



State of Montana
Office of the State Public Defender

Agency IT Plan
Fiscal Year 2012-2017

May 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY1

SECTION 1: AGENCY ADMINISTRATIVE INFORMATION2

SECTION 2: AGENCY IT MISSION3

SECTION 3: AGENCY REQUIRED PROGRAMS4

SECTION 4: AGENCY IT PLAN – GOALS & OBJECTIVES6

SECTION 5: IT INITIATIVES (FY2012 – FY 2017).....11

SECTION 6: ENTERPRISE ALIGNMENT.....13

SECTION 7: PLANNED AGENCY IT EXPENDITURES14

SECTION 8: ADDITIONAL INFORMATION - OPTIONAL15

EXECUTIVE SUMMARY

The Office of the State Public Defender (OPD) ensures that persons charged in Montana that qualify for our services will receive timely, competent and vigorous representation by an attorney at public expense.

The Montana Public Defender Commission provides high-level supervision and direction for the statewide system. The Commission is responsible to establish statewide standards for attorneys providing public defender services and sets caseload and performance standards.

The Office of the State Public Defender operates as multiple statewide criminal defense law firms with a central office oversight of the system. As such, the state wide agency has some unique technical and IT-based challenges. Currently OPD has eight file servers at remote offices that serve file shares to users working physically in those offices. While this is a convenient solution for local file access at these office locations, it also has created a set of unique challenges based on the existing network and application topology. Additionally, the agency must protect private and privileged information while at the same time safeguarding the work product of its staff and attorneys. While OPD is not a criminal justice agency, it operates within a criminal justice environment that requires collaboration between OPD and criminal justice agencies. Some of the agency's unique challenges are as follows:

- The case management system, JustWare, is not being fully utilized to increase operating efficiencies of our attorneys and staff. It is critical that we develop the system and use it to the fullest extent possible. This will have the most direct impact in IT supporting the Agency's Mission.
- There are personnel and funding challenges structure, manage, and operate an adequate Information Security Management (ISM) program to address the constant change in technology and associated security requirements.
- The agency's servers require an operational overhead to maintain regular on-site backups; the server hardware is aging and warranties are expired; the server disk space is limited and presents problems with growth in additional file storage; and there is a lack of redundancy for the servers with potential for significant downtime and data loss for the agency.
- The agency needs to develop a standardized solution for desktop management.
- The agency lacks document collaboration.

Due to funding issues, the agency has extended its computer replacement process.

SECTION 1: AGENCY ADMINISTRATIVE INFORMATION

Role: Plan Owner

Name: William Hooks, Chief Public Defender
Telephone Number: (406) 496-6082
Email Address: WHooks@mt.gov

Role: IT Contact

Name: Kyle Belcher, Computer Supervisor
Telephone Number: (406) 770-3218
Email Address: KBelcher@mt.gov

Role: IT Contact (Alternate)

Name: Harry Freebourn, Administrative Director
Telephone Number: (406) 496-6084
Email Address: HFreebourn@mt.gov

Role: Information Security Manager (ISM)

Name: Kyle Belcher, Computer Supervisor
Telephone Number: (406) 770-3218
Email Address: KBelcher@mt.gov

IT Inventory

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

SECTION 2: AGENCY IT MISSION



The mission of the Office of the State Public Defender is to provide effective assistance of counsel to indigent persons accused of crimes and other persons in civil cases who are entitled to the assistance of counsel at public expense.

Employees of the Information Technology Department of OPD are dedicated to providing the highest level of technical leadership and information technology services to support the agency's mission and critical business functions. The IT function is headed by the Computer Supervisor. The Computer Supervisor reports directly to the Administrative Director, who in turn, reports directly to the Chief Public Defender. The mission of the Computer Supervisor and his staff is to provide customer service to the agency by supporting the information and reporting needs using the appropriate technologies and information systems. All activities and projects of the agency's IT department will support OPD's mission and goals. Projects are prioritized and allocated resources such that those with the most direct impact in supporting the agency's mission and goals come first.

SECTION 3: AGENCY REQUIRED PROGRAMS

Information Risk Management Program (IRMP) General Description

The Office of the State Public Defender (OPD) has ***a plan to implement*** a department-wide (agency) information security management program compliant with §2-15-114, MCA and State Information Technology Systems Division *Information Security Programs* policy. 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. Integration of these three programs is critical to the confidentiality, integrity, and availability of information which is associated with each program.

