Information Technology Master Plan (ITMP)

Guidelines & Instructions for Maryland State Agencies

Fiscal Year 2015

Table of Contents

1 Overview

1.1 Purpose

This document provides guidance, instructions and required format for an Agency Information Technology Master Plan (ITMP), due on August 12, 2013.

These guidelines and instructions apply to all entities subject to Maryland State Finance and Procurement Law, including, but not limited to State Finance and Procurement articles 3A-302-3A-309.

1.2 Overview

Each Agency must produce an annual ITMP describing a six year plan for the Agency's information technology goals, along with the strategies, projects, and resources needed to achieve those goals. The ITMP also contains information about Agency cyber security measures for Agency systems containing sensitive information.

The Agency ITMP provides context for the Agency's information technology (IT) budget requirements. An ITMP should support the Agency's annual budget submission, along with any Information Technology Project Requests (ITPRs) for Major IT Development Projects (MITDPs), and any Managing for Results (MFRs) metrics.

The Department of Information Technology (DoIT), Department of Budget and Management (DBM) Office of Budget Analysis (OBA) and the Department of Legislative Services (DLS) all review the ITMP for the following:

- Consistency with statewide IT direction
- Support of statewide business objectives
- Presence of sound and secure IT infrastructure plans and strategies
- Support for subsequent requests for funding

1.3 Agency Exemptions

An Agency may be granted an exemption if it meets the criteria for an exemption. An exemption request must be made in writing to DoIT and approved for each fiscal year.

- There are no exemptions for any Agency regarding DoIT cyber security reporting. An Agency must either meet the reporting requirements as defined in Section 6.7 or submit a statement indicating that the Agency has no information systems containing Personally Identifiable Information (PII).
- An Agency with no current or planned IT projects or IT procurements may request exemption from completing an Agency ITMP.

2 Aligning Agency ITMP with State ITMP

The 2015 State ITMP provides a framework for articulating the Governor's current priorities and IT Perpetual Objectives, including establishing Supporting Strategies for meeting them. The State ITMP is posted at: http://www.doit.maryland.gov/ Search: State IT Master Plan.

Governor's Priorities

- Strengthen and grow the ranks of our middle class including our family owned businesses and our family farms
- Improve public safety and public education in every part of our state
- Expand opportunity – the opportunities of learning, of earning, of enjoying the health of the people we love, and to enjoy the health of the environment that we love – to more people rather than fewer

Perpetual Objectives

The State ITMP provides a general direction for long range IT planning through four Perpetual Objectives intended to be in effect for multiple years. The Perpetual Objectives that serve as the foundation for Agency IT planning are:

- Consolidation
- Standards
- Interoperability
- Cyber Security

Supporting Strategies

The State ITMP establishes Supporting Strategies that align with the Perpetual Objectives. Each Agency ITMP will describe planned initiatives that:

- Facilitate Agency-specific responsibilities by helping enhance business processes,
- Demonstrate collaboration with other Agencies in the deployment of technology, and
- Support the Perpetual Objectives and Supporting Strategies of the State ITMP.

The Agency will categorize each initiative as one or more of the following:

- Statewide
- Line-of-Business
- Location-Specific
- Intra-Agency
- Inter-Agency

3 Agency ITMP Instructions & Format

3.1 General Preparation Instructions

Agencies are required to submit an ITMP containing six parts:

- Section One - general information
- Section Two - summary information about the Agency's business functions, major goals and key strategies to achieve those goals
- Section Three - information about the Agency IT strategic direction
- Section Four - Agency IT portfolio
- Section Five - Agency Six Year Report
- Section Six - Cyber Security

3.2 Agency ITMP Format and Content

The attached template contains instructions for completing an Agency ITMP (See Appendix A).

4 ITMP Submission Requirements

4.1 ITMP Submission Procedure

Submit the ITMP electronically by uploading the completed ITMP to the ITAC web site at: https://www.itac.state.md.us.

The Agency ITMP is due on August 12, 2013.

4.2 DoIT Staff Assistance

DoIT staff members are available to answer questions and provide feedback to Agencies on their respective ITMPs. For information concerning guidelines and formatting, please contact your Agency's assigned DoIT Office of Project Oversight Project Manager (OPM). If your Agency does not have an assigned OPM, contact Carla Thompson for assistance at Carla.Thompson@maryland.gov.

Please contact DoIT to answer security-related content questions (Section 6 of the ITMP) Bruce.Eikenberg@maryland.gov.

5 Acronym List

Acronym	Definition
COTS	Custom Off The Shelf
CTD	Cost to Date
DBM	Department of Budget and Management
DLS	Department of Legislative Services
DoIT	Maryland Department of Information Technology
EAC	Estimate At Completion
ETC	Estimate To Complete
FF	Federal Funds
FY	Fiscal Year
GF	General Funds
GIS	Geographic Information System
IA	Interagency Agreement
ISP	Information Security Policy
IT	Information Technology
ITAC	Information Technology Advisory Council
ITMP	Information Technology Master Plan
ITPR	Information Technology Project Request
MFR	Managing for Results
MITDP	Major Information Technology Development Project
MITDPF	General Funds Appropriated for the Project and Accounted in the Major IT Development Fund
MOU	Memoranda Of Understanding
O&M	Operations and Maintenance
OPO	Office of Project Oversight
OPM	Oversight Project Manager
PIR	Project Implementation Request
PMI	Project Management Institute
PPR	Project Planning Request
RF	Reimbursable Funds
SF	Special Funds
SDLC	Systems Development Life Cycle
TPC	Total Planned Cost

6 Appendix A – ITMP Template

Information Technology Master Plan (ITMP) for Maryland State Archives

Fiscal Year 2015

6.1 ITMP Overview

This ITMP contains the following sections describing the Agency's current and future information technology (IT) initiatives and status:

All sections are required unless exempted by DoIT for this fiscal year.

