that are derived from unevaluated or bulk data (i.e. information that has not been tested to determine that it meets intelligence system submission criteria) are not intelligence information if they are returned to the submitting agency. This information and its products cannot be retained, stored, or made available for dissemination in an intelligence system unless and until the information has been evaluated and determined to meet system submission criteria. The proposed definition of "Analytical Information and Work Products" in Section 23.3(b) has also been deleted. To address the above issues, the definition of "Intelligence System" has been modified to define a "Criminal Intelligence System or Intelligence System" to mean "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information." Comment: Several commentors raised questions regarding the concept of "evaluated data" in the definition of "Criminal Intelligence Information", requesting guidance on what criteria to use in evaluating data. Another questioned whether there needed to be an active investigation as the basis for information to fall within the definition and whether information on an individual who or organization which is not the primary subject or target of an investigation or other data source, e.g. a criminal associate or co-conspirator, can qualify as "Criminal Intelligence Information." Response: The definition of "Criminal Intelligence Information" has been revised to reflect that data is evaluated for two purposes related to criminal intelligence system submissions: (1) to determine that it is relevant in identifying a criminal suspect and the criminal activity involved; and (2) to determine that the data meets criminal intelligence system submission criteria, including reasonable suspicion of involvement in criminal activity. As rewritten, there is no requirement that an "active investigation" is necessary. Further, the revised language makes it clear that individuals or organizations who are not primary subjects or targets can be identified in the criminal intelligence information, provided that they independently meet system submission criteria. CommentResponseOPERATING PRINCIPLES - SECTION 23.20(c) Comment: One respondent took the position that "Reasonable Suspicion", as defined in Section 23.20 (c), is not necessary to the protection of individual privacy and Constitutional rights, suggesting instead that information in a funded intelligence system need only be "necessary and relevant to an agency's lawful purposes." Response: While it is agreed that the standard suggested is appropriate for investigative or other information files maintained for use by or within an agency, the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of "hits" in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural. Comment: The prior commentor also criticized the proposed definition of reasonable suspicion for its specific reference to an "investigative file" as the source of intelligence system information, the potential inconsistency between the concepts of "infer" and "conclude" as standards for determining whether reasonable suspicion is justified by the information available, and the use of "reasonable possibility" rather than "articulable" or "sufficient" facts as the operative standard to conclude that reasonable suspicion exists. Response: The reference to an "investigative file" as the information source has been broadened to encompass any information source. The information available must provide a basis for the submitter to "believe" there is a reasonable possibility of the subject's involvement in the criminal activity or enterprise.

The concept of a "basis to believe" requires reasoning and logic coupled with sound judgment based on experience in law enforcement rather than a mere hunch, whim, or guess. The belief that is formed, that there is a "reasonable possibility" of criminal involvement, has been retained because the proposed standard is appropriately less restrictive than that which is required to establish probable cause.

OPERATING PRINCIPLES - SECTION 23.20(d) Comment: Section 23.20(d) prohibits the inclusion in an intelligence system of information obtained in violation of Federal, State, or local law or ordinance. Would a project be potentially liable for accepting, maintaining and disseminating such information even if it did not know that the information was illegally obtained? Response: In addition to protecting the rights of individuals and organizations that may be subjects in a criminal intelligence system, this prohibition serves to protect a project from liability for disseminating illegally obtained information. A clear project policy that prohibits the submission of illegally obtained information, coupled with an examination of supporting information to determine that the information was obtained legally or the delegation of such authority to a properly trained participating agency, and the establishment and performance of routine inspection and audit of participating agency records, should be sufficient to shield a project from potential liability based on negligence in the performance of its intelligence information screening function. OPERATING PRINCIPLES - SECTION 23.20(h) Comment: One commentor requested clarification of the "periodic review" requirement in Section 23.20(h) and what constitutes an "explanation of decision to retain" information.

