2004

Report to the Legislature

Submitted by the
Criminal and Juvenile Justice Information Policy Group

January 2005
Amended March 2005

CriMNet 2004 Annual Report to the Legislature
Table of Contents

I. Executive Summary

Background:
Justice and public safety services in Minnesota are delivered by 1,100 agencies and branches of local, state and federal government. These agencies often are headed by elected officials and have different enabling authority and funding sources. The information systems for each agency were often developed to meet individual operational needs without consideration of other justice agency needs. Justice and public safety services are comprised of many decisions from an initial decision to investigate; to arrest; to detain; to release pre-trial; to charge , adjudicate and dispose a case, as well as sentence to an array of penalties and conditions. All of these decisions are based on information. Often that information is missing, incomplete, inaccurate or not available in a timely manner because of the inability of the agencies to collect and share critical pieces of information needed at the various decision points.

CriMNet is Minnesota's program to integrate criminal justice information. This program involves defining what information criminal justice professionals' need, identifying barriers that prevent sharing of information among criminal justice professionals, offering solutions for these criminal justice professionals, and creating the business and technical standards that are needed to share information. Specifically, the scope of CriMNet is to:

Support the creation and maintenance of a criminal justice information framework that is accountable, credible, seamless, and responsive to the victim, the public, and the offender. ***As a result, the right information will be in the hands of the right people at the right time and in the right place.***

- By the *right information*, we mean that information will be accurate and complete and expressed in a standardized way, so that it is reliable and understandable.
- By the *right people*, we mean that people with different roles in the criminal justice system will have role-based views of the information that they need to do their jobs, and that access to certain private information is properly restricted.
- By the *right time*, we mean that practitioners and the public are provided information when they need it – as events occur.
- By the *right place*, we mean wherever the information is needed.

The primary result CriMNet seeks is:

- To accurately identify individuals
- To make sure that criminal justice records are complete, accurate, and readily available
- To ensure the availability of an individual's current status in the criminal justice system
- To provide standards for data sharing and analysis
- To maintain the security of information

- To accomplish our tasks in an efficient and effective manner.

The CriMNet Program is made up of a number of projects and initiatives at the state and local level to improve integration.

Efforts to improve the sharing of criminal justice information began in the early 1990s, guided by the provisions ofM.S.299C65 which created the Criminal and Juvenile Justice Information Policy Group (Policy Group). The Policy Group comprised of four commissioners from the executive branch and four members of the judicial branch, was charged with the responsibility for setting the direction for statewide criminal justice information system integration. The Criminal and Juvenile Justice Information Task Force (Task Force), currently made up of the members of the Policy Group and 29 other representatives (criminal justice professionals, legislators, state agency representatives, local municipality representatives and citizen members) was also created to assist the Policy Group in making recommendations to the legislature regarding criminal justice information systems. And in 2001, the legislature created a central program office to coordinate and oversee criminal justice information integration that has come to be known as CriMNet.

Early integration activities in the mid 1990's until 2000 included creating a domestic abuse order for protection data base and system to make restraining orders available to dispatchers and to squad cars with mobile data terminals; a juvenile criminal history; a predatory offender database; a database of arrest/booking photos; a database of statewide probation data; providing electronic fingerprint capture technology at most booking locations statewide; creating an enterprise information technology architecture for integration and an early local integration planning program.

From 2001 until mid 2003, the CriMNet Program focused almost solely on the technical aspect of creating an integration backbone that could link some of these statewide data repositories including some that were created under the above early integration activities. There are currently five statewide repositories that can be searched through the backbone: Minnesota Repository of Arrest Photos (MRAP), Predatory Offender Registry (POR), Statewide Supervision System (S3), Court Web Services (CWS) and the Minnesota Prison Information System. The Search Function has been in pilot phase since February 2003 and was rolled out statewide in late November 2004.

In 2003, with the lessons learned, it became very clear to the CriMNet Office and others involved in the program that while this technical piece of statewide integration is extremely valuable to criminal justice professionals, the solution to statewide integration was just as much about how criminal justice professionals do their business as it was about their technology needs. The CriMNet Office, leadership, and many stakeholders realized the business processes affecting information sharing had not received sufficient attention and had to become the priority.

Also in 2003 and early 2004 the Office of the Legislative Auditor conducted a program and financial audit. It can be found at: http://www.auditor.leg.state.mn.us/Ped/2004/pe0405.htm. The Legislative Auditor made a comprehensive set of recommendations to strengthen the CriMNet program. After the release of the audit in March 2004, the Policy Group met several times to review the report. On April 6, 2004 the Policy Group reported back to the Auditor on its plans to incorporate the recommendations of the audit. It then completed the activities specific to the Policy Group, and directed staff to incorporate the remaining Auditor's recommendations into the program.

One of the most significant activities was to create and adopt a program scope statement to guide the work of the office. The Policy Group adopted the CriMNet Scope Statement in June 2004 (see appendix A). **Much of the work of CriMNet in the second half of 2004 has been to build the programmatic infrastructure recommended by the Auditor, and begin the projects in the approved scope statement. (see section IV. for detailed project descriptions). In addition, the innovative local grant program has the largest counties in the state as well as several smaller counties and county cooperatives doing local and local-to-state integration. This work poises the program to make great strides in calendar 2005.**

Progress in 2004:

Program Scope

The scope statement is the foundation of the program and a key component for program management and program controls. A Task Force delivery team, consisting of a number of stakeholder representatives, drafted the CriMNet Scope Statement and presented it as a recommendation to the Task Force and Policy Group. The scope statement prioritizes a number of initiatives based on the two major goals in the CriMNet Strategic Plan, which was approved in September 2003. Goal 1: develop a blueprint for integration, and Goal 2: make available consolidated, complete and accurate records. Each of the two broad goals contained a number of specific objectives. Objectives in the scope statement include user requirements, business and technical standards, assistance to criminal justice agencies, development of an identification protocol, data quality, data practices, the search function and middleware service functions.

Projects

The CriMNet Program has begun a number of projects supporting CriMNet goals and objectives, and it has prioritized projects in a comprehensive short-term work plan for FY05 and a broader long-term work plan for FY06/07 and beyond.

A major project has been to rollout the search function statewide to more criminal justice professionals, as well as to add new data sources. Currently, additional data sources will

be made available in the 2006/2007 biennium as noted below including, warrants, stolen vehicles, orders for protection, driver files, and registered vehicle files.

Several projects are underway to increase the accuracy of justice records and ensure that they are only available to those legally authorized to have access to them. These projects include: The Development and Maintenance of Data Practice Compliance Standards; the Establishment and Maintenance of a Data Quality Process Project; and, the Technical Security Project. Section IV. has a detailed explanation of these important policy-driven initiatives.

In early 2005, warrant, orders for protection, stolen vehicle, criminal history, and driving record data, to name a few, will be added to the backbone search function. This will very significantly improve the value of CriMNet search. In addition workflow (automatic system to system data sharing) will begin to be added, starting with the eComplaint. This feature will significantly reduce duplication of data entry and increase the timeliness and accuracy of criminal justice information.

Another critical project that will add business value is the Identification Protocol. Positive identification is a cornerstone of all justice and public safety decisions from an initial stop, to arrest, detention and release, adjudication, disposition and sanction. We have learned how most offenders adopt many alias names and dates of birth to avoid their true records. The Identification Protocol will set standards for the type of biometric ID (fingerprint, photo image, etc.), or other identifier (drivers license number, etc.) based on the type of case or severity of charge. It will also create a "web service", a computer program or routine using contemporary technologies, which can be called and used by any other computer information system if it has the appropriate access and security approvals. The standard will be completed in the first quarter of calendar 2005 and the service in mid 2005. **The eventual result will be that all Minnesota justice and public safety records will be connected to a positive identifier thereby making offenders accountable for their behavior and providing better information to practitioners.**

Other projects are foundational to all future integration efforts. The Agency Assessment Project will provide data to extrapolate the total cost and effort to complete statewide integration. The User Requirements, Technical and Business Standards, Workflow and Business Process initiatives will provide the business (and technical) requirements for future integrations. The Service Agreement Project will establish clear expectations for source system agencies and for using agencies on data practices and audit processes for example.

Program Management, Oversight, and Controls

A standard program and project management methodology, as required by the Office of Technology, has been put into practice for the CriMNet Program and the individual projects. Each project has developed its own scope statement including objectives, deliverables, risks, budget and milestones. As projects begin, these scope statements are

presented to the Task Force for their approval. Each project is monitored closely and must submit weekly status reports to the CriMNet Program Manager. The CriMNet Office reports project status and financial status of the projects on a monthly basis to the Task Force and on a quarterly basis to the Policy Group.

As part of the financial reporting process and consistent with the Legislative Auditor's recommendations, the CriMNet Office has begun to allocate all expenditures to the projects CriMNet is involved in. All expenditures, including employee hours, contractor hours and purchases, are coded to a specific project and tracked through the state accounting system. The Task Force and Policy Group are provided financial reports which break out the expenses for each project in the following categories: full-time employees, consultants, software, hardware, infrastructure and other. This new system has allowed the CriMNet Program Office to more closely monitor and analyze project costs and provides more accountability for the funds spent on integration efforts. These new cost accounting procedures also allow for more accurate budgeting for future projects.

A new staffing organization for the CriMNet Program Office was created to incorporate positions focused on the business needs for integration efforts. One of the highlights of 2004 has been filling authorized positions to meet Program needs. The new staffing structure created two teams within the CriMNet Program Office – a business service center and a technical service center. A technical development arm of the Program was also created to continue work on technical projects such as the integration backbone (this development arm was transferred into the Criminal Justice Information System (CJIS) division of the Bureau of Criminal Apprehension (BCA)). In all, 26 permanent positions were created; however, there are still six of the original 26 positions that need to be filled and the executive director is considering realigning a few of the positions within the organizational structure. The lack of adequate staff was considered by the Legislative Auditor to be one of the greatest hindrances to the CriMNet Program since its inception in 2001.

An additional focus for 2004 has been improving communication, both at an internal and external level. A scope statement for the CriMNet Communications Plan has been developed and approved. This comprehensive communications plan will provide a structured communications framework that can be adapted to the CriMNet Program and any individual project within it. The final plan was completed in December 2004. Providing the detailed project status and financial reports to the Task Force and Policy Group on a regular basis has been an important step toward improving communication with CriMNet stakeholders. Another step taken to improve communication is the development of a formal issue submittal process where stakeholders are able to submit issues they feel the CriMNet Office should review and possibly take action on. These issues are reported on to the Task Force until they are resolved, passed on to the appropriate entity or closed. The CriMNet Program has also been much more proactive with stakeholders and potential "users" through the creation of business and technical

standards committees and the facilitation of user groups to discuss issues and gather feedback.

Conclusion:

The CriMNet Program has made significant, initial progress in statewide data sharing through the Search Function and the Workflow Function with the eComplaint. It has also put in place important, foundational program management and program control components in the areas of staffing, scope, planning, and communication consistent with the Legislative Auditor's recommendations.

With the progress made in 2004, CriMNet is poised to make significant future progress in statewide criminal justice information integration with the appropriate program controls in place to plan effectively, use resources wisely, measure success and provide accountability to the citizens of Minnesota.

II. Legislative Recommendations

Pursuant to Minnesota Statute 299C.65, Subdivision 2, the Criminal and Juvenile Justice Information Policy Group (Policy Group) must provide a report to the Legislature on December 1 each year detailing the statutory changes and/or appropriations necessary to ensure the efficient and effective operation of criminal justice information systems. This same statute requires the Criminal and Juvenile Justice Information Task Force (Task Force) to assist the Policy Group in developing recommendations.

The Task Force due-diligence work groups have met to consider proposed legislative recommendations. At the November 5, 2004 meeting of the Task Force, the recommendations brought forward by the work groups were given consideration, and recommendations to the Policy Group were made accordingly.

The following recommendations are being made by the Policy Group:

- Revise and update Minnesota Statute 299C.65
  See Appendix B

- Revise Minnesota Statutes 13, 299C.10, 299C.14, 299C.17, 299C.65, 611.272 related to Data Practices
  See Appendices C and D

- Allocate a specific state funding appropriation for grants to local entities for integration projects.