- Section One - general information
- Section Two - summary information about the Agency's business functions, major goals and key strategies to achieve those goals
- Section Three - information about the Agency IT strategic direction
- Section Four - Agency IT portfolio
- Section Five - Agency Six Year Report
- Section Six - Cyber Security

6.2 Section 1 – General Agency Information

1. Agency Name (ACRONYM) Maryland State Archives (MSA)

Provide the full Agency name and acronym

2. Chief Information Officer (CIO) Name and Contact Information:

Name	Wei Yang
Title	Director, Information Systems Management
Telephone Number	410-260-6462
Email address	Wei.Yang@Maryland .Gov

3. Chief Financial Officer (CFO) Name and Contact Information

Name	Nasrolah Rezvan
Title	Fiscal Administration
Telephone Number	410-260-6481
Email address	Nasrolah.Rezvan@Maryland.Gov

4. ITMP Approved By

Provide the name, title and contact information of the Agency Executive Sponsor

Name	Timothy D. Baker
Title	Deputy State Archivist
Telephone Number	410-260-6402
Email address	Tim.Baker@Maryland.Gov

5. Plan Date

Provide the date the plan was approved by the Agency Executive Sponsor — 8/12/13

6.3 Section 2 – Agency Business Functions, Goals, and Key Strategies

Provide an executive summary of the Agency's major business functions. List long, mid and short term goals and key strategies to achieve those major business functions. Long term is considered longer than 5 years, mid-term is considered 2-5 years and short term is considered less than 2 years. If this information is documented in an Agency strategic plan, then the Agency strategic plan may be attached in place of Section 2.

Executive Summary:

The State Archives is the record keeper for all agencies of Maryland State and local government. Of all the materials generated by our government, only a small portion are deemed so important that they are designated for permanent retention. Records document the lives of our people, the governments they create, and the rights they secure.

Section 3 – Agency Strategic Direction

Topics in this section must be addressed in order.

1. Summary of Agency IT Environment

The Agency's "IT environment" consists of any and all elements supporting any information technology solutions, including: personnel performing IT tasks, actual IT systems, the physical infrastructure that run these systems, controls over IT-related code and documentation, and governance of all these things.

Background

Describe historical events that have had a significant impact on performance of the Agency's mission and the IT architecture supporting the Agency's core business activities. Core business activities are those that either support or produce the Agency's primary products and services.

We are faced with some daunting challenges with regard to what of the electronic record we should and must be saving, whether it is for legal purposes or for the necessary enlightenment of the public over time.

The State Archives is Maryland's historical agency and permanent records repository for government records, the ultimate repository of the people's records, as one Court

Clerk has pointed out. An archives is the conscience of the public, the repository of its collective memory, recording the history of the State. The Records Management Division of the Department of General Services has responsibility for non-permanent or temporary records that can be disposed of after a period of time. The Archives and Records Management currently share responsibility for the creation of disposition and retention schedules. After records of an agency of State government are reviewed or appraised by archivists and records managers, a determination is made for each type of record whether to keep the record and for how long; based on the record's administrative, financial or historical value. The deposition and retention schedules cite if the record can be destroyed after some predetermined time; transferred to Records Management for eventual destruction; or transferred to the Archives for permanent retention.

Although the vast majority of Maryland's permanent records exist in paper form and on microfilm, the past decade has witnessed the rapid growth of electronic records. The same basic issues of appraisal, access, and preservation of information that pertain to paper records also pertain to electronic records. Records once kept in paper or on microfilm now exist on a variety of computer information systems. Many of these are permanent records, but their electronic form is fragile and easily lost. Developing strategies to preserve electronic records is a challenge to the agencies that manage the information, the information system professionals as well as archivists and records managers.

Satisfactory management of electronic records requires that records be actively managed throughout their life cycle: from creation, through all phases of access and use, to final disposition, whether that is permanent storage or eventual destruction. It is important to understand the distinction between the life cycle of records and the life cycle of information systems that create, manage and use the records and the life cycle of the media on which the records are stored. The life cycle of records often exceeds the life cycle of the information system in which the records are originally created or captured.

Likewise, some storage media will significantly outlast the hardware and software necessary to retrieve and display the records stored on them. To successfully manage and maintain electronic records, it is important to determine if the records will be needed beyond the life of the system where they are currently stored and, if necessary, to plan for the migration of the records to a new system before the current system is retired.

The successful management and preservation of electronic records, however is not something that we can undertake alone. It will take the creative energy of IT professionals, archivists and records managers working together to preserve the

essential information of government in a permanent format that is accountable, verifiable, and susceptible to a transparent migration from the media format of today to the media format of tomorrow in the most effective and cost efficient manner possible.

The first step is to carefully examine IT operations with regard to what must be saved permanently as the permanent public record and what form that record should take. The second is to use the state's Records Retention and Disposal scheduling process, as required by law, to make rational decisions about disposition of records.

Drivers and Issues:

Years ago, Maryland state government had a strong records management program. It began with a strong management team at the Department of General Services Records Management Division and was complimented by a capable staff of records management professionals able and willing to assist agencies in the development of records inventories and schedules. In addition, most agencies employed professional records management staff which assisted DGS in the development of the five year statewide inventory of records holdings. Over the past twenty years most all of those staff have been lost to layoffs and attrition. The Records Management Division has but a few individuals left to coordinate the state's records management program.