Response: The periodic review requirement is designed to insure that system information is accurate and as up-to-date as reasonably possible. When a review has occurred, the record is appropriately updated and notated. The explanation of decision to retain can be a variety of reasons including "active investigation", "preliminary review in progress", "subject believed still active in jurisdiction", and the like. When information that has been reviewed or updated and a determination made that it continues to meet system submission criteria, the information has been "validated" and begins a new retention period. The regulation limits the retention period to a maximum of five years without a review and validation of the information. OPERATING PRINCIPLES - SECTION 23.20(i) Comment: One commentor requested a definition of "remote terminal" and asked how OJP would determine whether "adequate policies and procedures" are in place to insure the continued integrity of a criminal intelligence system. Response: A "remote terminal" is hardware that enables a participating agency to input into or access information from a project's criminal intelligence data base without the intervention of project staff. While the security requirements set forth in Section 23.20(g)(1)-(5) should minimize the threat to system integrity from unauthorized access to and the use of system information, special measures are called for when direct remote terminal access is authorized. The Office of Justice Programs will expect any request for approval of remote terminal access to include information on the following system protection measures: 1. Procedures for identification of authorized remote terminals and security of terminals; 2. Authorized access officer (remote terminal operator) identification and verification procedures; 3. Provisions for the levels of dissemination of information as directed by the submitting agency; 4. Provisions for the rejection of submissions unless critical data fields are completed; 5. Technological safeguards on system access, use, dissemination, and review and purge; 6. Physical security of the system;

7. Training and certification of system-participating agency personnel; 8. Provisions for the audit of system-participating agencies, to include: file data supporting submissions to the system; security of access terminals; and policy and procedure compliance; and 9. Documentation for audit trails of the entire system operation. Moreover, a waiver provision has been added to ensure flexibility in adapting quickly to technological and legal changes which may impact any of the requirements contained in this regulation. See Section 23.20 (o). Comment: Related to the above discussion, another commentor asked whether restrictions on direct remote terminal access would prohibit remote access to an "index" of information in the system. Response: Yes. The ability to obtain all information directly from a criminal intelligence system through the use of hardware based outside the system constitutes direct remote terminal access contrary to the provisions of Section 23.20(i)(1), except as specifically approved by OJP. Thus, a hit/no hit response, if gleaned from an index, would bring a remote terminal within the scope of the requirement for OJP approval of direct remote terminal access. Comment: One commentor pointed out that the requirement for prior OJP approval of "modifications to system design" was overly broad and could be read to require that even minor changes be submitted for approval. The commentor proposed a substitute which would limit the requirement to those modifications "that alter the system's identified goals in a way contrary to the requirements of (this regulation)."

Response: While it is agreed that the language is broad, the proposed limitation is too restrictive. The intent was that "modifications to system design" refer to "major" changes to the system, such as the nature of the information collected, the place or method of information storage, the authorized uses of information in the system, and provisions for access to system information by authorized participating agencies. This clarification has been incorporated in the regulation. In order to decentralize responsibility for approval of system design modifications, the proposed regulation has been revised to provide for approval of such modifications by the grantor agency rather than OJP. A similar change has been made to Section 23.20(j). OPERATING PRINCIPLES - SECTION 23.20(n) Comment: Several commentors expressed concern with the verification procedures set forth in Section 23.20(n). One suggested that file information cannot "verify" the correctness of submissions but instead serves to "document" or "substantiate" its correctness. Another proposed deleting the requirements that (1) files maintained by participating agencies to support system submissions be subject to the operating principles, and (2) participating agencies are authorized to maintain such files separately from other agency files. The first requirement conflicts with the normal investigative procedures of a law enforcement agency in that all information in agency source files cannot meet the operating principles, particularly the reasonable suspicion and relevancy requirements. The important principle is that the information which is gleaned from an agency's source files and submitted to the system meet the operating principles. The second requirement has no practical value. At most, it results in the creation of duplicative files or in submission information being segregated from source files. Response: OJP agrees with both comments. The word "documents" has been substituted for "verifies" and the provisions subjecting participating agency source files to the operating principles and authorizing maintenance of separate files have been deleted. Projects should use their audit and inspection access to agency source files to document the correctness of participating agency submissions on a sample basis. FUNDING GUIDELINES - SECTION 23.30(b) Comment: One commentor asked: Who defines the areas of criminal activity that "represent a significant and recognized threat to the population?" Response: The determination of areas of criminal activity focus and priority are matters for projects, project policy boards and member agencies to determine, provided that the additional regulatory requirements set forth in Section 23.30(b) are met. MONITORING AND AUDITING OF GRANTS - SECTION 23.40(a)