III. CriMNet Grant Program

New 2004 Grant Awards (pending contract execution)

Grantee	Amount	Purpose	Grant Period
Dakota County	$350,000	CJIIN Integration Hub The Hub Project is designed to achieve the goal of recording and sharing consolidated complete and accurate records of an individual's interaction with the criminal justice system. The hub will enable the pushing and pulling of messages, data and documents back and forth between Dakota County criminal justice agencies' databases and state databases. They would partner with Ramsey County to complete the logical design of the proposed functionality and evaluate and select an architecture.	October 2004 – September 2005
Hennepin County	$400,000	Adult Field Services Update The Update Project is designed to assist Hennepin County in completing the redesign and redevelopment of the Adult Field Services System (AFS) to a web-enabled application that exchanges data with other components of the criminal justice system by using web services and adapters connected to the Hennepin County Information Broker/Hub. AFS is the primary case record keeping system in Adult Probation at Hennepin County and is critical to the criminal justice process within Hennepin County and the State of Minnesota.	October 2004 – September 2005
Buffalo PD - Wright County	$49,000	County-wide Data System Interfaces The Interface Plan is to improve criminal justice system efficiency and function through electronic exchange of information and innovative processes, and to ensure accurate information to the project partners and system users in a timely manner. The three main	October 2004 – September 2005

		goals are to: 1) Improve the efficiency of the report writing process through the use of a unified field reporting system. 2) Create a system of delivery of electronic data between all Wright County law enforcement agencies, the State of MN, and other project partners to eliminate the need for redundant data entry and 3) Provide immediate access to shared data	
Ramsey County	$750,000	Identification Service and Data Exchange Hub The Hub is designed to address the problems of identifying individuals and sharing information. This project will result in more accurate information because it will be entered only once. It will result in more timely information because data collected at the earlier processing stages will become immediately available to agencies that become involved at a later stage. The project will put a reliable building block in place on which to build further integrations. A hub will be developed which provides capacity for any Ramsey County jurisdiction to share information electronically. The goal of this project is to build adapters, deploy an identification service, and implement a data exchange hub in order to electronically exchange data between the following: Ramsey County Criminal Court, Ramsey County Sheriff's Office, Ramsey County Attorney's Office, the new identification service and the Ramsey County Community Corrections Department.	October 2004 – September 2005
St. Louis County	$200,000	Interfaces with MNCIS There are four major components to the Interface Project. First it will provide the interface necessary to move citation information passing from automatic citation writers to the new Record Management	October 2004 – September 2005

		System (SHIELD) and citation information passing from SHIELD to the new Minnesota Court Information System (MNCIS), reducing the potential for mistakes and reducing the staff costs associated with multiple entries of the same data. St. Louis County Court Administration estimate that revenue collected from tickets will increase by 5% to 10% with additional resources made available, in addition to a cost saving from not having to enter approximately 30,000 citations in 2003 manually. Transferring the citations electronically will reduce errors, save entry time and provide improved customer service. Second, a paperless warrant system allows for the reduction in paper, reduced physical handling, increased speed in processing, and reduced error rate in entering data into the state system. This effort will automatically connect the Sheriff's Office, County Attorney's Office, and the Courts to allow warrant information, offense report, complaint, and other supporting documents to be exchanged. In addition, a hotlink will be established between the Sheriff's system and the BCA's Warrant Hotfile.	
MCCC – MCAPS	$160,000	County Attorney System Integration The MCCC-MCAPS Integration project is to improve, develop and implement a case management system that will replace the existing MCAPS case management system in the 57 county attorney offices and city attorney offices currently running the existing version. This is a joint effort by MCCC's County Attorney User Group to develop a common case management application and uniform business	October 2004 – September 2005

		practices. Business process analysis and reengineering will be an important part of this project. The grant funds will allow 57 county attorneys and city attorneys to move forward with this goal and also create data exchanges regarding individuals, incidents and cases through the CriMNet hub consistent with the parameters and specifications of the CriMNet backbone architecture.	
MCCC – CSTS	$160,000	Corrections User Group Integration The Integration Project is designed to develop a more comprehensive integration of information systems between Department of Corrections (DOC) and non-DOC agencies. This would encompass all supervision cases statewide, not just DOC cases, and would include critical information exchange between prisons and field supervision staff. The goal is to transfer information between systems, thus eliminating duplicate data entry and chance of errors or discrepancies in data. The project would create a seamless, efficient system that simplifies the transition of case information and offender data. This paperless transfer of data from one operational system to another will enhance the probation officer's ability to provide uninterrupted supervision of an offender. The ability to import data into a local CSTS system from COMS would reduce data entry time and the chance of error while improving the timely flow of essential data.	October 2004 – September 2005
Total New Grant Awards:	**$2,125,000**		

Implementation Grant Projects Underway and Reported in 2002 and 2003 Annual Reports

Grantee	Amount	Purpose	Grant Period
Anoka County	$1,169,149	Records Management System Integration (complete), Detention Project, Anoka/Dakota Joint Case Management Project	July 2002 – April 2005
Dakota County	$1,355,000	CJIIN Web System, County Attorney Case Management Integration, Records Management System Integration (complete)	July 2002 – April 2005
St. Louis County	$ 800,000	Records Management System Project	July 2002 – April 2005
Hennepin County	$ 420,000	City of Minneapolis Attorney's Prosecution Case Management System, Hennepin County Workhouse Management System, Arrest and Booking Process Re-engineering	July 2003 – September 2005
Minnesota Counties Computer Cooperative (MCCC)	$ 640,000	Court Services Tracking System	July 2002 – December 2004
LOGIS	$390,000	Public Safety Information Systems Integration	July 2003 – September 2005
Total Grant Awards:	**$4,774,149**		

IV. Current CriMNet Initiatives

Seek and Maintain User Requirements

May 2004 – December 2004

The CriMNet Program will document user requirements by actively and continuously seeking the input, assistance, and participation of stakeholders to define the business objectives and priorities for sharing information. This project has transformed to maintenance mode as of December 2004.

Progress and milestones:

- Develop requirements maintenance process - Completed
- Complete phase I feedback final reports - Completed
- Facilitate JAD sessions - Completed
- Complete phase II final report – 2/1/05
- Maintain business requirements – 1/1/05

Develop and Maintain Technical and Business Standards

September 2004 – On going

In order to improve the efficiency and effectiveness of information sharing, the CriMNet program will coordinate, champion, and maintain business standards, including data practice statutory requirements. CriMNet will facilitate the data collection and analysis to identify barriers to successful information sharing and to define the business standards for effective data sharing. Moreover, CriMNet will develop security and connectivity standards, define system architecture for the integration and sharing of information, develop standard statewide tables, and develop data model definitions that define event content and triggers, data standards, and definitions.

Progress and milestones:

- Create business steering committee – Completed
- Create technical steering committee – Completed
- Create a process for vetting and approving standards – Completed
- Create and populate Business Reference Model (BRM) – 12/31/06
- Create and populate Technical Reference Model (TRM) – 12/31/06

Provide Expertise & Assistance to Criminal Justice Agencies

April 2004 – June 2005

CriMNet will coordinate and provide assistance ranging from answering questions about CriMNet to providing high-level technical assistance on information sharing. This will

be an on-going activity. The criminal justice community can also submit issues for the CriMNet Office to address.

Progress and milestones:

- Create support infrastructure to assist criminal justice agencies and scope statement approved – Completed
- Address exchange forum and integration support – not determined
- Addressed the following issues submitted to the CriMNet Program:
    - Targeted Misdemeanors
        - A workgroup has met and an automated process is being worked on to pass targeted misdemeanors from court records to the criminal history system. When complete, all targeted misdemeanors statewide back to 2001 will be part of the criminal history system.
    - Predatory Offender Registration Accuracy §243.166 & §243.167
        - Staff from the Courts and BCA has been working to identify individuals that are not included in the POR database but were required to register. Follow-up on these individuals is almost complete. Work continues on where and how business processes may need to change to improve and automate registration.
    - Criminal Complaint
        - A workgroup of users met and came up with recommended changes to the format and design of the Uniform Criminal Complaint Form (UCC). Process inefficiencies still need to be addressed and work will continue in this area.
    - Minnesota Statute Table
        - CriMNet has been established as the owner of the Minnesota Statute Table enhancements and of the delivery to criminal justice agencies statewide. Currently, user requirements for enhancements are being completed and implementation is planned by the end of 2004.

Complete Agency Assessments

July 2004 – December 2004

CriMNet will assess capabilities and status of criminal justice agencies to assist in determining priorities for information sharing. Maintenance and updates of agencies information will continue.

Progress and milestones:

- Compile list of criminal justice agencies - Completed
- Conduct dry run of inventory documents and methods - Completed
- Post questionnaire to criminal justice agencies – Completed
- Build criminal justice information database – Completed

- Populate database with questionnaire responses – 1/1/05
- Update and maintain database – not defined yet

Develop and Maintain Data Practice Compliance Standards

February 2004 – December 2005

CriMNet will work with the Department of Administration and others to develop standards for the sharing of criminal justice information that ensure compliance with Minnesota data practices laws for participating agencies. This effort will include establishing mechanisms for individuals to review their non-confidential data shared through or by CriMNet and a process to challenge the data accuracy.

Progress and milestones:

- Complete data practices delivery team scope statement – Completed
- Assimilate reports and legislative changes into policy and procedures – 2/1/05
- Approve data practices policies and procedures at the Task Force – 03/15/05
- Implement verification "system" – 06/30/05
- Audit reports and data trail audit, system and policy correction – not defined yet

Establish and Maintain Identification Protocol

August 2004 – June 2006

The fundamental basis of criminal justice information is positive identification. CriMNet will evaluate current methods of identifying offenders, establish a protocol for offender identification, and develop a standard for linking records for participating agencies.

Progress and milestones:

- Develop Identification Roadmap scope statement - Completed
- Develop identification service requirements – 01/03/05
- Complete identification protocol document – 05/01/05
- Complete conceptual design document – 06/01/05
- Complete phased implementation plan document - 02/01/06
- Complete identification services – 06/06

Establish and Maintain a Data Quality Process

July 2004 – December 2006

CriMNet will establish standards for the validation of data and information that is shared for participating agencies. Much more work is needed before the timeline is finalized

Progress and milestones:
- Complete first on-site visit - Completed
- Develop initial scope statement - Completed
- Develop data integration standards - 05/31/06
- Develop Data Reference Model (DRM) - 06/01/06

Rollout the CriMNet Search Function
May 2004 – November 2004

CriMNet will develop and execute a plan for rolling out the "CriMNet Search Function" to criminal justice agencies.

Progress and milestones:
- Review and finalize business plan - Completed
- Review security verification - Completed
- Complete performance testing - Completed
- Create production support infrastructure and test production readiness - Completed
- Implement statewide rollout – Completed

Security
December 2004 - ongoing

It is the goal of this project to develop a detailed plan that would enable all agencies in the state of Minnesota to securely exchange electronic of criminal justice information. This includes the transmission of secure documents between agencies as well as the facilitation of secure searching of criminal justice records. An RFP process has been initiated to solicit vendors to assist us in executing this project.

Progress and milestones:
Select a vendor to assist in the security project – 1/15/05
Additional milestones to be determined.

Establish and Maintain the CriMNet Middleware Service Functions
June 2004 – May 2005

CriMNet will define a range of system services based on user requirements to implement information sharing between criminal justice agencies.

Progress and milestones:
- Complete initial scope of work - Completed

- Define and create CriMNet service delivery team - Completed
- Define and create CriMNet service working group - Completed
- Define "high-level" service architecture - 2/15/05
- Create Service Component Reference Model (SRM) – 5/15/05

Workflow and Business Processes

June 2004 - ongoing

Workflow is the capability to automatically and electronically move information from one application to another. In 2004, technical work has been completed to allow workflow through the CriMNet backbone. In addition, the specific workflow and surrounding business processes of the criminal complaint has been a particular focus. A workgroup has worked to define the business process improvements as well as the desired workflow for this product. Currently, this work is being transformed into technical specifications for implementation

Progress and milestones:

- Complete business plan for workflow – 2/1/05
- Develop and implement e-complaint workflow – to be determined
- Complete workflow final specification – to be determined

Service Agreements

July 2004 – December 2005

CriMNet will establish standardized data practices and audit policies and procedures to which participating agencies must agree to in order to transfer data. CriMNet staff will meet with a cross-section of users to determine present business needs and data practices and procedures as they relate to criminal justice data. This information will be used to create service agreements that are efficient, user-friendly and comply with state and federal data practices requirements.

Progress and milestones:

- Review work to incorporate CJIS agreements – Completed
- Rewrite scope statement - Completed
- Present scope statement to Task Force for approval - Completed
- Draft user system service agreement - 2/11/05
- Draft source system service agreement – 2/24/05

Communications

June 2004 – December 2004

A comprehensive communications plan will address all aspects of the CriMNet Program's internal and external communication. This structure communications framework can be adapted to the CriMNet Program and any individual project within it.