As described in NIST SP 800-39, the agency has ***a plan to 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 an acceptable level, while ensuring legal and regulatory mandates are met in accordance with MCA §2-15-114.

The agency's program will have 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 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. During implementation of the information security management plan, we will identify vulnerabilities, sensitivity, and weaknesses which require restructure, new equipment, or personnel positions (funds increase) to appropriately mitigate the associated risk.

Future Security Program Plans

Over this strategic period we plan to develop and implement a stronger department-wide (agency) information security management program compliant with §2-15-114, MCA and State Information Technology Systems Division *Information Security Programs* policy, as referenced in agency objective 1-2. We currently have a working group with key personnel/stakeholders to continue the planning and development. The Public Defender agency will need an additional FTE to fill the Information Security Manager required position and possibly other resources such as new equipment. Resources will be defined within the next 6 months.

Continuity of Operations / Continuity of Government (COOP/COG) Program General Description

In 2009, the Office of the State Public Defender joined with the Department of Administration *Continuity Division* for the development of a continuity plan for operations and government which when complete will provide the record and structure that will facilitate disaster recovery capability with minimal and acceptable timelines for continued operations and services. The completion date of the program is unknown as OPD is working in conjunction with DOA. 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.

Future COOP/COG Program Plans

Over this strategic period we plan to develop and implement an extended COOP/COG program that encompasses information stored in electronic format on the various servers and systems of our agency, as referenced in agency objectives 3-1 and 3-2. The Public Defender agency will need new equipment and software to implement a COOP/COG solution. Resources will be defined within the next 6 months.

SECTION 4: AGENCY IT PLAN – GOALS & OBJECTIVES

Goal Number 1:

IT Goal 1 Improve our existing Information Technology network and application topology

Description: Our goal is to provide the highest quality technology-based services in the most cost-effective manner, and to facilitate OPD's mission through IT support of training, management and reporting. Most importantly, applied technology should support outstanding legal services to our client base.

Benefits: Better use of technology reflects increased cost effectiveness by streamlining and automating business processes. Additionally, we aim to increase productivity, enabling our staff to focus on the mission of our agency.

State strategic goal(s) and/or objectives(s) addressed Goal 1, Objectives 1-1, 1-2, 1-3, 1-4, 1-6 and Goal 2, Objectives 2-1, 2-2, 2-3, 2-4

Supporting Objective/Action

Objective 1-1 Enhanced Desktop Management

The Office of the State Public Defender consists of approximately 200 FTE and over 240 contractors that provide various legal services geographically dispersed statewide. Currently, OPD has no standardized image deployment solution and we rely on a manual image process for rebuilding user desktops and laptops. Software updates often require day long traveling. Asset management and software inventory are not centralized. The management of basic desktop services (office productivity tools such as Word, Outlook and internet connectivity) is critical to the day-to-day operations of OPD. Moreover, budget constraints create difficulty with adhering to the state's computer replacement cycle guidelines, making desktop management even more critical. The objective includes PC imaging, software distribution, patch management and centralized desktop configuration to:

- Streamline the building and configuring of PCs being deployed or reassigned;
- Automate the distribution of desktop applications and operating system upgrades;
- Manage software updates (currently using WSUS – windows security update server)
- Centralize software and hardware inventory to provide more accurate reporting; and
- Centrally manage certain desktop settings via policies (i.e., disabling games on all desktops, power management settings, firewall settings) to improve IT support and staff efficiencies.

Benefits: Successful completion of this objective will result in increased security, reduced travel time and lost productivity by employees, and in keeping the desktop environment current.

Risks: The major risk in not accomplishing this goal is a potential lack of applied standards and application updates, leaving us vulnerable to PC malware. Additionally, a less consistent platform decreases productivity and makes training challenging.

Objectives: This objective supports the OPD IT goal by keeping the desktop environment consistent and current.

Timeframe: The timeframe for completion of this objective is FY 2013.

Critical success factors: The resources and funding available to purchase the servers and licenses required to train and apply an ITSD supported product such as Microsoft Systems Center Configuration Manager (SCCM).

Supporting Objective/Action

Objective 1-2 Implement Enhanced Security

This objective is a multi-faceted effort to meet developing security needs of OPD and ITSD-mandated security requirements. The objective involves participation on the security advisory council, development of comprehensive user security awareness and audit programs, the implementation of measures to comply with the ITSD policy on sensitive data on portable devices, and planning efforts to comply with the Enterprise Information System Security Policy that is being developed by ITSD.