Comment: One commentor asked: "Who is responsible for developing the specialized monitoring and audit of awards for intelligence systems to insure compliance with the operating principles"?

Response: The grantor agency (the agency awarding a sub-grant to support an intelligence system) shall establish and approve a plan for specialized monitoring and audit of sub-awards prior to award. For the BJA Formula Grant Program, the State agency receiving the award from BJA is the grantor agency. Technical assistance and support in establishing a monitoring and audit plan is available through BJA. INFORMATION ON JUVENILES Comment: Can intelligence information pertaining to a juvenile who otherwise meets criminal intelligence system submission criteria be entered into an intelligence data base? Response: There is no limitation or restriction on entering intelligence information on juvenile subjects set forth in Federal law or regulation. However, State law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies. Therefore, State laws should be carefully reviewed to determine their impact on this practice and appropriate project policies adopted.

Executive Order 12291 These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises. **Regulatory Flexibility Act** These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act. **Paperwork Reduction Act** There are no collection of information requirements contained in the proposed regulation. **List of Subjects in 28 CFR Part 23** Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement. For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows: **PART 23--CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES** Sec.

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c). **§ 23.1 Purpose.** The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals. **§ 23.2 Background.** It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can

means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy. **.** (a) A project 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. (b) A project 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. (c) be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required. **§ 23.3 Applicability.** (a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647). (b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project Validation of Information **§ 23.20 Operating principles**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. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. (d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. (e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity. (f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence

information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property. (g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project; (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization; (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster; (5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and (6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years. (i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and (2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award. (k) A project shall make assurances that there will be no purchase or use in the course of the project of any

electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance. (l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation. (m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system. (n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records. (o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law. **§ 23.30 Funding guidelines.** The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria: (a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity. (b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or (3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20. (d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with

the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation. **§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.** (a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds. (b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20. (c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies. Laurie Robinson Acting Assistant Attorney General Office of Justice Programs (FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

1998 Policy Clarification

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

Comments

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and . . . meets criminal intelligence system submission criteria." Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual 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." 28 CFR 23.20(b) extends that limitation to [page 71753] collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 CFR Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the

identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only - it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

The Definition of a "Criminal Intelligence System"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information . . . ." Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "the term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation . . . ." 58 FR 48448-48449 (Sept. 16, 1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system . . ." do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

Additional guidelines will be issued to provide details of the above clarifications as needed.

Dated: December 22, 1998.

Nancy Gist Director, Bureau of Justice Assistance [FR Doc. 98-34547 Filed 12-29-98; 8:45 am] BILLING CODE 4410-18-P

- 21 -

LEIU Guidelines

CRIMINAL INTELLIGENCE FILE GUIDELINES

I. CRIMINAL INTELLIGENCE FILE GUIDELINES

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

II. CRIMINAL INTELLIGENCE FILE DEFINED

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
2. Are suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
2. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

III. FILE CONTENT

Only information with a criminal predicate and which meets the agency's criteria for file input should be stored in the criminal intelligence file. Specifically excluded material includes:

A. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.