The five year record inventory, (required by law), is an important starting point in determining the extent of permanent records that must be cared for. It has not ever been successfully conducted. The only way that this inventory will ever be successful is for there to be a statewide initiative to develop a web-based records inventory and scheduling database that agencies can feed into on an ongoing basis.

Electronic Records Management

"…The challenge is to determine which types of electronic records must be retained and for how long, as well as how to best preserve them and make them available…"

For presentation purposes we have grouped the drivers and issues into two categories: statewide and inter-agency specific.

Statewide

When viewed in the context of the statewide Information Technology Master Plan, some of the drivers and issues are as follows:

Platform – lack of standard platforms that support archival transfer of data

Disaster Recovery – The Archives can (and in many cases does) provide a reliable depository for essential agency records. Agencies should be encouraged to explore this opportunity.

In the standards arena, agencies should be encouraged to incorporate information life cycle management into their systems development initiatives and generally to their information technology practices. Our experience at the Archives is that few if any agencies have an information life cycle management mentality or capability. More importantly, few, if any, information technology operations recognize or accept any responsibility for adhering to the laws and regulations related to record retention and disposition.

Thus, generally speaking effective records management is a significant issue facing perhaps every agency of state and local government. Inadequate records management programs means, among other things, that there is no reliable inventory of records upon which the Archives can base good planning for the accessioning of permanent record material.

A related issue is that while we have fundamentally shifted from a paper-based records world to an information technology environment, the processes and procedures for identifying and effectively migrating permanent record material to the Archives has not yet matured. Indeed, there are many systems still being developed today that lack the ability to migrate data into an archival form and format for efficient transfer to the Archives. We speculate that many systems even lack the ability to migrate data forward into replacement systems when current applications and hardware become obsolete.

Email – A good example of some of the problems associated with the management of electronic records is exemplified by electronic mail (email).

Definitions:

- E-mail systems E-mail systems
- E-mail messages are electronic documents created and sent or received by a computer system. E-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.
- What is a record?

  "public record"

- "original or any copy of any documentary material ... made ... or received by [an agency] in connection with the transaction of public business" SG §10-611(g)(1)(i)
- can be in "any form", including without limitation: card, computerized record, correspondence, drawing, film or microfilm, form, map, photograph or photostat, recording, tape SG §10-611(g)(1)(ii)
- "public record" includes both printed and electronically stored versions of e-mail messages, e-mail messages never printed out, and includes e-mail messages related to agency business on employee's home computer. 81 Opinions of the Attorney General 140 (1996)

What E-mail should be kept and how long?

E-mail should not be given any special treatment because in essence it is just like any other form of written correspondence with the only differentiating quality being the medium or mode of delivery. E-mail itself is not to be considered a record series or category. It is a means of transmission of messages or information. Like paper or microfilm, e-mail is the medium by which this type of record is transmitted.

The two basic criteria in deciding what to keep are whether it is non-permanent or permanent. In basic terms non-permanent retention is based on the time-value to the business function of the agency, while permanent retention is based on the record's value after it no longer serves the agency's business requirement. E-mail messages that have significant administrative, legal fiscal and/or historical value should be categorized under the appropriate record series. Using the creating agencies current retention policy should be sufficient in guiding the record keeping.

Records with permanent value include but are not limited to the following:

- Documentation of state policy (laws, rules, and court decisions),
- Documentation of the policy process (minutes of meetings, transcripts of selected hearings),
- Protection of vital public information (births, deaths, marriages and reports).

Some suggestions on what the record creator should save:

- Personal E-mail [Delete]
- Transitory E-Mail [Delete after certain time]
- Intermediate E-Mail [Delete by schedule]
- Permanent E-Mail [Delete only when permanent copy is made, forward copy to archives]

Transitory documents are of informational value, which serve to convey information of temporary importance in lieu of oral communication. Intermediate documents have more significant value, may include but are not limited to: Routine correspondence, Activity Reports, and weekly fiscal reports. Permanent documents are records that are deemed of value over the life of creator. These may include but are not limited to: Meeting Minutes, Policy Statements, and End of Year Reports.

Who should save e-mail and how?

Some feel the individual who sends an e-mail message should maintain a record copy of the message. However, the varied use and wide distribution of e-mail may result in many exceptions to this rule that will have to be dealt with internally. There are clearly instances when the recipient should maintain the record. Again, these issues need to be discussed particularly in the context of the definition of a public record in the Public Information Act.

After brief periods in the IN-OUT boxes, messages of permanent value should be transferred to other boxes or to a central server, based on business and retention requirements as stated in an approved schedule; E-mail that is designated as permanent should be saved to an on-line storage folder or permanent near-line storage periphery.

In order to aid in the managing of the E-mail system the creator should provide descriptive subject lines. This not only enhances the e-mail but also makes retention much easier.

The system should be maintained in a format that preserves contextual information and that facilitates retrieval and access. The system should allow for periodic deletion of non-permanent messages. Both permanent and non-permanent records should be stored in a logical filing system.

System administrator/Records officer of the creating agency should manage the e-mail

system and forward on a periodic basis, per retention schedule, file folders containing saved e-mail to the Archives

All of the above, even though related specifically to email, argues well for the establishment of a more robust and comprehensive records management program in the State.

