



State of Montana
Montana Board of Crime Control

Agency IT Plan
Fiscal Year 2012-2017

Prepared July 2012

Brooke Marshall, Executive Director
Jerry Kozak, IT Manager



Board of Crime Control
5 S Last Chance Gulch
PO Box 201408
Helena MT 59620
(406) 444-3604
www.mbcc.mt.gov

Table Of Contents

EXECUTIVE SUMMARY	1
SECTION 1: AGENCY ADMINISTRATIVE INFORMATION	2
SECTION 2: AGENCY IT MISSION	3
<i>2.1 Agency IT Mission Statement.....</i>	<i>3</i>
SECTION 3: AGENCY REQUIRED PROGRAMS	4
<i>3.1 Security Program.....</i>	<i>4</i>
SECTION 4: AGENCY IT PLAN – GOALS & OBJECTIVES	7
<i>GOAL NUMBER 1:.....</i>	<i>7</i>
<i>GOAL NUMBER 2:.....</i>	<i>8</i>
<i>GOAL NUMBER 3:.....</i>	<i>9</i>
<i>GOAL NUMBER 4:.....</i>	<i>10</i>
SECTION 5: IT INITIATIVES (FY2012 – FY 2017).....	12
SECTION 6: ENTERPRISE ALIGNMENT.....	13
SECTION 7: PLANNED AGENCY IT EXPENDITURES	14
SECTION 8: ADDITIONAL INFORMATION - OPTIONAL	15

EXECUTIVE SUMMARY

The Montana Board of Crime Control (MBCC) is pleased to have the opportunity to present its IT Plan. There are currently a number of projects underway to enhance its information technology systems. These applications and databases have become critical players in the process of supporting our mission. Several major custom applications have recently been implemented. MBCC is proud of the success of these systems and they have been well received by our customers and the public.

Our Grant Management Information System (GMIS) is a great success. It tracks and automates most of the grant management activities within the agency. It has been recently enhanced to provide better access for external customers.

Our Montana Incident Based Reporting System (MTIBRS) has put Montana at the forefront of state crime data collection. We are very excited about upcoming opportunities to add Indian Lands crime statistics to our database. MBCC has recently implemented a new MTIBRS repository application. This is a highly automated system that better utilizes our MTIBRS subject matter experts and analysts time. It also provides a web based data input tool that is available at no cost to tribal and other small agencies who previously did not report crime statistics.

In addition, MBCC has implemented a state of the art MTIBRS Online Reporting System that provides highly customizable crime data reports, charts and graphs to law enforcement and the public. This was a 2009 EPP item.

MBCC has implemented a Juvenile Detention Reporting System (JDERS) that improves oversight and management in this very important area. Last legislative session, MBCC had an EPP item to provide funding for maintenance and user interface fees for this system.

The Board has also replaced an aging Victim Services Tracking System with a state of the art web based application. This will improve the ability of local victim service agencies to track the services they provide and has greatly enhanced compliance reporting.

MBCC continually works with its partners in the field and other states to review and analyze its use of technology to ensure that it employs cost effective, and well received IT solutions.

SECTION 1: AGENCY ADMINISTRATIVE INFORMATION

Role: Plan Owner

Name: Brooke Marshall
Telephone Number: (406) 444-3615
Email Address: BrookeMarshall@mt.gov

Role: IT Contact

Name: Jerry Kozak
Telephone Number: (406) 444-1621
Email Address: JerryKozak@mt.gov

Role: IT Contact (Alternate)

Name: Don Merritt
Telephone Number: (406) 444-2076
Email Address: DMerritt@mt.gov

Role: Information Security Manager (ISM)

Name: Jerry Kozak
Telephone Number: (406) 444-1621
Email Address: JerryKozak@mt.gov

IT Inventory

The IT inventory database located at <http://mine.mt.gov/enterpriseitinventory> was updated on April 13, 2012. As required by MCA 2-17-524(3)(c) the plan will be updated by June 30th, 2012.

SECTION 2: AGENCY IT MISSION



2.1 Agency IT Mission Statement

The Montana Board of Crime Control's mission is to proactively contribute to public safety, crime prevention and victim assistance through planning, policy development and coordination of the Justice systems in partnership with citizens, government and communities.

Through the Board's grant allocation and research and analysis programs, the Board plays an important role in shaping the IT environment of state and local criminal and juvenile justice systems.