Benefits: Successful completion of this objective will result in enhanced security capabilities of OPD, meeting ITSD-mandated state standards on security, improved enterprise security, and compliance with federal mandates (NIST Standards) to secure data, encryption of sensitive data and destruction of privacy information on a timely basis.

Risks: The main risk associated with not achieving this objective is the potential for sensitive agency information to fall into inappropriate hands, internal or external, so as to damage the agency's ability to serve its mission. A lack of funding to implement the systems necessary to protect information resources, including the appropriate level of contracted services and OPD staff to ensure training, auditing and security system implementation could cause the agency to be unsuccessful in attaining this goal.

Objective: This objective supports the agency IT goal by enhancing information security through a comprehensive security program.

Timeframe: The timeframe for completion of this objective is FY 2013.

Critical success factors: Training and funding available to increase user awareness of security requirements, ability to audit and protect the use of sensitive information, and increased compliance with state and federal security standards.

Goal Number 2:

IT Goal 2 Utilize our existing technology to better improve business operations of the Office of the State Public Defender

Description: This goal is to fully utilize the current technology of OPD to improve business operations, efficiency, and better serve those that qualify for our services.

Benefits: This goal provides automated tools to the staff of OPD that will improve the quality, integrity, and timeliness of information resources (briefs, video and reports) that are necessary to accomplish the mission of the agency in a cost effective and timely manner. It will also significantly improve operating efficiency of our attorneys and staff.

State strategic goal(s) and/or objectives(s) addressed: Goal 1, Objectives 1-1, 1-2, 1-3, 1-4, 1-6 and Goal 2, Objectives 2-1, 2-2, 2-3, 2-4

Supporting Objective/Action

Objective 2-1 Enhance JustWare Case Management Workflows and Data Integrity

OPD utilizes JustWare Defender for its case management system to manage and track cases. The case management system is critical to the operation of OPD. Currently, the system is not configured to maximize operating efficiencies and ensure data integrity. To effectively and efficiently represent our clients, there is a need for automation, data validation, and workflow enhancements to the existing system.

Benefits: The benefits to be derived from the successful completion of this objective are as follows:

- Improved data integrity – by implementing business rules in the system, we can ensure that all required case information is entered and that the information entered is validated based on predefined business processes. This will also help to ensure we are providing accurate and timely information to key stakeholders (Public Defender Commission, Legislature, and management).
- Increased operating efficiency – by improving how users view and enter information into the

system (workflow), we will realize increased operating efficiency of attorneys and staff.

- End user acceptance – simplifying and improving the user interface will increase user acceptance and satisfaction of the software, which has historically been an issue in the agency.

Risks: The anticipated risks associated with this objective are poorly defined business requirements, ineffective change management, business processes and procedures are not well defined and documented, an insufficient training program, and not having adequate resources dedicated to the project.

Objective: This objective supports the agency IT goal of improved business operations by providing an efficient interface for end users. It also supports the agency IT goal of providing accurate and timely information to key stakeholders.

Timeframe: The timeframe for completion of this objective is FY 2011 and ongoing.

Critical success factors: The successful completion of this objective is dependent on several factors:

- Adequate resources, including funding, personnel, and the consulting services of New Dawn Technology (vendor of JustWare).
- The development of comprehensive Change Management policies and procedures based on industry standards and best practices.
- Extensive involvement of key stakeholders, including end users, during the development process.
- Communication and training of all changes made to the system for all affected users.
- A full evaluation and understanding of current business processes, which are known to vary from office to office.

Supporting Objective/Action

Objective 2-2 Implement Expanded Video and Web-Based Conferencing

The use of web-based conferencing technology is becoming a critical element in OPD's efforts to effectively represent clients, to use staff resources efficiently and to reduce travel expenses. This objective is to develop our web-based video conferencing capabilities statewide. We plan to accomplish this by installing Vision Net video conferencing equipment in additional OPD offices. We may also implement a computer based meeting/collaboration tool such as Microsoft Lync, a service provided by ITSD.

Benefits: The benefits of adding additional video and/or web-based conferencing capabilities is increased access and improved communications with clients and courts, and also decreases travel.

Risks: The risk of not developing our video and web-based technology affects the ability to communicate effectively, the ability to train efficiently throughout the state, and increased travel costs.