Some other problems related to records management:

- Agencies tend to think of records in terms of paper files or series of paper files. Therefore, record retention programs tend not to include vitally important electronic record series
- Agencies have tried to hold onto records they designate as permanent
- Many record series are not considered by an agency to be a records series. Examples
    - Access Log Files
    - Security Log Files
    - Voice Mail
    - Email
    - Databases

Some issues related to data:

- Collection and transfer
    - Open standards for transfer and retention need development and frequent updating
    - Proprietary applications must include data migration / export function
- Conversion, assurance, consolidation and integration
- Integrity - - monitoring and audit data flow
- Security
- Correction and expungement
- Delivery and sharing
- As well as shielding and restricting
- Certification

Inter-Agency Specific Drivers and Issues

Some inter-agency specific drivers and issues are summarized below:

- **Interoperability constraints.** Collecting all of the electronic data designated for permanent retention presents a myriad of issues with regard to formatting, transferring, updating, validation and verification
- **Data integrity.** Converting data for preservation without losing content, style and quality
- **Data Security.** Network security is becoming much more complicated. So, too, is system security
- **Backup and restore.** Large amounts of data require different backup and restoration procedures
- **Data Delivery.** The public is now accustomed to receiving 24 x 7 service from the Archives via the web, yet we only have staff to operate weekday / daytime hours. Also, shielding and restricting access need to be effectively applied where law or regulation demand.
- **Framework training.** As increasingly sophisticated networking configuration is required, local IT staff need much more extensive training to remain qualified to manage large networks. Focusing on internal networking issues reduces the capacity to attend to application-level concerns.

IT Accomplishments:

Far and away the greatest accomplishment of the Archives in the last several years is the establishment of the electronic archives and successful partnership with the two entities that historically have created some of the largest records series in State government: the Circuit Courts and the Registers of Wills. These partnerships focus on migrating from paper systems to electronic records management and have the opportunity to save the state millions of dollars while providing much enhanced access to the records.

Another major accomplishment is the consolidation and integration of the many databases that provide the intellectual control over our vast holdings. Roughly a decade ago, the Archives had over 24,000 separate databases that provided our staff the means of finding records. Over the last 12 years we have worked to bring most all of those data sets together under our *Guide to Government Records*. Much work still needs to be done, but we are very proud of this major accomplishment.

Other accomplishments:

- ☐ Data Integrity – data ingest and data flow is routinely audited
- ☐ Data Security
  - Network protected by enterprise firewalls and host / PC firewalls monitored by IPS and MARS
  - Critical systems are set up to be dual-host locally and some are dual host remote
  - Critical databases mirrored locally and remotely
- ☐ Data Delivery – Multi-home Internet connections

IT Goals and Strategies:

Describe the Agency's IT goals, and strategies to achieve those goals, and how results will be measured. Include any pertinent reference to Agency MFRs, StateStat statistics and existing Agency IT-related business plan goals. List initiatives the Agency is undergoing to fulfill the goals and strategies.

Performance Measures	2013 Actual	2014 Estimated	2015 Estimated
Inputs:			
Electronic record storage capacity (gigabytes)	320,400	320,400	320,400
Outputs:			
Electronic data online (gigabytes)	121,856	122,908	123,960
Website files online (images, htmls, etc.)	246,894,363	269,130,003	291,365,643
Database records managed (millions)	14,589	15,589	16,589
Outcome:			
Data transferred via web (in gigabytes)	111,493	130,136	151,229
Percentage increase in data transferred from last FY*	16%	17%	16%
Efficiency:			
Ratio of electronic data online to storage capacity	38%	38%	39%

Statewide

Policy and programmatic initiatives that should be addressed include:

- With DoIT taking the lead develop model email retention and disposition policy and system
- Development of standards for preservation of the permanent record (pdf /a)

- Establishment of guidelines and standards for procurement authorities and agency staff establish to reference when drafting requirements documents for information systems
- Development of standards and processes for the export of data from legacy systems
- Development of model records retention and disposition schedules for information systems
- Development of model system for archiving of web presence and, most importantly government publications.

Goals and Strategies related specifically to Mdlandrec.net

1. **Security**

a. Improve password security by requiring users applying for new accounts to select a password reminder question and answer. Current account holders would be asked to select a question the first time that they access Version3 in order to update their account information. Users must answer their reminder question correctly to get the password by email
b. Reroute logout so that courthouse users are redirected to county home page instead of the MDLANDREC login screen. Improve validation in search forms to prevent users from entering invalid characters, make sure that required fields are entered prior to submitting the query to the server, and improve query performance. This validation also prevents users from locking up search threads on the servers by hitting the submit button numerous times if they think the search is taking too long.
c. Improve validation in search forms to prevent users from entering invalid characters, make sure that required fields are entered prior to submitting the query to the server, and improve query performance. This validation also prevents users from locking up search threads on the servers by hitting the submit button numerous times if they think the search is taking too long.

2. **Searching**

a. Modify database structure to improve performance and help prevent search queries from timing out.
b. Reduce the number of instances where user has to select desired book from a list of similarly named volumes by cross matching JIS volume references to MSA accession numbers.

c. Improve the accuracy of the value of the ending page of instruments derived from JIS CAIS/COTT data.

d. Add a new search box where the user can input a house number and street name. This search mimics the existing street address search available on the Real Property website. This search can be turned on or off based upon county.

e. Add data update date to website to reflect the most current dataset available in MDLANDREC

f. Add verified date for CAIS/COTT data on the search results and printed results page.

3. **Navigation** Improve navigation by:

a. Allowing users to view an entire instrument if they enter a page number in a jump box for a page in the middle of the

b. Reroute users to page-by-page navigation from the CAIS/COTT search when the ending page of the instrument is unknown so that the user can determine the end of an instrument

c. Reroute users to instrument-by-instrument navigation from the CAIS/COTT search when the ending page of an instrument is known.

d. Display hyperlink for the instrument view only if the ending page of an instrument is known.