B. Information on an individual or group merely on the basis of ethnic background.

C. Information on any individual or group merely on the basis of religious or political affiliations.

D. Information on an individual or group merely on the basis of non-criminal personal habits.

E. Criminal Offender Record Information (CORI), should be excluded from an intelligence file. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy.

F. Also excluded are associations with individuals that are not of a criminal nature.

State law or local regulations may dictate whether or not public record and intelligence information should be kept in separate files or commingled. Some agencies believe that separating their files will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded, as all information requested in the subpoena (both public and intelligence) must be turned over to the court. The judge then makes the determination on what information will be released.

The decision to commingle or separate public and intelligence documents is strictly a management decision. In determining this policy, administrators should consider the following:

A. Records relating to the conduct of the public's business that are prepared by a state or local agency, regardless of physical form or characteristics, may be considered public and the public has access to these records.

B. Specific types of records (including intelligence information) may be exempt from public disclosure.

C. Regardless of whether public record information is separated from or commingled with intelligence data, the public may have access to public records.

D. The separation of public information from criminal intelligence information may better protect the confidentiality of the criminal file. If a request is made for public records, an agency can release the public file and leave the intelligence file intact (thus less apt to accidentally disclose intelligence information).

E. Separating of files is the best theoretical approach to maintaining files; however, it is not easy to do. Most intelligence reports either reference public record information or else contain a combination of intelligence and public record data. Thus, it is difficult to isolate them from each other. Maintaining separate public and intelligence files also increases the amount of effort required to index, store, and retrieve information.

IV. FILE CRITERIA

All information retained in the criminal intelligence file should meet file criteria prescribed by the agency. These criteria should outline the agency's crime categories and provide specifics for determining whether subjects involved in these crimes are suitable for file inclusion.

File input criteria will vary among agencies because of differences in size, functions, resources, geographical location, crime problems, etc. The categories listed in the suggested model below are not exhaustive.

A. Permanent Status

1. Information that relates an individual, organization, business, or group is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

-Narcotic trafficking/manufacturing
-Unlawful gambling -Loansharking
-Extortion -Vice and pornography
-Infiltration of legitimate business for illegitimate purposes
- Stolen securities -Bribery
- Major crime including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson -Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation
- Threats to public officials and private citizens.

2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable--distinguished by a name and unique identifying characteristics (e.g., date of birth, criminal identification number, driver's license number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. NOTE: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.

B. Temporary Status:

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given "temporary" status. It is recommended the retention of temporary information not exceed one year unless a compelling reason exists to extend this time period. (An example of a compelling reason is if several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified temporary at the end of the one-year period, and a compelling reason for its retention is not evident, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1 **Subject/entity is unidentifiable** - subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2 **Involvement is questionable** - involvement in criminal activities is suspected by a subject/entity which has either:

-**Possible criminal associations** - individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.

-**Criminal history** - individual, organization, business, or group (not currently reported to be criminally active) that has a history of criminal conduct, and the circumstances currently being reported (i.e., new position or ownership in a business) indicates they may again become criminally active.

3. **Reliability/validity unknown** - the reliability of the information sources and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

V. INFORMATION EVALUATION

Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing.

The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy.

To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

Source Reliability:

(A) Reliable - The reliability of the source is unquestioned or has been well tested in the past.

(B) Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.

(C) Unreliable - The reliability of the source has been sporadic in the past.

(D) Unknown -The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity:

(1) Confirmed - The information has been corroborated by an investigator or another independent, reliable source.

(2) Probable - The information is consistent with past accounts.

(3) Doubtful - The information is inconsistent with past accounts.

(4) Cannot Be Judged - The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of the information to persons outside the agency. However, the classification of information in itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

Classification systems may differ among agencies as to the number of levels of security and release authority. In establishing a classification system, agencies should define the types of information for each security level, dissemination criteria, and release authority. The system listed below classifies data maintained in the Criminal Intelligence File according to one of the following categories:

Sensitive Sensitive

1. Information pertaining to significant law enforcement cases currently under investigation.
2. Corruption (police or other government officials), or other sensitive information.
3. Informant identification information.
4. Criminal intelligence reports which require strict dissemination and release criteria.