Objective: This objective supports the agency IT goal by providing enhanced technology solutions to improve the ability of staff to support OPD's mission and meet the needs of those that qualify for our services.

Timeframe: The timeframe for completion of this objective is FY 2012 and ongoing.

Critical success factors: Adequate funding must be provided for this objective to be successful. Communication of the availability of this technology and proper training on how to effectively use the technology are critical to the objective's success. Success will be measured by increased ability to communicate with clients and other participants in the criminal justice system, improved timeliness of communications, and reduced travel time and costs.

Supporting Objective/Action

Objective 2-3 Enhance JustWare Case Management Reporting to Support and Improve Operations

OPD utilizes JustWare Defender for its case management system to manage and track cases. The case management system is critical to the operation of OPD. Currently the system produces a vast number of reports but the agency needs to review them to assess their usefulness and accuracy. To effectively manage OPD's caseload, there is a need for enhanced reports.

Benefits: The benefits to be derived from the successful completion of this objective are enhanced management information that will be used to assign, reassign and track cases, and to provide information to stakeholders of OPD including the Public Defender Commission, the governor, the supreme court, the legislature, managers, and staff of the agency.

Risks: The anticipated risks associated with this objective are poorly defined business requirements, ineffective change management, business processes and procedures are not well defined and documented, an insufficient training program, and not having adequate resources dedicated to the project.

Objective: This objective supports the agency IT goal of improved business operations by providing relevant, accurate, and timely reporting to management so that the information needs of key stakeholders can be met.

Timeframe: The timeframe for completion of this objective is FY 2013 and ongoing.

Critical success factors: The critical success factors associated with this objective are identical to those outlined in ITO 2-1.

Goal Number 3:

IT Goal 3 Ensure Continued Operations

Description: This goal is to position OPD to recover from any catastrophic loss of computing services and to ensure that OPD's computing infrastructure is available to its employees on a continuous basis.

Benefits: Continued operation of a critical state service and continued productivity of OPD staff.

State strategic goal(s) and/or objectives(s) addressed: This goal supports the State IT Strategic Plan by ensuring continued operation of government as outlined in section 3 (Agency Required Programs) of this document.

Supporting Objective/Action

Objective 3-1 Develop and Implement OPD Disaster Recovery Plan

OPD is a critical partner in the criminal justice system and must ensure that its services are available on a continuous basis to meet the needs of our clients. OPD is also part of the state's Continuity of Operations project. The agency must assure that it is prepared to deal with the effects of a disaster and to be ready to reinstitute operations in a timely manner to continue to provide services to meet its mission.

Benefits: The ability to ensure continuous operation of OPD services is critical to satisfying Constitutional and legal requirements of state law.

Risks: The risk of this objective is the lack of funding to implement a comprehensive plan to prevent the loss of data and services.

Objectives: The objective supports the agency IT goal by providing an organized, deliberative and cost-effective method of ensuring the continued operation of critical OPD IT applications and services.

Timeframe: The timeframe for implementation of this objective is FY 2014.

Critical success factors: The critical success factors associated with this objective are OPD management commitment to the objective, adequate resources to create and maintain the plan and successful deployment of necessary resources to statewide offices.

Supporting Objective/Action

Objective 3-2 Develop and Implement Off-Site Backup Solution

OPD presently owns 8 servers that are past warranty. We have examined our needs, and anticipate centralizing data backup to the State Data Center for our remote offices. Currently, some servers are not located in secured areas and backups for the servers must be accomplished by changing tapes. The backup tapes are not located in secure locations nor are stored off-site. Some individuals that change out tapes are not trained IT personnel. The solution OPD is considering to accomplish a centralized off-site backup is Microsoft Systems Center Data Protection Manager 2012 (DPM).

Benefits: The benefits to be derived from the successful completion of this objective are better management of applications and data, the archiving of older material, and the evolution towards a single, centrally managed information backup. The consolidated central management of data will also allow a copy of data to be stored off-site to ensure continuity of operations in case of a disaster.

Risks: The primary risk associated with this objective is the inability to restore operations in the event of a disaster and significant loss of data.

Objectives: This objective supports the agency IT goal by allowing better management of data resources and the ability to accomplish continuity planning and disaster recovery.

Timeframe: The timeframe for implementation of this objective is FY 2014.