4. **Appearance** Website upgraded and overall appearance makes pages easier to read, user interfaces self explanatory, and navigation more efficient.

1. DB2 Download - CAIS. The DB2 download of CAIS Land Record index data from the Judicial Information Systems mainframe has been streamlined by a full redesign of the processes using state of the art programming tools and techniques. This allowed a redesign of the verification system along with the ability to download JIS MISC and PLAT along with LAND data. The new programming allows not only the daily update, but the ability to run an update during the day if such an emergency situation requires it. The new updates complete in about 40% of the time of the old updates

2. DB2 Download - COTT. The DB2 download of COTT Land Record index data from the Judicial Information Systems mainframe has been created with a full design of the processes. The COTT data is the data that were replaced by the CAIS set of data starting in the early 1990s. The COTT data did not have a separate nightly update in the original system, but that has been rectified in this version. The previous updates originally occurred monthly and then was updated to weekly. With this new version, there is a nightly updates of all COTT changes. The new updates complete in about 5% of the time of

the old updates.

3. **Instrument Verification.** To verify that all of the required data has been downloaded. The new verification system verifies to a different level of confidence depending on the step. All verifications except the Base Record Counts also perform any cleanup necessary to ensure both databases match. The individual verifications are list in order of confidence with the most confident at the bottom of the list:
    a. Base Record Counts: This nightly verification performs a count on each table and compares the counts to ensure each table matches.
    b. Year/Month Record Counts: This nightly verification performs a count on each table by Year and Month. Each Year/Month combination is compared between the databases to ensure each combination matches.
    c. Flag Comparison Verification: This nightly verification check to see if the Land Record flags between both database match.
    d. Partial Data Verification: This ad-hoc verification check will check an entire table by downloading the full table from DB2 and then doing a comparison. This can be a lengthily verification step and needs to be set up by staff before it is run.
    e. Full Data Verification: This verification check compares a single data field between both databases using the Year/Month record counts process to check to see if anything does not match. This process will run over the weekends and may be performed either monthly, bi-monthly or biannually

5. **Data Replication.** Complete the data replication model depicted in the Accomplishments section above.

Agency Support of the State IT Master Plan:

Discuss how each of the Agency's IT initiatives supports the statewide Perpetual Objectives and Supporting Strategies. Identify all categories that apply to the initiative (e.g. Statewide, Line-of-Business, Location Specific, Intra-Agency, and/or Inter-Agency).

MDlandrec.net and plats.net (Statewide)

Implementation of mdlandrec.net allowed the Judiciary and the Archives to consolidate access to land record instruments into one standard, consolidated system statewide as opposed to separate systems in each of the 24 circuit courts. Together, these projects:

- Make land records more widely accessible via the Internet
- Reduce or eliminate the need for people to visit the courthouse
- Enable the courts to provide constituents (state and local government, researchers and the land record user community) with comprehensive access to recent and historical land record filings in conjunction with existing materials relating to land use and ownership
- Free the courts from the costs of storing and caring for collections of large, deteriorating materials that are difficult and expensive to maintain and duplicate
- Over time, eliminate the need to maintain costly and bulky microfilm reader printer equipment and film storage devices in the State's courthouses
- Operate in conjunction with ELROI the recordation system
- Provide timely updates and efficient preservation of new land record filings
- Secure the State's significant investment in digital imaging and provide authentication and backup of scanned images through duplicate archival images in the electronic 'vaults' of the Maryland State Archives.

Disaster Recovery (Line of Business / Interagency)

The Archives is completing the build of a disaster recovery site at UMBC and would like to work with agencies to establish DR relationships in which the Archives holds on to security copies of data or hosts applications.

Information Retention Standards (Statewide)

The Maryland State Archives is in the initial phases of redrafting regulations related to records retention. In addition, the Archives will build and prototype a model web-based system for agencies to use to inventory records – a necessary perquisite to

development of a sound records management program.

Interoperability

Land Records Access

The Maryland State Archives is programming interfaces in to the *mdlandrec.net* system for both the State Department of Assessments and Taxation in support of the ground rent legislation passed last year and to the Maryland National Capital Parks and Planning Prince George's County PGAtlas project.

Current Environment:

Briefly describe the current Agency IT environment.

Optimize service delivery while maintaining effective cost controls

Information Technology must continue to improve the enabling infrastructure as technology and process improvements occur. The decision to effect change must be balanced with the

resources and funds available to properly support the business goals of the Maryland State Archives.