Confidential

1. Criminal intelligence reports not designated as sensitive.
2. Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Restricted

1. Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists.
2. Non-confidential information prepared for/by law enforcement agencies.

Unclassified

1. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).
2. News media information - newspaper, magazine, and periodical clippings dealing with specified criminal categories.

VII. INFORMATION SOURCE

In all cases, source identification should be available in some form. The true identify of the source should be used unless there is a need to protect the source. Accordingly, each law enforcement agency should establish criteria that would indicate when source identification would be appropriate.

The value of information stored in a criminal intelligence file is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

- The nature of the information reported.
- The potential need to refer to the source's identity for further or prosecutorial activity.
- The reliability of the source.

Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases when identifying the source by name is not practical for internal security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the intelligence unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information (for example "S60, a reliable police informant heard" or "a reliable law enforcement source of the police department saw" a particular event at a particular time).

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence files conforms with the agency's file criteria and has been properly evaluated and classified.

IX. FILE DISSEMINATION

Agencies should adopt sound procedures for disseminating stored information. These procedures will protect the individual's right to privacy as well as maintain the confidentiality of the sources and the file itself.

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "need-to-know" and a "right-to-know."

- **“Right-to-know"** Requestor has official capacity and statutory authority to the information being sought.

- **"Need-to-know"** Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

Information classification and evaluation are, in part, dissemination controls. They denote who may receive the information as well as the internal approval level(s) required for release of the information. In order to encourage conformity within the intelligence community, it is

Security Level	Dissemination Criteria	Release Authority
Sensitive	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Intelligence Unit Commander
Confidential	Same as for sensitive	Intelligence Unit Manager or designee
Restricted	Same as for Sensitive	Intelligence Unit Supervisor or designee
Unclassified	Not restricted Personnel	Intelligence Unit

recommended that stored information be classified according to a system similar to the following.

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. To eliminate unauthorized use and abuses of the system, a department should utilize a dissemination control form that could be maintained with each stored document. This control form would record the date of the request, the name of the agency and individual requesting the information, the need-toknow, the information provided, and the name of the employee handling the request. Depending upon the needs of the agency, the control form also may be designed to record other items useful to the agency in the management of its operations. This control form also may be subject to discovery.

X. FILE REVIEW AND PURGE

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to: ensure that the file is current, accurate, and relevant to the needs and objective of the agency; safeguard the individual's right of privacy as guaranteed under federal and state laws; and, ensure that the security classification level remains appropriate.

Law enforcement agencies have an obligation to keep stored information on subjects current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge

criteria and schedules. Operational procedures for the purge and the method of destruction for purged materials should be established.

A. Purge Criteria:

General considerations for reviewing and purging of information stored in the criminal intelligence file are as follows:

1. Utility

How often is the information used? For what purpose is the information being used? Who uses the information?

2. Timeliness and Appropriateness

Is this investigation still ongoing? Is the information outdated? Is the information relevant to the needs and objectives of the agency? Is the information relevant to the purpose for which it was collected and stored?

3. Accuracy and Completeness

Is the information still valid? Is the information adequate for identification purposes? Can the validity of the data be determined through investigative techniques?

B. Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every five years for permanent documents. Agencies should develop a schedule best suited to their needs and should contact their legal counsel for guidance.

C. Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. Disposal is used for all records or papers that identify a person by name. It is the responsibility of each agency to determine that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

XI. FILE SECURITY

The criminal intelligence file should be located in a secured area with file access restricted to authorized personnel.

Physical security of the criminal intelligence file is imperative to maintain the confidentiality of the information stored in the file and to ensure the protection of the individual's right to privacy.

Glossary

PUBLIC RECORD

Public record includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

"Member of the public" means any person, except a member, agent, officer, or employee of a federal, state, or local agency acting within the scop of his or her membership in an agency, office, or employment.