SECTION 3: AGENCY REQUIRED PROGRAMS

Information Security Management (ISM) Program General Description

3.1 Information Security Management (ISM) Program

The Montana Board of Crime Control (MBCC) takes security seriously. It has an information security program that is compliant with MCA 2-15-114. MBCC is currently in the process of examining the National Institute of Standards and Technology (NIST) framework for the development of a comprehensive plan for the reduction of risks the Agency is exposed to through the utilization of electronic information systems data processing. The objectives of utilizing NIST is to provide a proven and accepted approach in conducting risk assessments, developing IT policies, enhancing security controls and developing procedures for detecting and responding to incidents. In addition, the NIST framework will be used to develop plans and procedures for the continuity of MBCC IT operations. This is in alignment with the State of Information Technology Service's direction for an enterprise approach to protect sensitive and critical information being housed and shared on State and/or external/commercial information assets or systems.

MBCC obtains information technology services from the SITSD from the Department of Administration through service level agreements. MBCC information technology services being obtained from SITSD provide compliance with industry adopted guidelines and standards such as NIST.

3.1.a Workstation and Network Security

Individual workstation/network security is provided by Montana Windows Active Directory membership for all users and computers. This directory and the network over which it runs is owned and managed by the Department of Administration, State Information Technology Services Division (DOA SITSD).

3.1.b Database Servers

MBCC owns and manages two database servers. It utilizes industry standard security measures and user specific access security for all server access.

3.1.c Backup and Recovery

All but a few remaining databases are housed at the DOA SITSD Data Center and backed up there. These remaining databases are backed up nightly and the data is stored on the MBCC File & Print server which is housed at the DOA SITSD Data Center. An additional backup of all critical files is performed to encrypted portable hard drives once per week and stored in the MBCC safe. Periodic test restores are performed.

3.1.d Virus Scanning and Patching

All MBCC workstations, laptops and servers utilize state standard ESET NOD32 virus scanning software. Workstations and servers automatically receive current Windows patches from the DOA SITSD WSUS patching network. Laptops also utilize NOD32 and are manually patched on a regular cycle.

The agency's information security management program is challenged with limited resources, manpower and funding. While alternatives are reviewed and mitigation efforts are implemented, the level of acceptable risk is constantly challenged by the ever changing technology and associated risks from growing attacks and social structure changes. Specific vulnerabilities have been identified which require restructure, new equipment, or personnel positions (funds increase), and are addressed below in our future plans.

3.2 Future Security Program Plans

MBCC, as described in NIST SP 800-39, will develop and adopt the Information Risk Management Strategy to guide the agency through information security lifecycle architecture with application of risk management. This structure provides a programmatic approach to reducing the level of risk to acceptable levels.

This program has four components, which interact with each other in a continuous improvement cycle. They are as follows:

- Risk Frame – Establishes the context for making risk-based decisions
- Risk Assessment – Addresses how the agency will assess risk within the context of the risk frame; identifying threats, harm, impact, vulnerabilities and likelihood of occurrence
- Risk Response – Addresses how the agency responds to risk once the level of risk is determined based on the results of the risk assessment; e.g., avoid, mitigate, accept risk, share or transfer
- Risk Monitoring – Addresses how the agency monitors risk over time; “Are we achieving desired outcomes?”

The top critical controls we will begin to examine include the following:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Software Security
- Wireless Device Control

- Data Recovery
- Security Skills Assessment and Appropriate Training
- Controlled Use of Administrative Privileges, Least User Rights Implementation
- Maintenance, Monitoring, and Analysis of Security Audit Logs
- Controlled Access Based on the Need to Know
- Account Monitoring and Control
- Data Loss Prevention
- Penetration Tests and Risk Assessments

3.3 Continuity of Operations (COOP) Capability Program General Description

The Department of Administration Continuity Services develops agency's Continuity of Operations Capabilities, which provides the plans and structure to facilitate response and recovery capabilities to ensure the continued performance of the State Essential Functions of Government. This program involves two Blocks of focus; the first is to complete the Business Continuity Plans (BCP) involving two phases, the second Block works on the specific business processes or activity plans such as Emergency Action Plans (EAP), Information System Contingency Plan (ISCP), Communications Plans, Incident Management Plans, and more. This program is not a standalone process in that information which is identified and recorded under this structure can and often exists in the Records Management Program and associates with Information Security Management Program requirements.

Integration of these three programs is critical to the confidentiality, integrity, and availability of information, which is associated with each program.

MBCC is in the discovery phase of utilizing the Living Disaster Recovery Planning Software (LDPRS) which is provided by SITSD to facilitate the development of the continuity plan for MBCC data processing operations.