Ensure IT systems interoperability

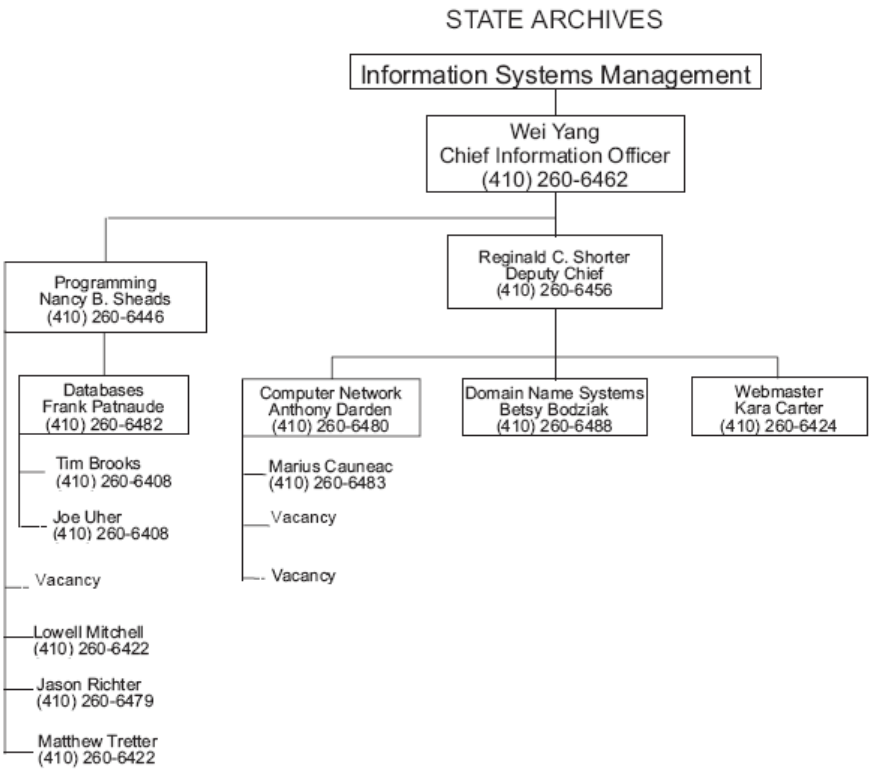
The IT systems supporting the Archives interface with the judicial and other state agencies, creating seamless delivery of services between these agencies is critical to an effective information environment and improved citizen access. Communication between IT personnel at the various agencies should strive to enforce common interface standards. Interoperability with partner agencies will continue to be a major catalyst and hurdle for IT system improvements.

Retention management

Improvements to patron services and information delivery processes require skilled administrative and technology personnel providing quality service delivery, assuring data reliability, controlled access to data, and maintaining data integrity.

IT Resources:

Provide the number of full time dedicated IT staff along with a high level summary of each resource's area of responsibility and expertise. Indicate how many are contractual full time employees and how many are State employees. Provide an organizational chart or narrative summary of your Agency IT department.



Future Environment:

Provide a summary of what the future Agency IT environment will look like, assuming successful completion of short and long-term IT goals. Briefly describe how the resulting future IT environment will enable the Agency to more effectively and efficiently accomplish its mission and deliver service to customers.

The Maryland State Archives is currently in the process of implementing workflow and routing concepts to increase efficiency by concentrating on the routine aspects of work activities. Workflow and routing typically separate work activities into well-defined tasks, roles, rules, and procedures which regulate most of the work. Within information technology, processes in the work place are partially or totally automated by information systems, i.e., computer programs performing tasks and enforcing rules which were previously implemented by humans.

MSA is still in the capturing of its business in terms of the business processes phase, and starting to reengineer each process to improve or adapt it to changing requirements within state government.

Business process redesign includes increasing customer / patron satisfaction, improving efficiency of business operations, increasing quality of deliverables, reducing

cost, and meeting new business challenges and opportunities by changing existing services or introducing new ones. MSA has started workflow management which in terms supports the reengineering of business and information processes.

It involves:

1. Defining workflows, i.e., describing those aspects of a process that are relevant to controlling and coordinating the execution of tasks which includes skills of individuals or information systems required to perform each task.

2. Providing for fast redesign and reimplementation of the processes as business needs and information systems change. Workflow management software will provide the ability to support integration and interoperability among other state agencies providing intra-state sharing with the current missions and goals of the ITMP.

Electronic Payment and Delivery : An electronic payment strategy is being developed, and the priority and sequence of electronic payment capabilities, to include delivery of birth certificates, land records, plats, and images.

Methodologies:

Describe Agency use of the Project Management Institute (PMI) methodology and use of the State's Systems Development Lifecycle (SDLC) processes and templates. Describe any other project management methodologies currently being used and the results realized by their use.

Currently MSA has adapted a methodology of system oriented workflow which will streamline the administrative task of each department, and minimizing human intervention.

Governance:

Describe the Agency's methods for governing IT projects and operations. Include any oversight boards, processes and procedures supporting the State SDLC, and Agency operational processes.

Security:

Identify the actions that the Agency has taken to secure its IT infrastructure including actions the Agency has taken to secure sensitive information such as personally identifiable information (PII). Discuss the Agency's implementation of IT disaster recovery.

The Archives continues to review and enhance security practices and measures as appropriate. MSA network, which hosts several critical systems, leverages a robust security package in support of audit recommendations and compliance. The Archives employs security monitoring, analysis, and response mechanisms to monitor network devices and applications, greatly improving threat identification, mitigation responses, and compliance with network security audits. In addition, Archives continues to

employ Disaster Recovery measures.

2. Agency Certification of Compliance with State Nonvisual Access Regulations

The Agency must certify that information technologies procured, and services provided, are compliant with State nonvisual access regulations (COMAR 17.06.02.01-.12). The IT Nonvisual Accessibility regulations can be found at: http://www.doit.maryland.gov/ *Search: Nonvisual Access.*

☐ By checking the box, the Agency certifies its compliance

6.4 Section 4 – Information Technology Portfolio

Providing detail on the Agency's IT portfolio helps support State IT strategic planning by providing a view of the State's overall IT portfolio. *Recommended: Print Section 4 contents and instructions to reference during data entry.*

IT Portfolio Contents:

- Baseline IT budget
- Current and planned IT Projects
  - Planned start and end dates for each project
  - Perpetual Objective and Supporting Strategy targeted for each project
  - Current State SDLC phase for each project (See Table 1 - State SDLC Phases)
  - For solicitations related to an IT project, provide Contract Award (planned or actual)
- All current and planned Agency IT procurement activity. The type of procurement (e.g. RFP, TORFP, IFB) should be documented as well as a schedule for planned procurement activities including, but not limited to, the following milestone dates:
  - Draft procurement kick-off
  - Procurement submission to DoIT for review
  - Release procurement
  - Begin proposal evaluation
  - Contract award