For purposes of these guidelines, public record information includes only that information to which the general public normally has direct access, (i.e., birth or death certificates, county recorder's information, incorporation information, etc.)

CRIMINAL OFFENDER RECORD INFORMATION (CORI)

CORI is defined as summary information to arrests, pretrial proceedings, sentencing information, incarcerations, parole and probation.

a. Summary criminal history records are commonly referred to as "rap sheets." Data submitted on fingerprint cards, disposition of arrest and citation forms and probation flash notices create

References

[i] State and Nonstate Associated Gangs: Credible "Midwives of New Social Orders", Max G. Manwaring, Strategic Studies Institute, May 2009

[ii] INSCT Institute for National Security and Counterterrorism Syracuse University – Mapping Global Insecurity, June 2010. http://insct.syr.edu/projects/mapping-global-insecurity/

[iii] Black Spots: Insecurity from beyond the horizon, Stanislawski, Bartosz Hieronim, Ph.D., Syracuse University, 2006, 351 pages

[iv] Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland, February 2010.

[v] Organized Crime in the United States: Trends and Issues for Congress, Kristin M. Finklea, Analyst in Domestic Security, Congressional Research Service. May 2009.

[vi] Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland, February 2010.

[vii] State and Nonstate Associated Gangs: Credible "Midwives of New Social Orders", Max G. Manwaring, Strategic Studies Institute, May 2009.

[viii] INSCT Institute for National Security and Counterterrorism Syracuse University – Mapping Global Insecurity, June 2010. http://insct.syr.edu/projects/mapping-global-insecurity/

[ix] Black Spots: Insecurity from beyond the horizon, Stanislawski, Bartosz Hieronim, Ph.D., Syracuse University, 2006.

[x] Kelly Greenhill, "Human Trafficking and Migrant Smuggling: New Perspectives on an Old Problem." Policy Brief, Harvard University, May 14, 2007.

[xi] Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy, Moisés Naím, 2005.

[xii] Ibid.

[xiii] Legal Issues and Privacy in Criminal Intelligence, Presentation at 2009 LEIU/IALEIA Conference by John Gordnier, Senior Assistant Attorney General of California, specializing in Criminal law and Criminal Intelligence

[xiv] Analyst Toolbox: A Toolbox for the Intelligence Analyst, Prepared by the U.S. Department of Justice's Global Justice Information Sharing Initiative Intelligence Working Group

[xv] Fusion Center Technology Guide: DHS/DOJ Fusion Process Technical Assistance Program and Services, U.S. Department of Justice's Global Justice Information Sharing Initiative (Global)

[xvi] Street Gang Patterns and Policies, Malcolm W. Klein and Cheryl L. Maxson, June 2006.

[xvii] U.S. Army, "A Whole-of-Government Approach," FM 3-07, Stability and Support Operations, Chapter 1-17, p. 1-4.

[xviii] U.S. Army, "Strategy for Stability Operations," FM 3-07, Stability and Support Operations, Chapter 1-77, p. 1-16.

[xix] ^ Joslyn, C. and Rocha, L. (2000). Towards semiotic agent-based models of socio-technical organizations, Proc. AI, Simulation and Planning in High Autonomy Systems (AIS 2000) Conference, Tucson, Arizona, pp. 70-79.

[xx] Maerder, James. and Mallinak, Kyle. "Counterinsurgency Doctrine and Implications for Domestic Gang Policy" Paper presented at the annual meeting of the Midwest Political Science Association 67th Annual National Conference, The Palmer House Hilton, Chicago, IL. 2011-03-07

[xxi] The National Criminal Intelligence Sharing Plan: Solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence, prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative.

[xxii] Analyst Toolbox: A Toolbox for the Intelligence Analyst, Prepared by the U.S. Department of Justice's Global Justice Information Sharing Initiative Intelligence Working Group