Progress and milestones:

- Draft preliminary communication plan - Completed
- Finalize detailed communication plan - Completed
- Solicit feedback and amend plan - Completed
- Present updated plan to the Task Force for approval - Completed
- Present updated plan to the Policy Group for approval – Completed

V. Additional Legislative Reporting Requirements

In addition to the annual report required in Minnesota Statute 299C.65, Subd. 2, the Criminal and Juvenile Justice Information Policy Group is also charged with studying and making recommendations to the Governor, the Supreme Court and the Legislature on the following fifteen items [Minn. Statute 299C.65, Subd. 1(d)].

As noted previously, the Office of the Legislative Auditor completed a financial and program audit of the CriMNet Program. One of the recommendations was to complete a scope statement for the CriMNet program. The audit and scope statement identify tasks and/or projects that also fall within the statutory reporting responsibility of the Policy Group. Those are so noted in the Status/Comments section of each reporting requirement.

299C.65, Subdivision 1d.	Status/Comments
1. A framework for integrated criminal justice information systems, including the development and maintenance of a community data model for state, county, and local criminal justice information	The CriMNet Strategic Plan and Scope Statement have as a major goal to "Develop a blueprint for the integration of criminal justice information. This goal includes developing a statewide integration plan as well as facilitating the development of state and local integration plans and services. As a part of achieving this goal, the CriMNet Program Office has implemented a project for developing a Business and Technical Standards Program. The Business and Technical Standards program will provide a process and venue for setting, changing, documenting, communicating, and providing access to information sharing standards. The process will include documentation of all standards (business and technical) through a Service Reference Model (SRM); Technical Reference Model (TRM); and overall "Blueprint for integration." **Recommendation:** Continue developing and documenting business and technical standards and an integration blueprint in collaboration with state and local stakeholders. Report annually on progress. ***Included in current Scope***
2. The responsibilities of each entity within the criminal and juvenile justice systems concerning the collection, maintenance, dissemination, and sharing of criminal justice information with one another	CriMNet developed an exchange-points model that documented current data responsibilities and needs for integration efforts across all criminal justice functions. In addition, the CriMNet Strategic Plan has identified several objectives that will facilitate the clarification of agency responsibilities relating to collection and dissemination as well as the sharing of criminal justice information. The CriMNet Program Office has initiated a Business Process Improvement Project with a goal of improving business processes that affect criminal justice system information collection and sharing. This project will enable

299C.65, Subdivision 1d.	Status/Comments
	greater effectiveness and efficiency by providing analysis, guidelines, documentation and plans for re-engineering. CriMNet has also embarked on a user requirements analysis effort geared towards documenting the criminal justice information landscape. This project has engaged a broad spectrum of criminal justice agencies and is synchronizing the Global Justice XML model with local business practices. This will result in a clear roadmap for selecting effective business improvements that will have the greatest positive impact on criminal justice information users. **Recommendation:** Report annually on progress. ***Included in current Scope***
3. Actions necessary to ensure that information maintained in the criminal justice information systems is accurate and up-to-date	An additional objective of the CriMNet program efforts is the development and monitoring of data quality standards as identified in the CriMNet Strategic Plan. The Business Process Improvement Project Team has begun identifying and prioritizing projects that will result in the increased accuracy and timeliness of criminal justice information shared statewide. **Recommendation:** Report annually on progress. ***Included in current Scope***
4. The development of an information system containing criminal justice information on gross misdemeanor-level and felony-level juvenile offenders that is part of the integrated criminal justice information system framework	**Recommendation:** Development of this system was completed in early 1998. Future reporting as needed.
5. The development of an information system containing criminal justice information on misdemeanor arrests, prosecutions, and convictions that is part of the integrated criminal justice information system framework	The MNCIS integration to the Criminal History File (CCH) includes targeted misdemeanors; as new counties are implemented on MNCIS, that data is now available in CCH. In addition, the Courts are developing a process to provide targeted misdemeanor data to CCH for the counties not yet converted to MNCIS. There will be additional analysis needed as a part of determining the scope of integration efforts and determining priorities prior to expanding efforts to non-targeted misdemeanor cases. **Recommendation:** Report annually on progress. ***Included in current Scope***
6. Comprehensive training programs and requirements for all individuals in criminal justice agencies to ensure the quality and accuracy of information in those systems	There are a number of training programs available to criminal justice agencies related to the accuracy and quality of data. In addition to specialized training provided by the BCA's Suspense Team, the CriMNet program office has also consolidated trainer/auditing functions with the BCA's other training

299C.65, Subdivision 1d.	Status/Comments
	programs to offer a more comprehensive delivery of statewide training on criminal history, Livescan, CriMNet Search and other statewide data functions. **Recommendation:** Report annually on issues identified by CriMNet business analysis and progress made. ***Included in current Scope***
7. Continuing education requirements for individuals in criminal justice agencies who are responsible for the collection, maintenance, dissemination, and sharing of criminal justice data;	A number of training/certification programs are available through the BCA in such areas as CCH, Live Scan, National Crime Information System (NCIC) and suspense file improvement. In addition, the consolidation of the BCA and CriMNet trainer/auditors has increased the effectiveness and efficiency of overall training efforts. Other CriMNet-related projects also offer specialized training (Statewide Supervision System, Court Web Access, Predator Offender Tracking, Minnesota Repository of Arrest Photos, etc). Data Practices training programs are planned to be developed and incorporated into existing training as appropriate. **Recommendation**: Future education requirements should be identified and prioritized through CriMNet strategic planning efforts.
8. A periodic audit process to ensure the quality and accuracy of information contained in the criminal justice information systems	As a part of future efforts (as identified in the CriMNet Strategic Plan), the importance of data quality standards was identified as a key objective. Achieving this objective will involve developing standards and processes for auditing as well as developing quality assurance standards and methods of evaluating data quality and accuracy. **Recommendation:** Report annually on progress and as needed on recommendations for process and legislative changes. ***Included in current Scope***
9. The equipment, training, and funding needs of the state and local agencies that participate in the criminal justice information systems	Currently the CriMNet Program Office is conducting a technology inventory of all criminal justice agencies in the state. The assessment includes an extensive questionnaire with follow-up by CriMNet staff. This assessment will identify the status of hardware/software platforms for each agency as well as identify IT resources. It will be possible to establish a baseline measure of readiness for integration. Agencies will also be asked to provide information about planned technology initiates, e.g., future upgrades or replacements of systems. This information will help to determine the degree of effort involved in rolling out particular CriMNet services to specific agencies and the agencies' ability to participate in information sharing and integration efforts. The initial phase of the assessment will be complete in December 2004. A database is being established to track and monitor this information for the future.

299C.65, Subdivision 1d.	Status/Comments
	Recommendation: Report annually on technology resource status of criminal justice agencies and needs related to information sharing and integration. ***Included in current Scope***
10. The impact of integrated criminal justice information systems on individual privacy rights	The Criminal and Juvenile Justice Information Task Force has created a Data Practices Subcommittee charged with developing recommendations related to the privacy interests of individuals. A report from that Subcommittee with regard to impacts on individual privacy rights is included as a part of this Annual report. **Recommendation:** Report annually or as needed. ***Included in current Scope***
11. The impact of proposed legislation on the criminal justice system, including any fiscal impact, need for training, changes in information systems, and changes in processes	**Recommendation:** The Criminal and Juvenile Justice Information Policy Group and Task Force will monitor proposed legislation and fiscal impacts and report as needed.
12. The collection of data on race and ethnicity in criminal justice information systems	**Recommendation:** Report completed and presented to Legislature. Future reporting as requested.
13. The development of a tracking system for domestic abuse orders for protection	**Recommendation:** System is completed. Future reporting as requested.
14. Processes for expungement, correction of inaccurate records, destruction of records, and other matters relating to the privacy interests of individuals	The Criminal and Juvenile Justice Information Task Force has created a Data Practices Subcommittee charged with developing recommendations related to the privacy interests of individuals as well as interests of public safety. Following approval by the Policy Group, any proposed policy changes and recommendations will be included in CriMNet Annual Reports. **Recommendation:** Make recommendations for process standardization and legislative/policy changes as needed. ***Included in current Scope***
15. The development of a database for extended jurisdiction juvenile records and whether the records should be public or private and how long they should be retained	The Court passes felony and gross misdemeanor-level and Extended Jurisdiction Juvenile (EJJ) data to BCA's Computerized Criminal History system. The BCA is in the process of researching juvenile record privacy and dissemination issues. A comprehensive policy will be developed in accordance with statutory provisions. **Recommendation**: Monitor and report as needed.

VI. Appendices

A. CriMNet Program Scope Statement (Approved June 2004)

B. Revisions to Minnesota Statute 299C.65

C. Revisions to Minnesota Statutes 13, 299C.10, 299C.14, 299C.17, 299C.65, 611.272 related to Data Practices

D. 2004 Data Practices Report

Appendix A

Program Scope Statement

June 2004

Version 1.0

Change Control

All changes to the document will be recorded in the table bellow.

Date	Version No.	Changed by:	Approved by:	Changes
06/30/2004	1.0		Policy Group	Approved by Policy Group

CriMNet
Program Scope Statement

Table of Contents

CriMNet
Program Scope Statement
June 2004

Preface

The Criminal and Juvenile Information Policy Group identified the need to formalize a CriMNet Scope document. This was also supported by the Legislative Auditor's program review of CriMNet. CriMNet Executive Director Bob Johnson formed a Scope Committee in January 2004 to prepare a CriMNet Scope document for approval.

Need/Benefit:

CriMNet will support the creation and maintenance of a criminal justice information framework that is accountable, credible, seamless, and responsive to the victim, the public, and the offender. ***As a result, the right information will be in the hands of the right people at the right time and in the right place.***

- By the *right information*, we mean that information will be accurate and complete and expressed in a standardized way, so that it is reliable and understandable.
- By the *right people*, we have in mind that people with different roles in the criminal justice system will have role-based views of the information that they need to do their jobs, and that access to certain private information is properly restricted.
- By the *right time*, we mean that practitioners and the public are provided information when they need it – as events occur.
- By the *right place*, we mean wherever the information is needed.

The primary results we seek are:

- To accurately identify individuals
- To make sure that criminal justice records are complete, accurate, and readily available
- To ensure the availability of an individual's current status in the criminal justice system
- To provide standards for data sharing and analysis
- To maintain the security of information
- To accomplish our tasks in an efficient and effective manner.[1]

[1] CriMNet Strategic Plan, v.1.0, September 2003

The benefits we hope to achieve are:

- Increased offender accountability
- Better criminal justice decision-making
- Appropriate sentencing from more accurate criminal history
- Increased staff safety
- More accurate offender information
- Better informed victims
- Safer communities.

CriMNet Program Responsibilities

The overall focus of the CriMNet program responsibility is on shared or exchanged electronic data/information between two or more agencies and the creation and maintenance of the business and technical standards that make those exchanges possible. CriMNet will manage issues and problems with electronic exchanges of information between agencies.

CriMNet will implement the sharing of criminal justice information through the development of agreed-upon business and technical standards and the fostering of collaborative efforts.

Objectives:

The CriMNet Program shall define, document, and maintain the technical and business standards for information sharing. The CriMNet Program will coordinate and provide technical assistance to agencies; communication of issues, barriers, and progress; and oversee the development of a statewide implementation plan.

(Note: The Criminal and Juvenile Justice Information Policy Group approved the CriMNet Strategic Plan in September 2003. The following sections in italics are directly quoted from the CriMNet Strategic Plan.)

1. Blueprint for Integration [2]

CriMNet Strategic Plan Goal 1: Develop a blueprint for the integration of criminal justice information

CriMNet will create and maintain a set of business and technical integration standards that support user justice information needs. CriMNet will collaborate with state and local planning efforts. The Criminal Justice Information Integration

[2] See Appendix A: Integration Definition

Blueprint will provide guidance useful to information integrators and describe what is required to participate in justice information sharing.

The CriMNet Program will serve as custodian for this blueprint for the integration of criminal justice information. The blueprint will be developed and used by state and local agencies to plan and support their information sharing efforts. The blueprint will include strategies, infrastructure definition, standards and interfaces. To accomplish this, the program will:

- *Maintain and make available a statewide integration plan that incorporates local planning and implementation efforts.*
- *Facilitate the integration of select state and local criminal justice information through collaboration among agencies.*
- *Provide expertise and assistance to support efforts for state and local integration plans and services.*
- *Ensure that the architecture and standards reflect agreed-upon requirements.*
- *Identify barriers to data sharing within the criminal justice community and recommend actions to remove the barriers.*

Initiatives include:

Seek and Maintain User Requirements: The CriMNet program will document user requirements by actively and continuously seeking the input, assistance, and participation of stakeholders to define the business objectives and priorities for sharing information.