Table 1 - State SDLC Phases

1 - Initiation	4 - Requirements Analysis	7 - Integration and Test
2 - Concept Development	5 - Design	8 - Implementation
3- Planning	6 - Development	9 - Operations and Maintenance (O&M)

IT Portfolio Scope

The Agency IT portfolio must include any current or planned future IT project meeting the following criteria:

- MITDP
    - Reminder: a project may be deemed an MITDP due to factors other than overall project size. See the definition for an MITDP online at: http://doit.maryland.gov/policies/pages/mitdps.aspx
- Major enhancement (project) being completed under an O&M contract,
- Current Memoranda of Understanding (MOU) or Interagency Agreements (IAs) in place that support an IT project,
- Existing public-facing geographic information system (GIS) initiatives undertaken or already in place including the URL (e.g. Maryland Department of Natural Resources (DNR) "Maps and Map Data" http://dnr.maryland.gov/gis/)

Data Instructions

Use the following instructions to guide completion of the IT Portfolio. Actual data requested varies by project or procurement type.

SDLC Phase –	Enter the SDLC phase as documented in Table 1 - State SDLC Phases
PIR Date –	Enter the date listed on the Agency PIR approval letter (for MITDP in SDLC phases 5-8)
Project Start Date -	Enter the planned or actual project start date for the project. If the project has halted and restarted, enter the start date on which the project restarted for the most recent of SDLC phases 1-4.
Planned End Date -	Enter the planned end date for the project including 1 full fiscal year of O&M beginning after the fiscal year in which the project ends.
PPR EAC $ -	If in SDLC phases 1-4, enter the estimated cost at completion of Phase 4. If in SDLC phases 5-9, enter actual costs at completion of Phase 4.
Project EAC $ -	Enter the estimated cost at completion of the project including 1 full fiscal year of O&M. Estimate at Completion (EAC) is the total updated estimated project cost, combining actual cost to date, plus planned expenditures for the remainder of the current fiscal year, plus planned expenditures for all remaining project years after current fiscal year.
CTD $ -	Enter actual costs through end of FY14. This number should match entries in the Agency's financial systems (e.g., ADPICS).
Project Description -	Enter a short summary of the project.
Project Status -	Enter a short analysis of the current state of the project as of the start of FY14.
Associated Contracts	Enter the name of all contracts, including MOUs and IAs supporting the project to date.

Funding Source - List all funding sources and dollar amounts for all years. FY14 and earlier dollars must be actuals; FY15 dollars are proposed/requested values. Dollar amounts must match other Agency deliverables, including the DA-21 Over the Target Request for FY15.

* During the FY13 budget cycle, Legislature established language that requires approval of an Agency's MITDP project funding request before an Agency can expend funds, for both the project's planning and implementation phases. This is known as the two-step Information Technology Project Request (ITPR) process. The process to request approval for project planning, document the project's attributes, and provide estimates of project schedule, funding and cost information was captured and began with the FY13 ITPR. The *FY15 ITPR Guidelines & Instructions* can be found at the DoIT website at: http://doit.maryland.gov/, Search: "Agency ITPR". (reference http://mlis.state.md.us/2011rs/bills/hb/hb0072e.pdf see pg. 51).

Note: A Project Planning Request (PPR) ITPR estimates the costs for SDLC Phases 1-4 only. After receiving PIR Authorization from DoIT, the Project Implementation Request (PIR) ITPR estimates the costs for SDLC Phases 5-9.

6.4.1 Baseline IT Budget:

Total FY14 Budget (actual):	$1,126,000
Requested FY15 Budget:	$1,126,000

6.4.2 Current Projects (Commencing FY 14 or earlier)

The Maryland State Archives has no current MITDP.

6.4.3 Current Procurements

The following section describes all IT procurements greater than $25,000 that are in any stage between in-development through evaluation.

If no current procurements exist, insert "<Agency name> has no current IT procurements."

6.4.3.1 Current Procurement 1

Copy the following table for each current procurement.

Procurement Title *(include ADPICS number)*	<insert title> (<insert ADPICS number>)
Procurement Type *(RFP, TORFP, PORFP, IFB plus Fixed Price, Time and Materials, or describe other)*	
Period of Performance *(include main period of performance and list option years available)*	<For example, 36 months plus two (2) one-year option years>

Procurement Schedule *(insert procurement milestone dates)*	Draft procurement kick-off: <insert date and "Actual" if date is an actual date> Submission to DoIT for review: Release procurement: Begin proposal evaluation: Contract award:
Associated with What IT Project	<insert IT project name as it appears in this document, including MOU, IA or O&M projects>
Projected Total Cost *(include all option years)*	

6.4.4 Current MOU or Interagency Agreements

The following MOU or IAs are currently in effect for any IT –related activities or support. List any MOUs or IAs regardless whether they support an MITDP.

6.4.4.1 Current MOU/IA Number 1

Type of Agreement (MOU or IA)	MOU
With Whom	University of Maryland Baltimore County
Cost	$100,000.00 per year
Term *(include start and end dates)*	2013-2018
Scope	Provide conditioned space and power in secure area
List all Projects Utilizing the named MOU/IA and associated services Provided	All MSA projects

Type of Agreement (MOU or IA)	MOU
With Whom	Towson University
Cost	$150,000.00 per year
Term *(include start and end dates)*	2013-2015
Scope	Provide IT consulting services for database management, application development and programming services as well as support for GIS appications at the Archives.
List all Projects Utilizing the named MOU/IA and associated services Provided	

Type of Agreement (MOU or IA)	MOU
With Whom	Maryland Environmental Services
Cost	Time and material as needed
Term *(include start and end dates)*	Ongoing
Scope	Support for such things as the automated environmental monitoring system at the Archives.
List all Projects Utilizing the named MOU/IA and associated services Provided	

6.4.5 Other IT Projects

This section describes other IT-related projects per the scope in Section 6.4, including major enhancements being completed under O&M Contracts and/or any current GIS projects.