3.4 Future COOP Program Plans

MBCC is planning to utilize the Living Disaster Recovery Planning Software (LDPRS) which is provided by SITSD. MBCC will be relying on the Security and Continuity Services section of SITSD to provide guidance and instruction on the use of LDPRS. MBCC plans to join with the Department of Administration Continuity Services for the development of our agency's Continuity of Operations Capabilities, which will provide the plans and structure to facilitate response and recovery capabilities to ensure the continued performance of the State Essential Functions of Government. The timeline for initiation and completion of each Block of focus is still being developed and coordinated with DOA Continuity Services; we expect to start by the end of CY2013.

SECTION 4: AGENCY IT PLAN – GOALS & OBJECTIVES

GOAL NUMBER 1:

ITG 1 Provide IT support for the process of making critical grant funding available to Montana public safety agencies.

Description: Provide IT support for the process of making critical grant funding available to Montana public safety agencies.

Benefits: The Montana local, state and private nonprofit agencies who are the primary recipients of the grants benefit from better information availability and easier grant application and monitoring processes.

Support of the State IT Strategic Plan: This supports Goal 2 by collecting and utilizing crime statistics to better utilize resources. It also supports Goal 3 by greatly increasing the access to crime data. MBCC actively participates in several statewide IT governance committees as discussed in Goal 5.

Supporting Objective/Action

ITO 1-1 Continue to support the Grant Management Information System (GMIS)

Business requirements: Provide efficient state-of-the-art processes for the grant management programs.

Benefits: Greater information sharing and efficiency for grantees and MBCC staff.

Risks: Potential unavailability of automated systems during critical periods of time.

Risks: Potential unavailability of automated systems during critical periods of time. Lack of participation by local agencies.

Timeframe: Ongoing.

Critical success factors: High availability, complete information, user reported ease of use.

Supporting Objective/Action

ITO 1-2 Continue to enhance and improve the GMIS System which includes OSAS (Online SubGrant Application System), GWIS (Grant Web Information System) and BMWAS (Board Member Webbased Access System)

Business requirements: Continue to enhance the automation of the grant management process.

Benefits: Better availability of grant information to grantees and program managers.

Risks: Potential unavailability of automated systems during critical periods of time.

Timeframe: Ongoing.

Critical success factors: High availability, complete information, user reported ease of use.

GOAL NUMBER 2:

ITG 2 Improve the overall quantity, accuracy and availability of Montana crime activity and detention data. Continue to improve the reporting to federal agencies, such as federal grantors and the FBI.

Description: MBCC maintains a number of database systems that collect and disseminate Montana juvenile and adult crime information, detention center information and law enforcement personnel information.

Benefits: Ability to provide adult and juvenile crime statistics to Montana agencies and the FBI.

Support of the State IT Strategic Plan: This supports Goal 1, to achieve maximum value of information through the active management of information technology. MBCC has increased the availability and value of information by providing better crime data to law enforcement agencies as well as the public.

Supporting Objective/Action

ITO 2-1 Continue maintaining and enhancing MBCC crime data collection systems. These include Montana's version of the National Incident Based Reporting System (MTIBRS), Juvenile Detention Reporting System (JDRS), Indian Lands Crime Data Collection, Drug Task Force Crime Data Collection, Juvenile Offense Statistical Data (CAPS & JCATS), Adult Detention Center System, Law Enforcement Manpower Database, Victims of Domestic and Sexual Violence database (PDQ) .

Business requirements: Continue to collect and analyze adult, juvenile and victim crime statistics to Montana agencies and the FBI. Continue to collect and analyze detention center information.

Benefits: Ability to provide adult crime, juvenile crime, victim and detention statistics to Montana agencies and the FBI.

Risks: Potential unavailability of automated systems during critical periods of time. Lack of participation by local agencies.

Timeframe: Ongoing.

Critical success factors: High availability, complete information, user reported ease of use, continuing certification from the FBI.

GOAL NUMBER 3:

ITG 3 Leverage current technologies to provide knowledge sharing opportunities for Montana public safety agencies.

Description: The MBCC provides and supports many web sites, publications and conferences that provide information about and encourage the sharing of important public safety information.

Benefits: All Montana public safety agencies and many other state and federal agencies benefit from enhanced availability of this information.

Support of the State IT Strategic Plan: This supports Goal 1, to achieve maximum value of information through the active management of information technology. MBCC coordinates and is involved in many statewide planning and knowledge sharing committees, conferences and workshops that help to coordinate IT and other activities between Montana law enforcement agencies.

Supporting Objective/Action

ITO 3-1 The Crime in Montana Publication

Business requirements: To provide crime statistics to Montana and other agencies.

Benefits: All Montana public safety entities and many other state and federal entities utilize this information for the process of analyzing crime. This ultimately leads to improved crime prevention capabilities in Montana.