Develop and Maintain Business Standards: In order to improve the efficiency and effectiveness of information sharing, the CriMNet program will coordinate, champion, and maintain business standards, including data practice statutory requirements. CriMNet will facilitate the data collection and analysis to identify barriers to successful information sharing and to define the business standards for effective data sharing.

Develop and Maintain Technical Standards (in compliance with the State of Minnesota Enterprise Technology Architecture): Develop security and connectivity standards, define system architecture for the integration and sharing of information, develop standard statewide tables, and develop data model definitions that define event content and triggers, data standards, and definitions.

Provide Expertise & Assistance to Criminal Justice Agencies: CriMNet will coordinate and provide assistance ranging from answering questions about CriMNet to providing high-level technical assistance on information sharing.

Prepare and Maintain a Statewide Implementation Plan: CriMNet will develop and maintain a comprehensive plan for statewide information sharing.

Complete Agency Assessments: Assess capabilities and status of criminal justice agencies to assist in determining priorities for information sharing.

2. *Accurate Criminal Justice Information*

CriMNet Strategic Plan Goal 2: Make available consolidated, complete, and accurate records of an individual's interaction with criminal justice agencies.

The fundamental component of the justice system is to ensure criminal justice information is available at the highest level possible. It is important that information be available at critical decision points:

- ***"Who are they?"***
- ***"At this decision point, what do we know about their record?"***
- ***"At this decision point, what is their current status in the justice system statewide?"***

Initiatives include:

Develop and Maintain Data Practice Compliance Standards: CriMNet will work with the Department of Administration and others to develop standards for the sharing of criminal justice information that ensure compliance with Minnesota data practices laws for participating agencies. This effort will include establishing mechanisms for individuals to review their non-confidential data shared through or by CriMNet and a process to challenge the data accuracy.

Establish and Maintain Identification Protocol: The fundamental basis of criminal justice information is positive identification. CriMNet will evaluate current methods of identifying offenders, establish a protocol for offender identification, and develop a standard for linking records for participating agencies.

Establish and Maintain Data Quality Standards: CriMNet will establish standards for the validation of data and information that is shared for participating agencies.

Rollout the "CriMNet Search Function": CriMNet will develop and execute a plan for rolling out the "CriMNet Search Function" to criminal justice agencies.

Establish and Maintain the CriMNet Middleware Service Functions: CriMNet will define a range of system services based on user requirements to implement information sharing between criminal justice agencies...

Each initiative is part of one or more projects that will require project level scope statements that will have associated with it costs, resources, schedules and

deliverables.

Program Approach:

The CriMNet Program provides the overall coordination and communication for the integration of criminal justice information. The program spearheads the strategic planning effort, takes an active role in communicating the need for an enterprise approach to integration, and provides assessments of justice practice needs.

The program must also provide standards to define integration from a business and technical perspective. To accomplish the business objectives, the program will be comprised of two service centers: 1) the Business Service Center and 2) the Technical Service Center.

Business Service Center

This function defines and operationalizes the CriMNet vision from the criminal justice business perspective. CriMNet integration efforts will be cooperative ventures among partners in the criminal justice arena, and partners will bring their own expertise to the table. As such, the CriMNet program will facilitate the development of a statewide integration approach based on the existing business approaches and the business requirements for effective data sharing in the future. Responsibilities of the Business Service Center include User requirements definition, Business process modeling, Data model definition, Data integrity and quality, Data practices, and Integration planning and implementation.

Technical Service Center

This function defines and operationalizes the CriMNet vision from the criminal justice technical perspective. CriMNet will facilitate the development of a statewide integration blueprint based on existing and proposed technical infrastructures for effective data sharing in the future. Responsibilities of the Technical Service Center include Data exchange support, Software services, and Agency support (Consult on methods for an agency to; modify applications to recognize business events and to consume event driven real time data exchanges; transform agency data to/from the standards exchange model; and on the use of web services, message oriented middleware, or other software to transport data).

APPENDIX A:

Integration Definition

Integration of Justice Information

Integrated justice information sharing generally refers *to the ability to share critical information at key decision points throughout the justice enterprise.* Moreover, this information sharing and access extends across agencies and branches of government at the local (that is horizontal integration), as well as interested parties at the local, State, and Federal jurisdictions (that is vertical integration).

Building integrated justice information systems does not mean that all information between agencies is shared, without regard to the event, the agencies involved or the sensitivity of the information. Agencies need to share critical information at key decision points throughout the justice system. There is explicit recognition that this sharing of information can be accomplished by any of a variety of technical solutions or combinations of technical solutions. Integrated justice does not presume any particular proprietary technological solution.

Moreover, the integration of justice information is properly viewed as a broad and significant **process** that is dynamic and multifaceted in nature, and part of the ongoing evolution in justice business practices, not as a simple project to share information with discrete beginning and termination points. Building integration and information sharing capabilities in justice often contemplates fundamental changes in business practices across agencies and jurisdictions, and between branches of government. As a consequence, integration typically raises important legal, constitutional and policy issues that must be addressed. Integration also affords an important opportunity to reengineer operations in substantive respects. Mapping the information exchanges among justice agencies often identifies significant duplication in data entry, redundant processing and circuitous business processes that are evidence of the piecemeal automation practices in most jurisdictions.

Expanding Demand for Information Sharing

Moreover, integration and information sharing between justice agencies, with other governmental agencies, and with the general public raises new and important privacy and confidentiality issues that must also be addressed.

It is important to recognize that integrated justice information sharing is designed not only to meet the operational needs of participating justice agencies, but also to address the increasingly expansive information demands of society. The need to electronically share accurate and complete information in a timely and secure manner has been triggered by a host of State and Federal legislative directives in recent years.

These programs are designed to improve public safety and the well being of our citizens in such ways as:

- Restricting the sales of firearms to persons without criminal records, a history of mental illness or other prohibiting factors.
- Restricting and/or monitoring licensing of elder-care, child-care and health-care service providers.

Providing community notification of the location or release of sexually violent predators.

Functional Components of Integration

The Criminal Justice Information Integration Blueprint will provide guidance useful to information integrators and will describe what is required in order for a state system or local jurisdiction to participate in justice information sharing. The blueprint will address what is required in order to share information. Integrated justice information sharing generally refers to the ability to access and share critical information at key decision points throughout the justice enterprise. The functions normally considered in integration efforts between agencies include the ability to:

1. Automatically **query** local, regional, statewide and national databases to assess the criminal justice status of a person, such as determining whether a person is currently wanted by another jurisdiction, has charges pending in another jurisdiction, is currently under some form of correctional supervision, or has a criminal history at the local, state, or national level.
2. Automatically **push** information to another agency, based on actions taken within the originating agency (for example, reporting arrest information – together with supporting fingerprint and mug shot – to state and national criminal history repositories based on new information in the local database; when law enforcement agency makes an arrest and enters this information in its records management system, it should "push" information to the prosecuting attorney's office for use in the prosecutor case intake process).
3. Automatically **pull** information from another system for incorporating into the recipient agency system (for example, populating a correctional information system with offender information captured in presentence investigation, together with court sentencing information),
4. **Publish** information regarding people, cases, events and agency actions (for example, both electronic and paper publishing of information regarding scheduled court events, crime mapping, availability of community resources, criminal history records, sex offender registries, etc.).
5. **Subscription/Notification** of key transactions and events regarding subjects, events and cases (for example, probation agencies and individual probation officers should be able to formally subscribe to a notification service that will automatically notify them of whenever one of their clients is arrested or otherwise involved in the justice system).

Integration efforts are designed to automate many of these operations, reengineer systems and processes, and achieve new capabilities with greater efficiency and effectiveness.

Foundation Principles of Integration

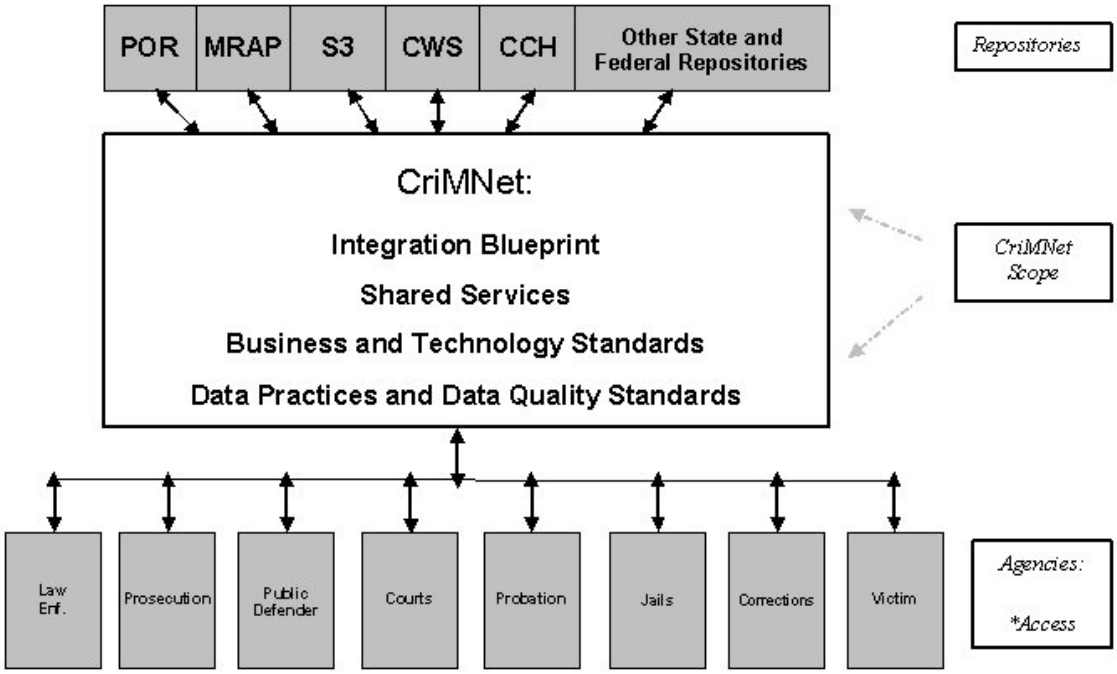
Integration is designed to address the operational needs of justice agencies. In spite of these varying objectives, there are several fundamental principles that guide the development of integrated justice information systems.

1. Information is captured at the originating point, rather than reconstructed later.
2. Information is capture once and reused, rather then re-captured when needed again.
3. Integrated systems fulfilling these functions are comprised of, or derived from the operational systems of the participating agencies; they are not separate from the systems supporting the agencies.
4. Justice organizations retain the right to design, operate and maintain systems to meet their own operational requirements. However, as with any network capability, participants must meet agreed-upon data, communication and security requirements and standards in order to participate.
5. Whenever appropriate, standards will be defined, with user input, in terms of performance requirements and functional capabilities, rather than hardware and software brand names.
6. Security and privacy are priorities in the development of integrated justice capabilities, and in the determination of standards.
7. Integration builds on current infrastructure and incorporates capabilities and functionality of existing information systems where possible.
8. Establishing and confirming the positive identity of the record subject is crucial.