Critical success factors: Adequate funding to replace the obsolete remote office servers, purchase the required hardware and software to centralize backups, and funding to provide training to IT personnel. Support and buy-in from management, stakeholders, and Network Administrators.

SECTION 5: IT INITIATIVES (FY2012 – FY 2017)

Initiative 1 Microsoft Systems Center Configuration Manager

Description: As noted in agency objective 1-1, a large challenge for OPD has been distributing software updates and new software within a geographically dispersed agency. OPD seeks solutions for remote management, software inventory, software delivery, imaging and policy enforcement. OPD proposes that SCCM provides our solution. Additionally, SCCM provides an accurate inventory of all the hardware and software assets in OPD.

This initiative will require the purchase and licensing for SCCM, at a cost of approximately \$600. The balance of our hardware/server infrastructure needs will be centralized with ITSD. The server infrastructure will cost about \$5,800 annually. ITSD is considering providing support for SCCM. The server infrastructure can be budgeted through ITSD during the FY 2014-2015 biennium. Implementation and training costs are not included in the figures above and are pending. All necessary resources will be defined within the next 6 months.

Initiative 2 IJIS Broker Project: Participation of OPD in the IJIS Broker Project

Description: The IJIS Broker project is vital to public safety because it creates exchanges that allow a wide range of agencies to share real-time information quickly, securely and accurately. The IJIS Broker project, began in 2005, is currently managed by the Department of Justice and includes participants from courts and corrections.

Primary exchanges being developed to share critical information among local and state justice agencies include:

- Arrest/Booking
- Prosecutor Charging Decision
- Pre-sentence Investigation
- Sentencing Recommendation
- Judgment Order
- Notice of Hearing
- Hearing Order
- Petition to Revoke
- Correctional Status Events

The Office of the State Public Defender was created after the initiation of the IJIS Broker project. However, OPD is a critical state-level participant in the criminal justice system. OPD's participation in the IJIS Broker project is critical to OPD's ability to receive and share information among and between the various agencies involved in the criminal justice system. Participation by OPD will require resources and funding to make the necessary modifications to JustWare in order to exchange information with other IJIS Broker participants.

The Montana Department of Justice is the lead agency on development of the IJIS Broker project. New

Dawn Technologies, which provides the JustWare application software for county prosecutor offices and OPD, has been involved in the IJIS Broker project. OPD has received an estimate of \$50,000 (\$10,000 of which is annual support/maintenance costs) to purchase the necessary software to develop information exchanges for JustWare to share with the IJIS Broker. OPD has also received a rough estimate of \$80,000 to build these information exchanges (\$10,000 of which is annual support/maintenance costs). The initial investment for the software, development, and implementation is estimated at \$130,000 plus ongoing maintenance of \$20,000. These numbers are just an estimate and will change as requirements are defined.

Initially, most, if not all, of the prosecutor and court information exchange elements developed for exchange by JustWare (such as arrest/booking, pre-sentence and other notice and hearing information elements) constitute critical information that is needed by OPD in its own JustWare supported information system. OPD should explore with the Departments of Justice and Corrections and the Supreme Court Administrator's Office the possibility of including any future costs of participation in the IJIS Broker in the annual federal grant application under the National Criminal History Records Program to the U.S. Department of Justice.

Initiative 3 OPD Disaster Recovery Plan and Off-Site Backup

Description: As noted in objectives 3-1 and 3-2, OPD needs to develop and implement a disaster recovery plan and off-site backup solution for information that resides in an electronic format. The solution OPD is considering to accomplish a centralized off-site backup is Microsoft Systems Center Data Protection Manager 2012 (DPM). To develop and implement this solution, OPD would need funding to purchase the required hardware and software to centralize backups, and funding to provide training to IT personnel. The estimated hardware and software cost is \$15,000 (\$1,500 of which would be an annual recurring ITSD service cost). Implementation and training costs are not included in the figures above and are pending. All necessary resources will be defined within the next 6 months.

SECTION 6: ENTERPRISE ALIGNMENT



Communities of Interest Participation

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	256,000	256,000	256,000	256,000	256,000	256,000
Operating Expenses	740,000	745,000	755,000	755,000	755,000	755,000
Initiatives	0	20,000	150,000	0	0	0
Other expenditures	100,000	165,000	70,000	50,000	50,000	100,000
Totals	1,096,000	1,186,000	1,231,000	1,061,000	1,061,000	1,111,000

SECTION 8: ADDITIONAL INFORMATION - OPTIONAL