Risks: That the information would be incomplete due to non-participation from agencies or computer system issues, or MBCC resource issues.

Timeframe: Yearly.

Critical success factors: Complete statistical information. Accurate and useful analysis of the information. Positive response from the consumers of the publication.

Supporting Objective/Action

ITO 3-2 Continue maintaining and enhancing the MBCC public web site with Montana crime data and information.

Business requirements: To provide easy access to Montana crime data and other public safety related information.

Benefits: Provides an easily accessible avenue to disseminate important public safety data.

Risks: That the information would be incomplete due to non-participation from agencies or

computer system issues, or MBCC resource issues.

Timeframe: Ongoing.

Critical success factors: The Web interface is easily accessible and valuable to users.

Assessment is through user feedback.

Supporting Objective/Action

ITO 3-3 Provide IT support for public safety conferences.

Business requirements: To encourage knowledge sharing between Montana public safety agencies.

Benefits: Increases overall knowledge sharing and networking within the Montana public safety community.

Risks: Potential low participation due to complicated or inaccessible sign up procedures.

Timeframe: Ongoing. Several per year.

Critical success factors: Positive feedback from attendees.

GOAL NUMBER 4:

ITG 4 Continue to enhance the efficiency and effectiveness of Board of Crime Control staff through the improved delivery of technology in-house.

Description: Provide up to date and cost effective computer hardware and software to MBCC staff.

Benefits: This contributes to the ability of staff to perform work tasks efficiently and effectively.

Support of the State IT Strategic Plan: This supports Goal 2, to aggressively use technology to extend capabilities that enhance, improve, and streamline service delivery. MBCC leverages state and industry standard technology to enhance and improve in-house technology and works closely with DOA SITSD in providing IT support and services where appropriate. This also supports Goal 3, to build an infrastructure / architecture that provides citizens and employees of the state access to information however and whenever they need it. Access to information is enhanced through application of appropriate technology.

Supporting Objective/Action

ITO 4-1 Maintain MBCC desktop workstations at current technology levels.

Business requirements: Utilize cost effective current technology to enhance work efforts.

Benefits: The advantages of current technical capabilities will be realized. MBCC will be current with state standards to enhance information exchange with other agencies.

Risks: MBCC should not adopt technology until it is proven reliable and stable.

Support of the agency IT goal: Improve the use and availability of technology.

Timeframe: Ongoing.

Critical success factors: MBCC staff has access to the latest cost effective hardware and software.

Supporting Objective/Action

ITO 4-2 Provide data and desktop security through pro-active security protection and regular monitoring.

Business requirements: Utilizes technology to improve overall staff performance.

Benefits: Increases availability, reliability of technology, protects confidential files, and data from unauthorized use.

Risks: The potential of viruses, adware, spyware and other malicious programs to disrupt computer use.

Timeframe: Ongoing.

Critical success factors: Computer systems are kept free of malicious programs. Confidential data is kept secure.

Supporting Objective/Action

ITO 4-3 Provide redundant backup and restore capabilities for all agency data and files.

Business requirements: Provide continuity of business in the event of data loss, caused by human error, system failure or natural disasters.

Benefits: Continuity of business.

Risks: Failure in this area could result in critical data or computer file loss.

Support of the agency IT goal: Technology is stable and always available.

Timeframe: Ongoing.

Critical success factors: Data restore tests are completed successfully. Backup system auditing reveals no problems.

SECTION 5: IT INITIATIVES (FY2012 – FY 2017)

No Initiatives

SECTION 6: ENTERPRISE ALIGNMENT

Communities of Interest Participation

- Government Services
- Public Safety
- Human Resources
- Environmental
- Education
- Economic
- Cultural Affairs
- Finance

SECTION 7: PLANNED AGENCY IT EXPENDITURES

<u>Expense Category</u>	<u>FY2012</u>	<u>FY2013</u>	<u>FY2014</u>	<u>FY2015</u>	<u>FY2016</u>	<u>FY2017</u>
Personal Services	\$80,090	\$88,210	\$89,974	\$91,774	\$91,774	\$93,000
Operating Expenses	\$241,975	\$220,975	\$232,375	227,193	238,193	\$227,193
Initiatives						
Other expenditures						
Totals	\$322,065	\$309,185	\$322,349	\$318,967	\$329,967	\$320,193

MBCC expects IT expenditures to remain relatively stable during this planning period.

SECTION 8: ADDITIONAL INFORMATION - OPTIONAL

Other types of information that support the agency's IT Plan. Some examples might include other COI participation, reference to other IT plans such as GIS plan, eGovernment plan, security plan, staffing issues and constraints, etc.