APPENDIX B:

CriMNet Responsibility Diagram

The boundaries of CriMNet in relation to the various criminal justice agencies and data repositories are illustrated below:



As illustrated by the above diagram, responsibilities can be summarized by the following three areas:

- Local responsibility for data
- Agencies responsible for repositories
- CriMNet responsible for standards and technology for shared events and data

POR – Predatory Offender Registration
MRAP – Minnesota Repository of Arrest Photos
S3 – Statewide Supervision System
CWS – Court Web Services
CCH – Computerized Criminal History

APPENDIX C:

CriMNet Development Service Center

Development Service Center

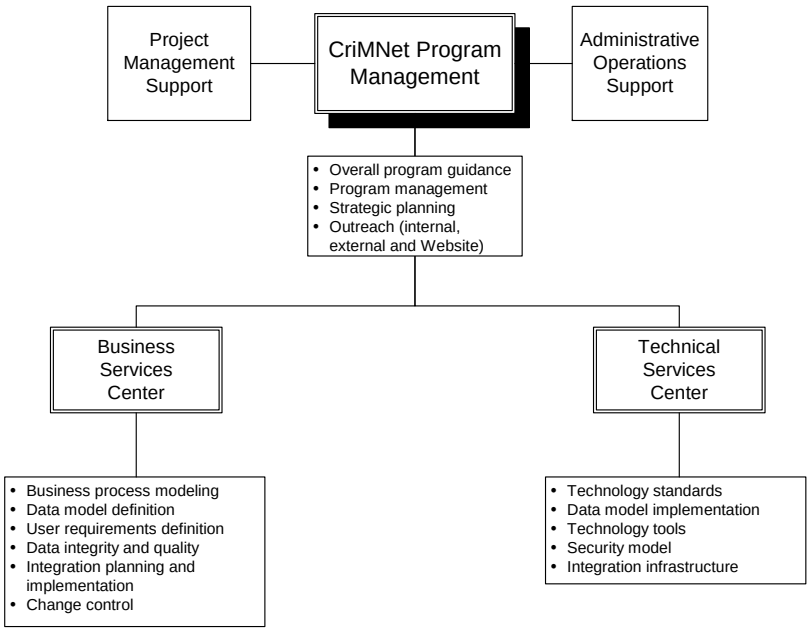
A Development Center currently exists to deliver integration components and services (e.g., broker, search functionality, subscription, etc.). The Development Center was originally a function of the CriMNet Program; however both the Criminal and Juvenile Justice Information Task Force and the Aeritae Risk Assessment recommended that the Development Center be moved into a line organization. In April 2004, the Development Center was moved to the Criminal Justice Information Systems Division within the Bureau of Criminal Apprehension. The Development Center continues to be funded by CriMNet.

APPENDIX D:

CriMNet Program Functional Organization Chart

CriMNet Functional Organization

Friday, June 6, 2003



Appendix B

299C.65 Criminal and juvenile information policy group.

Subdivision 1. **Membership, duties**. (a) The criminal and juvenile justice information policy group consists of the commissioner of corrections, the commissioner of public safety, the commissioner of administration, the commissioner of finance, ~~and~~ four members of the judicial branch appointed by the chief justice of the supreme court, and the chair and first vice chair of the criminal and juvenile justice information task force. The policy group may appoint additional, nonvoting members as necessary from time to time.

(b) The commissioner of public safety is designated as the chair of the policy group. The commissioner and the policy group have overall responsibility for the successful completion of statewide criminal justice information system integration (CriMNet). The policy group may hire an ~~program manager~~ executive director to manage the CriMNet projects and to be responsible for the day-to-day operations of CriMNet. The executive director shall serve at the pleasure of the policy group in unclassified service. The policy group must ensure that generally accepted project management techniques are utilized for each CriMNet project, including:

(1) clear sponsorship;

(2) scope management;

(3) project planning, control, and execution;

(4) continuous risk assessment and mitigation;

(5) cost management;

(6) quality management reviews;

(7) communications management; ~~and~~

(8) proven methodology; and

(9) education and training.

(c) Products and services for CriMNet project management, system design, implementation, and application hosting must be acquired using an appropriate procurement process, which includes:

(1) a determination of required products and services;

(2) a request for proposal development and identification of potential sources;

(3) competitive bid solicitation, evaluation, and selection; and

(4) contract administration and close-out.

(d) The policy group shall study and make recommendations to the governor, the supreme court, and the legislature on:

1) a framework for integrated criminal justice information systems, including the development and maintenance of a community data model for state, county, and local criminal justice information;

2) the responsibilities of each entity within the criminal and juvenile justice systems concerning the collection, maintenance, dissemination, and sharing of criminal justice information with one another;

3) actions necessary to ensure that information maintained in the criminal justice information systems is accurate and up-to-date;

4) the development of an information system containing criminal justice information on gross misdemeanor-level and felony-level juvenile offenders that is part of the integrated criminal justice information system framework;

5) the development of an information system containing criminal justice information on misdemeanor arrests, prosecutions, and convictions that is part of the integrated criminal justice information system framework;

6) comprehensive training programs and requirements for all individuals in criminal justice agencies to ensure the quality and accuracy of information in those systems;

7) continuing education requirements for individuals in criminal justice agencies who are responsible for the collection, maintenance, dissemination, and sharing of criminal justice data;

8) a periodic audit process to ensure the quality and accuracy of information contained in the criminal justice information systems;

9) the equipment, training, and funding needs of the state and local agencies that participate in the criminal justice information systems;

10) the impact of integrated criminal justice information systems on individual privacy rights;

11) the impact of proposed legislation on the criminal justice system, including any fiscal impact, need for training, changes in information systems, and changes in processes;

12) the collection of data on race and ethnicity in criminal justice information systems;

13) the development of a tracking system for domestic abuse orders for protection;

14) processes for expungement, correction of inaccurate records, destruction of records, and other matters relating to the privacy interests of individuals; and

15) the development of a database for extended jurisdiction juvenile records and whether the records should be public or private and how long they should be retained.

Subd. 2. **~~Report, t~~ Task force.** ~~(a) The policy group shall file an annual report with the governor, supreme court, and chairs and ranking minority members of the senate and house committees and divisions with jurisdiction over criminal justice funding and policy by December 1 of each year.~~

~~(b) The report must make recommendations concerning any legislative changes or appropriations that are needed to ensure that the criminal justice information systems operate accurately and efficiently. To assist them in developing their recommendations,~~ T~~t~~he policy group shall appoint a task force to assist them in their duties. The task force shall monitor, review and report to the policy group on CriMNet-related projects and provide oversight to ongoing operations as directed by the policy group. The task force shall consist~~ing~~ of ~~its members or their designees and~~ the following ~~additional~~ members:

~~the director of the office of strategic and long-range planning;~~

1) two sheriffs recommended by the Minnesota sheriffs association;

2) two police chiefs recommended by the Minnesota chiefs of police association;

3) two county attorneys recommended by the Minnesota county attorneys association;

4) two city attorneys recommended by the Minnesota league of cities;

5) two public defenders appointed by the board of public defense;

6) two district judges appointed by the conference of chief judges, one of whom is currently assigned to the juvenile court;

7) two community corrections administrators recommended by the Minnesota association of counties, one of whom represents a community corrections act county;

8) two probation officers;

9) four public members, one of whom has been a victim of crime, and two who are representatives of the private business community who have expertise in integrated information systems;

10) two court administrators;

11) one member of the house of representatives appointed by the speaker of the house;

12) one member of the senate appointed by the majority leader;

13) the attorney general or a designee;

~~14) the commissioner of administration or a designee;~~

14) an individual recommended by the Minnesota league of cities; ~~and~~

15) an individual recommended by the Minnesota association of counties~~.~~ ;

16) the director of the sentencing guidelines commission;

17) one member appointed by the commissioner of public safety;

18) one member appointed by the commissioner of corrections;

19) one member appointed by the commissioner of administration; and

20) one member appointed by the chief justice of the supreme court

In making these appointments, the appointing authority shall select members with expertise in integrated data systems or best practices.

~~(c)~~ The commissioner of public safety may appoint additional, nonvoting members to the task force as necessary from time to time.

Subd. 3. **Report** The policy group, with the assistance of the task force, shall file an annual report with the governor, supreme court, and chairs and ranking minority members of the senate and house committees and divisions with jurisdiction over criminal justice funding and policy by January 15 of each year. The report must provide the following:

(a) status and review of current integration efforts and projects;
(b) recommendations concerning any legislative changes or appropriations that are needed to ensure that the criminal justice information systems operate accurately and efficiently; and
(c) summary of the activities of the policy group and task force.

~~Subd. 3. **Continuing education program.** The criminal and juvenile information policy group shall explore the feasibility of developing and implementing a continuing education program for state, county, and local criminal justice information agencies. The policy group shall consult with representatives of public and private post-secondary institutions in determining the most effective manner in which the training shall be provided. The policy group shall include recommendations in the 1994 report to the legislature.~~

~~Subd. 4. **Criminal Code numbering scheme.** The policy group shall study and make recommendations on a structured numbering scheme for the Criminal Code to facilitate identification of the offense and the elements of the crime and shall include recommendations in the 1994 report to the legislature.~~

Subd. 4~~5~~. **Review of funding and grant requests**. (a) The criminal and juvenile justice information policy group shall review the funding requests for criminal justice information systems from state, county, and municipal government agencies. The policy group shall review the requests for compatibility to statewide criminal justice information system standards. The review shall be forwarded to the chairs and ranking minority members of the house and senate committees and divisions with jurisdiction over criminal justice funding and policy.

(b) ~~The policy group shall also review funding requests for criminal justice information systems grants to be made by the commissioner of public safety as provided in this section. Within the limits of available appropriations, the commissioner of public safety shall make grants for projects that have been approved by the policy group.~~ The CriMNet program office, in consultation with the criminal and juvenile justice information task force and with the approval of the policy group, shall create the requirements for any grant request and determine the integration priorities for the grant period. The CriMNet program office shall also review the requests submitted for compatibility to statewide criminal justice information systems standards.

(c) ~~If a funding request is for development of a comprehensive criminal justice information integration plan, the policy group shall ensure that the request contains the components specified in subdivision 6. If a funding request is for implementation of a plan or other criminal justice information systems project, the policy group shall ensure that:~~

~~(1) the government agency has adopted a comprehensive plan that complies with subdivision 6;~~

~~(2) the request contains the components specified in subdivision 7; and~~

~~(3) the request demonstrates that it is consistent with the government agency's comprehensive plan.~~

The task force shall review funding requests for criminal justice information systems grants and make recommendations to the policy group. The policy group shall review the recommendations of the task force and shall make a final recommendation for criminal justice information systems grants to be made by the commissioner of public safety. Within the limits of available state appropriations and federal grants, the commissioner of public safety shall make grants for projects that have been recommended by the policy group.

(d) The policy group may approve grants only if the applicant provides an appropriate share of matching funds as determined by the policy group to help pay up to one-half of the costs of the grant request. The matching requirement must be constant for all counties. The policy group shall adopt policies concerning the use of in-kind resources to satisfy the match requirement and the sources from which matching funds may be obtained. Local operational or technology staffing costs may be considered as meeting this match requirement. Each grant recipient shall certify to the policy group that it has not reduced funds from local, county, federal, or other sources which, in the absence of the grant, would have been made available to the grant recipient to improve or integrate criminal justice technology.

(e) All grant recipients shall submit to the CriMNet program office all requested documentation including grant status, financial reports and a final report evaluating how the grant funds improved the agency's criminal justice integration priorities. The CriMNet program office shall establish the recipient's reporting dates at the time funds are awarded.

~~Subd. 4~~6~~.~~ **~~Development of integration plan~~**. ~~(a) If a funding request is for funds to develop a comprehensive criminal justice information integration plan to integrate all systems within a jurisdiction, the requesting agency must submit to the policy group a request that contains the following components:~~

~~(1) the vision, mission, goals, objectives, and scope of the integration plan;~~

~~(2) a statement of need identifying problems, inefficiencies, gaps, overlaps, and barriers within the requesting agency's jurisdiction, including those related to current systems and interfaces, business practices, policies, laws, and rules;~~

~~(3) a list of agency heads and staff who will direct the effort and a statement demonstrating collaboration among all of the agencies involved;~~

~~(4) a statement that the integration plan would integrate all systems within the six major business functions of the criminal justice community, including incident reporting, investigation, arrest, detention, adjudication, and disposition, including postsentence supervision and treatment, and related civil, family, and human services proceedings, processes, and services, to the extent it was cost beneficial;~~

~~(5) a statement demonstrating that the requesting agency has consulted with individuals involved in day-to-day business practices, use, and operation of current criminal justice information systems so as to identify barriers and gaps;~~

~~(6) a planning methodology that will result in at least the following deliverables:~~

~~(i) an identification of problems in the state's criminal justice data model, where applicable, including data policy problems and proposed changes;~~

~~(ii) a function and process model that includes business process improvement and redesign opportunities, prioritized business change objectives, and short-term opportunities for improvement that can be pursued immediately while developing and implementing the long-range integration plan;~~

~~(iii) a technology model that includes network, communication, and security standards and guidelines;~~

~~(iv) an application architecture;~~

~~(v) a complete gap analysis that includes identification of gaps, omissions, and redundancies in the collection and dissemination of criminal justice information in the requesting agency's jurisdiction;~~

~~(vi) an assessment of current and alternative directions for business practices, applications, and technology, ranging from simple modifications to complete redesign;~~

~~(vii) a business process redesign model, showing existing and redesigned process and process vision, future performance targets, design principles, new process flow, and benefits; and~~

~~(viii) a long-range integration plan that includes time frames for the retirement, renewal, or redevelopment of systems and applications identified in clauses (i) to (vii) along with justification based on age, business processes not supported, and data deficiencies;~~

~~(7) projected timelines for developing and executing the plan;~~

~~(8) an estimate of the resources needed to develop, execute, operate, and maintain the integration plan;~~

~~(9) a statement that the final integration plan will contain all the components in this subdivision in final form;~~

~~(10) an identification of how the applicant will satisfy the match requirements of subdivision 8; and~~

~~(11) any other matters the policy group deems necessary for successful development or implementation of the integration plan and resulting systems.~~

~~(b) An agency may submit an interim integration plan to the policy group if it identifies high priority integration tasks during the development of the integration plan. The interim plan shall identify the tasks and the business case for completing these tasks in advance of completing the entire plan.~~

~~Subd. 5~~7. **~~Implementation of integration plan~~**. ~~If the request is for funds to implement an integration plan, the requesting agency must submit the following to the policy group:~~

~~(1) an integration plan containing the components described in subdivision 6;~~

~~(2) a description of how implementation of the integration plan will improve operation of the criminal justice system in the requesting agency's jurisdiction;~~

~~(3) an identification of how the applicant will satisfy the match requirement in subdivision 8; and~~

~~(4) a means for evaluating outcomes of the plan's implementation.~~

~~Subd. 6~~8. **~~Local match~~**. ~~(a) The policy group may approve grants only if the applicant provides an appropriate share of matching funds as determined by the policy group to help pay up to one-half of the costs of developing or implementing the integration plan. The matching requirement must be a constant for all counties. The policy group shall adopt policies concerning the use of in-kind resources to satisfy the match requirement and the sources from which matching funds may be obtained. Local operational or technology staffing costs may be considered as meeting this match requirement.~~

~~(b) The policy group shall consult with the task force when carrying out its powers and duties under paragraph (a).~~

~~(c) Each grant recipient shall certify to the policy group that it has not reduced funds from local, county, federal, or other sources which, in the absence of the grant, would have been made available to the grant recipient to improve or integrate criminal justice technology.~~

~~Subd. 7~~8a. **~~Criminal justice technology infrastructure improvements~~**. ~~(a) Within 30 days of the submission of the Hennepin county integration plan funded by a grant under Laws 1999, chapter 216, article 1, section 7, subdivision 6, or September 1, 2000, whichever is earlier, the policy group shall:~~

~~(1) assess the needs of state, county, and municipal government agencies for electronic fingerprint capture technology, electronic photographic identification technology, and additional bandwidth to transfer and access the data from electronic fingerprint capture technology and electronic photographic identification technology to the state's central database; and~~

~~(2) choose locations and agencies to receive this technology.~~

~~(b) Within the limits of available appropriations, the commissioner of public safety shall purchase and distribute the technology infrastructure improvements as directed by the policy group. The commissioner shall begin the purchasing process within 30 days of receiving notice of the policy group's decisions. The commissioner shall distribute the improvements as soon as practicable after beginning the purchasing process.~~

~~(c) If feasible, the policy group shall direct the commissioner to distribute the technology infrastructure improvements described in this subdivision in 100 locations. However, no more than 30 percent of the improvements may be distributed in one county.~~

~~Subd. 8~~9. **~~Documentation and reporting requirements~~**. ~~Every recipient of matching funds to develop or implement an integration plan shall submit to the policy group all requested documentation, including final plans and a report evaluating whether and how the development or implementation of the integration plan improved the operation of the criminal justice system in the requesting agency's jurisdiction. The policy group shall establish the recipient's reporting dates at the time funds are awarded.~~

Appendix C

CriMNet Legislative Proposal Overview
November 29, 2004

(Approved by the Criminal and Juvenile Justice Information Policy Group)

Section 1. Provides a cross reference to MN Stat. Chapter 13 in the CriMNet's 299C section.	**A new subdivision is added to Minn. Stat. 299C.65 Subd. 1a as follows:** 299C.65 Subd. 1a. Data classification. Data held by and accessible through CriMNet is classified under section 13.873.
Section 2. Amends the MN Gov't Data Practices Act **(MGDPA)** traveling data provisions to provide that data coming from the judicial branch shall follow court rules of access when in the possession of government entities. Currently, there are no provisions that provide for judicial data that comes to gov't entities.	**Create a new paragraph to MN Stat. 13.03 Subd. 4 as follows:** (e) To the extent that judicial branch data is disseminated to government entities by the judicial branch, the data disseminated shall have the same level of accessibility in the hands of the agency receiving it as it had in the hands of the judicial branch entity providing it.
Section 3, Subd. 1 Subd 1(a) defines "CriMNet" as a statewide system. Under the MGDPA, statewide systems have unique responsibilities. Subd 1(b) defines "CriMNet data" as criminal justice data that is held or accessed by CriMNet. Subd. 1(c) defines "audit trail data"	**Create a new section MN Stat Chapter 13:** 13.873 CriMNet data classification. Subd. 1. Definitions. (a)"CriMNet". For the purposes of this chapter, "CriMNet" is a statewide system as defined in section 13.02 Subd. 18, which integrates or interconnects data from multiple criminal justice agency information systems. (b) "CriMNet data" are criminal justice agency data created, collected, used or maintained in the prevention, investigation and prosecution of crime and any resulting criminal justice system response, held or accessed by CriMNet. (c) "audit trail data" are data created, used or maintained by CriMNet for the purposes of ensuring and verifying that CriMNet

	was only accessed by authorized persons for authorized purposes.
Section ~~5~~ 4. Creates a requirement for those law enforcement and community correction agencies operating secure juvenile detention facilities to fingerprint current probationers whose court disposition in suspense. This is for those persons still on probation for the offense in suspense.	**A new paragraph is added to Minn. Stat. 299C.10 Subd. 1(a) as follows:** (6) persons currently involved in the criminal justice process, on probation, parole, or in custody for the offenses in suspense whom the superintendent of the bureau identifies as being the subject of a court disposition record which cannot be linked to an arrest record, and whose fingerprints are necessary in order to maintain and ensure the accuracy of the bureau's criminal history files, to reduce the number of suspense files, or to comply with the mandates of MN Stat. 299C.111, relating to the reduction of the number of suspense files. This duty to obtain fingerprints for the offenses in suspense at the request of the bureau shall include the requirement that fingerprints be taken in post-arrest interviews, while making court appearances, while in custody or while on any form of probation, diversion or supervised release.
Section ~~6~~ 5. Creates a process where prosecutors can make a showing in district court to obtain fingerprints for persons involved in the CJS for a new offense who may also have an old conviction in suspense.	**Create a new subdivision in 299C.10 as follows:** Subdivision 1a. The superintendent of the bureau shall inform a prosecuting authority that a person prosecuted by that authority is the subject of a court disposition record in suspense which requires fingerprinting under this section. Upon being notified by the superintendent or otherwise learning of the suspense status of a court disposition record, any prosecuting authority may bring a motion in district court to compel the taking of the person's fingerprints upon a showing to the court that the person is the subject of the court disposition record in suspense.
Section ~~7~~ 6. ●Clarifies that the duty to fingerprint extends to agents, employees, subordinates of prosecutors, courts, probation. ●Allows taking of fingerprints of those currently on probation by law enforcement.	**Minn. Stat. 299c.10 Subd. 1(c) is amended to read as follows:** (c) Prosecutors, courts, and probation officers and their agents, employees, and subordinates, shall attempt to ensure that the required identification data is taken on a person described in paragraph (a). Law enforcement may take fingerprints of an individual who is presently on probation.
Section ~~8~~ 7.	**Minn. Stat. 299C.14 is amended to read as follows:**

Clarifies that penal institution officials must provide information necessary to ensure accuracy and reduce the number of suspense files.	299C.14 Information on released prisoner. It shall be the duty of the officials having charge of the penal institutions of the state or the release of prisoners therefrom to furnish to the bureau, as the superintendent may require, finger and thumb prints, photographs, distinctive physical mark identification data, other identification data, modus operandi reports, and criminal records of prisoners heretofore, now, or hereafter confined in such penal institutions, together with the period of their service and the time, terms, and conditions of their discharge. This duty to furnish information includes but is not limited to requests for fingerprints as the superintendent of the bureau deems necessary to maintain and ensure the accuracy of the bureau's criminal history files, to reduce the number of suspense files, or to comply with the mandates of Minn. Stat. 299C.111, relating to the reduction of the number of suspense files where a disposition record is received that cannot be linked to an arrest record.
Section ~~9~~ 8. Brings this statutory provision in line with the provisions of Rule 9.01, Subd. 1 of the Minn. Rules of Criminal Procedure (requiring prosecutors to disclose witness conviction histories to defense counsel). Clarifies that CriMNet may be used to obtain authorized information. Also clarifies that prosecutors' data systems are unavailable to public defenders.	**Minn. Stat. 611.272, is amended to read as follows:** **611.272 Access to government data** The district public defender, the state public defender, or an attorney working for a public defense corporation under section 611.216 has access to the criminal justice data communications network described in section 299C.46, as provided in this section. Access to data under this section is limited to data ~~regarding the public defender's own client as~~ necessary to prepare criminal cases in which the public defender has been appointed, as follows: (1.) access to data about witnesses in a criminal case shall be limited to records of criminal convictions; (2.) access to data regarding the public defender's own client which includes ~~including~~, but is not limited to, criminal history data under section 13.87; juvenile offender data under section 299C.095; warrant information data under section 299C.115; incarceration data under section 299C.14; conditional release data under section 299C.147; and diversion program data under section 299C.46, subdivision 5. The public defender has access to data under this section whether accessed via CriMNet or other methods. The public defender does not have access to law enforcement active investigative data under section 13.82, subdivision 7; data protected under section 13.82, subdivision 17; or confidential arrest warrant indices data under section 13.82, subdivision 19, or to data systems maintained by a prosecuting attorney. The public defender has access to the data at no charge, except for the monthly network access charge under section 299C.46, subdivision 3, paragraph (b), and a reasonable

	installation charge for a terminal. Notwithstanding section 13.87, subdivision 3,; 299C.46, subdivision 3, paragraph (b); 299C.48, or any other law to the contrary, there shall be no charge to public defenders for Internet access to the criminal justice data communications network.

Appendix D

December 15, 2004

To: Recipients of the CriMNet Annual Report
Re: Data Practices considerations

The CriMNet data practices legislative proposal for 2004 required the Criminal and Juvenile Justice Information Task Force (Task Force) to submit a report to the legislature regarding a number of data practices concerns, including web-based access to CriMNet data by data subjects, coordination of data challenges, using CriMNet for non-criminal justice background checks, and other matters.

Though the full 2004 legislature ultimately did not vote on the submitted legislative proposal, the Task Force initiated the study and, with the approval of the Criminal and Juvenile Justice Policy Group (Policy Group), is submitting the attached report.

The Data Practices Delivery Team of the Task Force spent much of 2004 examining the issues regarding access by data subjects, subscription, and non-criminal justice background checks. While the group considered the enormous range of possibilities that technology brings to criminal justice information sharing, it also recognized the complexities and the care with which information should be managed in this electronic age.

Primarily, the report examines the potential inadvertent collateral consequences that may be triggered by otherwise well-intended recommendations regarding data policy. As a result, the report contains does not propose specific statutory language; rather, it highlights possible solutions, policy-related considerations, and offers real-world scenarios to add context to the discussion.

Ultimately, policy making regarding electronic information requires a careful balance between the need for criminal justice agencies to share data and the rights of individuals to access their data and to know who else is accessing their data.

The Data Practices Delivery Team, Task Force, and Policy Group expect discussions regarding these issues to continue. Members of each group welcome the opportunity to continue to participate in these discussions.

Respectfully submitted,

Robert Sykora
Chair, Data Practices Delivery Team
First Vice Chair, Criminal and Juvenile Justice Information Task Force

Criminal & Juvenile Justice Information Task Force and Policy Group

CRIMNET DATA POLICY REPORT

Approved by Task Force on November 5, 2004.
Approved by the Policy Group on December 15, 2004.
Amended by the Policy Group on March 23, 2005

Executive Summary

In 2003, the Criminal and Juvenile Justice Information Task Force and Policy Group worked on data practices issues extensively, and the Legislature utilized these recommendations as it debated data policy during the 2004 session. Recognizing that many such policy questions remain unresolved following those efforts and noting that discussions during the 2004 session highlighted new issues, the Task Force asked its Data Practices Delivery Team[3] to augment the 2003 recommendations with further policy development. The Delivery Team developed this report's basic content in several meetings between March and October 2004.

Task Force members received this document in draft form just before its October meeting, having a month to review it prior to discussing and amending it during a two-hour session at its November 5, 2004 meeting. With a single dissenting vote, the Task Force voted to approve the contents of this document. The Policy Group considered the report at its November 29th meeting and approved it unanimously on December 15, 2004.

The Policy Group and Task Force in this document set forth relevant issues and develop illustrative scenarios that are intended to be helpful to policy makers as they work to understand the full impact of statutory provisions intended to guide the creation and use of CriMNet.

Addressed in this document are three substantive areas: (1.) data challenges and coordination; (2.) public access and expanded data subject access; and, (3.) access and use of private data by non-criminal justice professionals. We were also concerned with the possibility of federal-state conflicts of laws on data practices issues but learned from the Department of Administration's Information Policy and Analysis Division (IPAD) that an IPAD summer intern researched the issue and determined, to the division's satisfaction, that no serious conflicts were found.

The primary theme of this document is an examination of the possible inadvertent collateral consequences that could be triggered by otherwise well-intended data policy recommendations. This examination involved protracted discussion and debate at all levels. The Task Force is grateful to all those who contributed their time and energy to further this effort.

--Robert Sykora
Task Force vice chair, Data Practices Delivery Team chair

[3] Data Practices Delivery Team membership list is attached as Appendix A.

Contents

DATA CHALLENGES AND COORDINATION

I. At Issue

A key goal of CriMNet is to provide complete and accurate data regarding individuals in the criminal justice system. To support that goal, it follows that CriMNet aims to assure that any disputed data or incomplete records be remedied, and that individual's rights under the Minnesota Government Data Practices Act (MGDPA) be upheld. To that end, the Data Practices Delivery Team recommends the establishment of a coordinated data challenge process and certain technical design enhancements.

II. Background and processes governed by current law

Under Minn. Stat. 13.04, Subd. 4, subjects of data can challenge the accuracy and/or completeness of public and/or private data kept about them by a government entity. A data subject can only challenge data and cannot challenge other things, such as the procedures a governmental entity uses to give or deny a person some benefit.

To initiate a data challenge, a data subject must make a written challenge to the responsible authority for the government entity that keeps the data. For many data subjects, locating the correct responsible authority is a difficult process. In some instances, data may be held by more than one entity. Data challenges may be made to each entity which keeps the data to be challenged or can be made to the originating agency which then has an obligation to pass changes to all other entities that received the data. (Individuals can challenge at each entity, but can start with the first and, assuming that the data there are corrected, individuals can require that other recipients be notified.)

Within agencies, few employees are familiar with the terms "data challenge," "responsible authority" or "data practices compliance official" or with the process of challenging data. Agency heads are frequently unaware that they are the responsible authority or data practices compliance official (DPCO) for their agency under the Minnesota Government Data Practices Act. For many agencies, receiving a data challenge is extremely rare.[4] In the written data challenge request, the data subject should specifically identify how or why the data are

[4] To-date, there have been no MGDPA data challenges to the systems which may be searched using CriMNet..

inaccurate or incomplete. The data subject should propose how the data should be corrected by adding, changing, deleting or removing data.

The responsible authority of each government entity will determine how that entity will review data challenges and what steps will be taken to make a determination of the accuracy and/or completeness of data. ***The best way to set requirements is to establish requirements for the process and the content of data challenges in the individual entity's data practices policies and procedures.***

The responsible authority has 30 days to review and make a determination on the validity of a data challenge. During this 30-day timeframe, the disputed data can only be disclosed if the data subject's statement of disagreement is included with the disclosure. The responsible authority can agree with all, part or none of the challenge. If the responsible authority agrees with the challenge, he/she must make the changes the data subject requested as soon as is reasonably possible, and make reasonable efforts to notify anyone who received the data in the past, including anyone the data subject requests be notified.

If a data challenge is rejected, the data subject can appeal that decision to the commissioner of the Department of Administration. The time period for appealing is 60 days for data subject who are notified of the right to appeal by the responsible authority and 180 days for those who receive no notice of their appeal rights.

III. Suggested ways CriMNet can assist with data challenges

Background

Currently, CriMNet does not maintain, copy or store data from participating repositories. At some point, CriMNet will maintain copies of certain key data elements, also known as "index information," from each source system. This method speeds searches and ensures that some minimal data is always available even when a source system is off-line. Currently, CriMNet has other data that can be challenged, but the vast majority of the anticipated challenges will be for individual criminal justice data that is maintained at the local level or in a state repository; such as, Statewide Supervision System or Computerized Criminal History. By statute, data challenges for the source system data should be directed to that system.

- **Possible Business Solutions**

  Note: These items indicate possible solutions for assisting agencies.

  1. ***Provide ability to access contact information for the responsible authority and data practices compliance official designated by each source system, along with contact information (excluding the judicial branch).*** As previously mentioned, finding the responsible authority is often an enormous challenge for data subjects. Having a CriMNet website listing would assist both data subjects and participating agencies. Through the CriMNet user agreements, agencies participating in CriMNet would agree to provide CriMNet with the name and contact information for their responsible authority and DPCO (with updates as they occur). It may be possible for CriMNet to develop an interface which allows source systems to update this information versus providing updates in a manual manner. The website would also notify the public that judicial branch data are subject to Court Rules of Access and that if they wish to challenge judicial branch data they should contact a county court administrator's office.
  2. ***Develop a means to indicate disputed data in CriMNet and include a dispute statement.*** Currently, there is no means to identify disputed data that is displayed on the CriMNet Search System. Local source systems/repositories have not been developed to easily allow disputed data to be flagged and accompanied with the disputed statement. When challenges occur, frequently source systems either provide challenge information in comment fields or completely remove data during the challenge period.
  3. ***Provide identification and dissemination of the location of data on an individual data subject.*** Currently individuals are required to check each criminal justice agency (more than 1,500 in Minnesota) to determine who has data about them. CriMNet can assist data subjects by providing them with a list of agencies that have contributed data about them to source systems that are displayed on the CriMNet Search System. Data subjects may be aware of data they wish to challenge in one source system, but unaware of all of the locations where that data may also be maintained. Providing listing of agencies to the data subject would facilitate their more easily challenging and correcting data.

4. ***Serve as resource to data subject seeking to locate the appropriate source system for the purposes of making a data challenge.*** CriMNet could serve as a resource to data subjects seeking to locate the appropriate source system responsible authority to submit a challenge. There may be instances where even data subjects do not know where certain data they wish to challenge originated. The CriMNet responsible authority or CriMNet DPCO could access CriMNet to determine who the appropriate responsible authority (RA) is to receive the challenge. The DPCO or Responsible Authority would notify the data subject of the responsible authority.

5. ***Provide technical assistance in data challenges to local agencies (by CriMNet responsible authority and data practices compliance official).*** As previously mentioned, data challenges are rarely received by some local agencies. With the limited experience in processing a challenge, many agencies would welcome the assistance from CriMNet when they receive a challenge on how to appropriately process the challenge. CriMNet RA and DPCO officials could provide technical expertise and assistance to local agencies to meet their challenge obligations.

6. ***Provide model policies.*** CriMNet could offer participating entities model policy and procedure language on what is required to make a data challenge.

- **Possible Technical Solutions**

  Note: There are a number of technical solutions that could, subject to cost-benefit analysis, assist citizens in the data challenge process. Following are examples of the kinds of solutions that can be considered.

  1. ***Develop a display icon in the CriMNet summary which, when activated by the data custodian, would show that data are disputed.*** In addition, CriMNet could add clear warning information in the detail to indicate that the data are disputed and provide the statement of dispute.

  2. ***Create a centralized disputed data service (CDDS).*** The CDDS service would allow agencies to access and then manage disputed data that are published on the CriMNet site. This solution could be flexible enough to support flagging of data or to actually help track and document the dispute through the whole business process.

This solution could provide a viable alternative to the many agencies that do not have a dispute module within their core records management system as mentioned previously.

3. ***Provide messaging to assist agencies with communications during the Disputed Data Process.*** Agencies may be required to communicate with a number of contacts from other criminal justice agencies, as well as the data subject, during the data challenge. These contacts can vary. Communications may be required with other originating agencies, Department of Administration (in cases of appeal), and other individuals within an agency (besides the Responsible Authority/ DPCO).

   It is the originating responsible authority that has the capabilities to review the issue within the proper context and to make changes to the source data when necessary. For these purposes the "originating responsible authority" is the person in the entity where the data problem first exists. A CriMNet Workflow Messaging and Subscription-based solution could be utilized to assist agencies with communicating relevant information and increase efficiencies in the data challenge process. Such a messaging solution would help facilitate and focus the process so that the agency's responsible authority handles the dispute quickly. For data subjects, the subscription-based solution could be utilized to help agencies quickly and consistently communicate information to individuals that are not criminal justice agencies but are involved in the dispute.

4. ***Develop personal identification numbers (PINs) system for data subjects.*** Developing and providing a PIN process could assist data subjects by allowing greater on-line data practices services and access to information. A legislative change to classify and protect PIN data may be appropriate prior to implementation of this system.

5. ***Improve ability of agencies to contact those who accessed disputed data being corrected.*** Enhanced audit trail information through CriMNet could enable source agencies to better meet their obligations to make reasonable efforts to notify known users who accessed data that has been challenged and corrected.

- **User Agreements**

A number of enhancements to the coordination of data challenges for agencies and data subjects could be addressed by incorporation into the CriMNet user agreement/contract with participating agencies and repositories without statutory change.

The following are examples of items that could be an incorporated as duties of the agency/repository wishing to participate in CriMNet:

1. Inform and update CriMNet on the responsible authority/data practices compliance officer for your data
2. Agree to allow CriMNet to assist the agency in data challenges that come to CriMNet on your data
3. Agree to place a notice in the CriMNet integrated system when you receive a data challenge.

The following are examples of some technical tools that CriMNet could agree to provide and fund:

1. Provide for automated flagging of data in multiple places when challenged, post statement of disagreement
2. Be a place where data subjects can be assisted in locating the appropriate source system to make a data challenge.
3. Coordinate determining accuracy/completeness of data challenged with locals.
4. Provide for improved tracking to determine who received bad data and provide mechanism for notice to those who received it.
5. Provide technical assistance, as needed, for data challenges.
6. Provide model policies and procedures for the content of data challenges.

PUBLIC ACCESS / EXPANDED DATA SUBJECT ACCESS VIA CRIMNET

I. At Issue

In examining this issue, the delivery team quickly concluded that questions about broader access to information raise deeply complicated issues. The group focused its suggestions on the issue of subscription, in direct response to legislation proposed during the 2004 legislative session, though other policy considerations are defined and explained. In essence, more issues were raised than could be fully explored at this time, and the delivery team expects to contribute further to this effort.

All in the working group agreed that data subject access via subscription would have negative, unintended consequences. What

follows are real-life scenarios intended to illustrate the potential consequences of a broadly accessible subscription service.

CriMNet recognizes the rights of individuals to have access to data about themselves; however, subscription is not the proper mechanism to deliver that information. There are a number of other ways to provide access to data subjects that do not carry the volume of unintended consequences inherently associated with subscription services.

II. Subscription

- **Background**

1. *Subscription* is a technology enhancement planned for CriMNet that would allow a subscriber to receive notification, either via email or other alert, that new information is available via CriMNet, based on the subscriber's identified criteria. *For example*, this subscription feature was conceived to allow a probation officer to receive alerts in the event a probationer had an arrest or conviction in another jurisdiction.
2. *Auto-Subscription* involves a subscription service that provides automatic notification when new information about a data subject is available, or a search has been performed.
3. *Consent to Subscription* would allow the data subject to consent to have others receive subscription updates about the consenter.

- **Considerations:**

1. Subscription services should be limited to criminal justice professionals. Within their properly defined roles there are existing institutional constraints on what data they see and how they may use it.
2. Data subjects should have access to data about themselves, but it should be provided through a non-subscription function.

Rationale:

- **POSSIBLE CONSEQUENCE: Subscription may tip-off someone involved in an investigation and hamper that investigation.**

Scenarios

1. Bench warrants ordinarily are issued in open court, therefore are public record. Potentially, an individual allowed to subscribe to his or her own criminal justice

system data could get a notification email advising the subject that a warrant has just been issued for their arrest. It could be a safety risk for law enforcement serving arrest warrants to provide advance knowledge to the subject of the warrant.

2. A victim of domestic violence reports a situation to the police, who investigate and determine there is insufficient evidence to proceed and close the case, making it public. The perpetrator receives a notification that a complaint has been made against him.
3. A child has alleged abuse against a parent and police are investigating. While the investigation is active, the Minnesota Government Data Practices Act would allow the parents with a subscription to get notice that law enforcement has confidential information. Once the investigation is closed, the parents would be able to get access to the substance of the report. (When police interview a juvenile, they must ask if that juvenile does not want her/his parents notified. If the answer is "yes," the information could not be provided to the parents.)
4. Individuals involved in criminal enterprises – such as prostitution, drug trafficking, or gangs – could subscribe via consent to criminal justice activities related to members of their enterprise, including their encounters with law enforcement or the courts.

- **POSSIBLE CONSEQUENCE: Individuals may be compelled to give consent to subscription for others to receive notifications about private data resulting from their interaction with criminal justice entities.**

Scenarios:

1. Allowing landlords, employers, and other individuals in positions of power to monitor criminal justice system data, via subscription, about their prospective employees, tenants, etc. could result in decisions regarding housing and employment being based on incomplete information.

2. For example, Employee or Tenant is considered a suspect in a burglary investigation, and is later cleared. However, Employer or Landlord, having subscribed by consent to the person's criminal justice data, receives notification of that person's suspect status and may base decisions solely on that information.
3. Even victims and witnesses will have their names associated with a closed, and therefore public, criminal case.

- **POSSIBLE CONSEQUENCE: When investigations prompt law enforcement to search records based on broad criteria in an attempt to narrow down clues and identify suspects, notification to all the subjects whose names were retrieved is impractical and burdensome to the criminal justice system.**

Scenarios:

1. An officer searches for an unnamed person with the characteristics of a Caucasian male in a red Camaro. There may be a number of hits, resulting in every Caucasian male with a red Camaro receiving notification or the real unknown subject being tipped off that law enforcement is looking for him.
2. An officer searches for a common name, such as Michael Johnson and returns hundreds of hits. Though the officer may only select one or two records to pursue, every Michael Johnson with a subscription would receive notification that his record was searched.

III. Other Policy-Related Considerations

A. Identification

- **Proper identification** of an individual is essential, and there is already a significant problem in the criminal justice system with assuring that a data subject is properly attached to the correct record. Criminal justice professionals have the resources to cross-check to verify that they have the right person. Members of the public will not have that option.

- **Consent to subscription and identity theft issues.** Policymakers should consider that methods must be in place to verify individuals are who they say they are, and to rectify errors if a theft of someone's identity takes place.

  Scenarios:

  1. Ron Johnson submits a rental application, but uses Carl Perkins' name and identifying details. Ron, posing as Carl, consents to the landlord receiving a subscription to Carl's criminal justice information accessible via CriMNet.
  2. If Ron commits a crime while using Carl's name, the record really belongs to Ron, not Carl. As long as the record of a crime is present and available to employers, landlords, schools, lenders, etc., Carl is severely disadvantaged. Wider and more rapid dissemination of these data makes the negative consequences more severe.

B. **Business Practice Issues**

- **Context and access.** When criminal justice information is disseminated to the public, it must be complete, accurate and contextual. There are situations where a human gatekeeper may be necessary to explain data, provide the necessary context, or to make decisions about proper dissemination under the Minnesota Data Practices Act.

Scenarios

1. Criminal justice professionals are bound by the legal constraints inherent to their jobs, what data they may see and how they may use it. Those constraints are enforced by the agencies they work for. The law requires that criminal justice agencies and their employees abide by these constraints. These are institutional controls to assure they abide by the law. When access to data is granted outside the boundaries of that controlled environment, there is no way to control how that information will be used.
2. Information provided either on paper over the counter or via a computer terminal in a criminal justice agency has the advantage of allowing the requestor to ask clarifying questions – about the contents or the correct identity of its subject. The same opportunity to clarify does not exist when information is gathered electronically from a remote location (e.g. from one's

home). While the opportunity to contact the agency for clarification is there, people gathering information at remote locations are less likely to take that step. The increased chance of misunderstanding or misinterpreting the criminal justice data increases the chance of communicating bad information. Incorrect information will either hamper the potential public safety benefit of these systems or result in a disadvantage to the data subject.

3. When corrections need to be made, an inaccurate, opened electronic record cannot be called back for correction
4. Online access to personal data by the public is different primarily because of the lack of legal controls such as training and employee accountability. Government employees accessing data can be held to standards of conduct whereas members of the general public cannot.

- **Terms of subscription privileges.** Without expiration of subscription by consent, the result would be a lifetime of monitoring. For example, an ex-employer or former landlord could continue to have the ability to see private data on the subject of the data. This doesn't mean electronic dissemination is to be avoided; it simply means that a new set of policies should be considered to intelligently regulate the process of electronic dissemination.

Scenario

1. Sexual assault data is private to the victim, but if by consent a victim released data to an employer or landlord, that victim could potentially be vulnerable to embarrassment or to further victimization. One solution may be putting in place a business practice to revoke subscriptions if the information is used inappropriately.

C. Data Classification

- ***Proper and timely data classification is an essential, underlying concept that must be a part of any analysis of these issues.***
- In this context, *data classification* refers to the decision by the originating agency as to how a piece of data is classified under the Minnesota Government Data Practices Act (MGDPA): confidential (*e.g.*, active law enforcement investigatory data); private (*e.g.*, sexual assault victim data); or public (all other data;

note that all data are public under the MGDPA unless classified otherwise)

- **Dynamic data classifications create an obstacle as CriMNet attempts to provide public data and data subject access.** Access to data via CriMNet is premised upon the timely and accurate data classification process at the originating and submitting agency level. Put simply, CriMNet cannot properly allow access to certain data if the originating agency doesn't tell CriMNet how the data is classified. Another aspect of the dynamic data classification problem is what to do when data, once released under consent, change their classification and become confidential again.

Scenario

1. A law enforcement investigation may be active on Monday and inactive by Friday. From a Data Practices Act perspective, it is classified as confidential on Monday and public on Friday. The CriMNet Responsible Authority has no way of knowing whether the local agency considers the data active or inactive, and so will be unable to make a decision about release of audit trail data.

- It is not just current and ongoing data that have to be classified and reclassified. The entire historical record must be maintained subject to record retention laws. Old investigations can become active, and active investigations can become inactive.
- If a person gets data subject's consent on Monday, and gets the data on Tuesday, but the classification changes to confidential (e.g., a reactivated law enforcement investigation) on Wednesday, how can the person receiving the data be prevented from disseminating it downstream? How can this release of now-confidential data be restricted?
- **Intermingled data in law enforcement reports**. If person A's confidential data is in a police report right next to Person B's private or public data, release of the report by CriMNet would be complicated. Police reports are a tangle of public, private and confidential data and require manual redaction before release. We are not aware of any currently-available technology that can on a "lights-out" basis (i.e., no human involvement) solve the dynamic classification problem and make a determination which data can and which cannot be released.

ACCESS AND USE OF PRIVATE DATA BY NON-CRIMINAL JUSTICE PROFESSIONALS, VIA CRIMNET

I. At Issue

While currently, the public is not able to use CriMNet to access computerized criminal history information, there may be a time in the future when that functionality is available. In anticipation, the following section explores both current practices and considerations if this future enhancement is explored.

II. Non-criminal justice entities accessing private data under current practices

Public Entities

Statutorily Mandated Checks

(for public safety or employment decisions)

Alcohol & Gambling Enforcement	Casino employees
Department of Human Services	Foster care & Daycare licensing; health care; personal care
Driver & Vehicle Services	School Bus Drivers; Driving instructors
School Districts	District employees; contractors; volunteers
Department of Education	Teacher license applicants
Private Detective Board	Private Investigator License Applicants
Board of Social Work	Social Worker's License Applicants
Fire Departments	Firefighters
Secretary of State	Voters to determine eligibility to vote
Federal Public Housing Programs	Public Housing applicants
Cities	Child Services Workers
Public Housing Authority	Public Housing Applicants
Social Service Agencies	Adoptive parents/household members
Department of Commerce	Check Cashing facility owners/operators; Bail Bondsmen

Informed Consent/Others
(for public safety, verification or application approval)

Government Agencies (Cities, Counties, State & Federal)	Employment Applicants
Social Security Administration	S.S. recipients

Private Entities

Statutorily Mandated Checks
(For application approval)

Security/ Private investigation firms	Security guards & investigators
Management companies/landlords	Apartment Managers
Bus companies	Passenger Carriers
Churches, Camps, etc	Child Services Workers
Social Services	Adoptive parents/household members

Informed Consent/Others

General Employers	Employment Applicants
Management companies/landlords	Tenant Applicants

Research, Policy and Program Evaluation

Researchers[5]	Media
	Government Agencies
	Universities
	Individuals
	Non-profits

III. Non-criminal justice entities who currently need more than CCH data

- Department of Human Services and other state agencies (e.g. DPS) must be notified if individual is subsequently convicted of (or in some cases charged with) a disqualifying offense.
- Researchers
- If they (other entities listed above) could get it, they'd want it.

[5] For access to private data, researchers must sign non-disclosure agreement.

IV. Future considerations

1. Demand for background checks driving CriMNet design.
    - Keep in mind purpose of statutorily mandated background checks.
    - Keep in mind purpose of CriMNet.
    - Better criminal justice system.
    - Better background checks for statutorily mandated checks.
    - No need to be influenced by Non-Criminal Justice entities that are not statutorily mandated to do background checks.
    - Exception-researchers for use in policy making, program evaluation, and budgeting.
2. Anticipated future demands for information through CriMNet

Public Safety-Related Checks

Benefits · Immediate, up-to-date information · Increased public safety	Barriers · Current statutes don't allow · How would entities access CriMNet? · What information do entities have access to and how would that be determined?
Dangers · Misidentification · Too new; not enough time to confirm; in-process outcome unknown	Consequences · An individual doesn't get a job or loses a job, housing or other benefit

<u>Employment-Related Checks</u>

Benefits · More appropriate hires	Barriers · Individual privacy rights
Dangers · Misidentification · Too new; not enough time to confirm; in-process outcome unknown · Hiring decisions made arbitrarily, which hampers rehabilitation	Consequences · Increased unemployment · Increased recidivism · Increased racial and economic disparities

Housing-Related Checks

Benefits	Barriers
· More appropriate tenant decisions	· Individual privacy rights
Dangers · Housing decisions made arbitrarily, which undermines rehabilitation · Hurts an individual's ability to obtain housing	Consequences · Increased homelessness · Increased recidivism · Increased racial and economic disparities

Policy, Program Evaluation and Budgeting Research

Benefits	Consequences
· More efficient budgeting · More comprehensive data resulting in better informed policy making · Increased public oversight and accountability	· How do they obtain extract data?
Dangers · Not understanding the data · Third-party dissemination of identifying data	

For-Profit Uses of Data

Benefits	Barriers
· None	· Individual privacy rights
Dangers · Not understanding the data · Third-party dissemination of identifying data	

Note: In all cases, the primary liability lies with: CriMNet, other agencies providing the data, and agencies making decisions.

3. Data held by non-criminal justice agencies that may be beneficial to criminal justice agencies through CriMNet:
    - Financial data-for public defender determination.
    - Driver License Information.
    - Health data-to determine eligibility for gun permits (commitments through DHS).
    - DNR-violations, hunting licenses.
    - Civil court data.

Note: Use of this data would require that the purposes for use be defined and that guidelines differentiate between public and private non-criminal justice agencies.

4. Other issues to address
    - Data privacy
    - Duty for providing access and appropriate processes for providing access.

APPENDIX A

DATA PRACTICES DELIVERY TEAM MEMBERSHIP

Area	Voting member and designated proxy
County Attorney	Phil Carruthers
	Proxy:
Defense	Bob Sykora (chair)
	Proxy: Steve Holmgren
County Corrections	J. Hancuch
	Proxy: Dave Gerjets
Department of Corrections/S3	Deb Kerschner
	Proxy: Dan Storkamp
Court Administrators	Susan Stahl
	Proxy: Jane Morrow
Appellate Courts	Deb Dailey
	Proxy:
MNCIS	Nancy Harms
	Laurel Higgins
Sentencing Guidelines	Barbara Tombs
	Proxy: Jill Payne
Sheriff	Bob Fletcher
	Proxy: Dave Fenner
Local law enforcement	Ron Whitehead
	Proxy:
BCA	Julie LeTourneau
	Proxy: Susan Rico
Information Policy & Analysis / Dept of Admin	Katie Engler
	Proxy:
Attorney General	Angela Helseth
	Proxy: Jeff Bilcik
Public	Terri Nelson, ACLU of Minnesota