The Maryland State Archives has no current other IT projects.

6.4.6 Planned Future Projects (Commencing FY15)

This section contains information about any MITDP projected to start in FY15.

The Maryland State Archives has no future MITDPs.

6.4.7 Future IT Procurements

The following section describes all IT procurements of a value of $25,000 or greater that are: planned for award that expect to utilize funds in FY15.

6.4.7.1 Future Procurement 1

Copy the following table for each future procurement.

Procurement Title *(include ADPICS number if one exists)*	<insert title> (<insert ADPICS number>)
Procurement Type *(RFP, TORFP, PORFP, IFB plus Fixed Price, Time and Materials, or describe other)*	
Period of Performance *(include planned main period of performance and list option years available)*	<For example, 36 months plus two (2) one-year option years>
Procurement Schedule *(insert procurement milestone dates)*	Draft procurement kick-off: <insert date and "Actual" if date is an actual date>

	Submission to DoIT for review: Release procurement: Begin proposal evaluation: Contract award:
Associated with What IT Project	<insert IT project name as it appears in this document, including MOU or O&M projects>
Projected Total Cost *(include all option years)*	

1.1.1 Future MOU or IAs

The following MOU or IA pertaining to IT currently are planned for FY15 or beyond.

The Maryland State Archives has no planned IT MOUs.

1.1.2 Other Future IT Projects

This section describes planned future "other" IT-related projects per the scope in Section 6.4, including major enhancements being completed under O&M Contracts and/or any current GIS projects.

The Maryland State Archives has no planned other IT projects.

1.2 Section 5 - Six Year IT Project Outlook

The Department of Legislative Services (DLS) requires DoIT to submit a projection for all Agency projects that may request funds for FY2015 through FY2020 in a Six-Year IT Project Outlook Report. The Six-Year IT Project Outlook Report includes any projects within the six year horizon that are expected to be within SDLC Phases 1 through 9 (Initiation through O&M), including any planned projects that have not yet begun SDLC Phase 1 (Initiation).

The following data is required to be included in the report, beginning in in Section 6.6.1:

Project name – enter the name of the project (if project is listed in Section 4, the names must match)

Brief description – enter a brief description of the project (if project is listed in Section 4, the descriptions must match)

Project Data by Fiscal Year –

Fiscal Year – If the project is an MITDP that has not yet started phases 5-9, enter as much as is known. *Do not delete years from the table.*

Funding Source – GF = General Funds

RF = Reimbursable Funds

SF = Special Funds

FF = Federal Funds

MITDPF = General Funds appropriated for the project and accounted for in the Major IT Development Fund

N/A = the project or system is projected to be closed out prior to a fiscal year

Estimated Project SDLC phase – List all phases expected to be partially performed during the fiscal year. Estimate for all projects unless the project is projected to be closed out prior to a fiscal year (enter "N/A" if this occurs).

Estimated Expenditures – Enter estimated dollars for the fiscal year and funding source. Enter "TBD" for an MITDP not starting Phase 5 before FY15. Enter "0" if the project is projected to be closed out prior to a fiscal year.

Total Estimated Cost – Estimated cost through the 6 year outlook period

1.2.1 Six Year IT Project Outlook

Complete the table below for each IT project or system expected to require funds in fiscal years 2015 through 2020.

1.2.1.1 WorkFlow (Use Word Style Heading 3 for each project)

Project Name	WorkFlow and Routing Management
Brief Description	Workflow management software will provide the ability to support integration and interoperability among other state agencies providing intra-state sharing with the current missions and goals of the ITMP.

Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	N/A	1 - Initiation, 2 - Concept Development	$ 125,000.00
2016	N/A	3- Planning, 4 - Requirements Analysis	$ 100,000.00
2017	N/A	6 – Development, 7 - Integration and Test	$ 550,000.00
2018	N/A	8 - Implementation	$ 250,000.00
2019	N/A	9 - Operations and Maintenance (O&M) – Year 1	$ TBD
2020	N/A	9 - Operations and Maintenance (O&M) – Year 1	$ TBD

		Total Estimated Cost	**$**

1.2.1.2 E-Commerce (Use Word Style Heading 3 for each project)

Project Name	E-Commerce Electronic Payment
Brief Description	An electronic payment strategy is being developed, and the priority for sequence of electronic payment capabilities.

Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	N/A	1 - Initiation, 2 - Concept Development	$ 100,000.00
2016	N/A	3- Planning, 4 - Requirements Analysis	$75,000.00
2017	N/A	6 – Development, 7 - Integration and Test	$ 200,000.00
2018	N/A	8 - Implementation	$ TBD
2019	N/A	9 - Operations and Maintenance (O&M) – Year 1	$TBD
2020	N/A	9 - Operations and Maintenance (O&M) – Year 1	$TBD
		Total Estimated Cost	**$**

1.2.1.3 Enterprise Document Management (Use Word Style Heading 3 for each project)

Project Name	Document and Content Management
Brief Description	To assist the entire state of Maryland seeking to manage the creation, storage, retrieval and expiry of information stored as documents

Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	N/A	1 - Initiation, 2 - Concept Development	$ 125,000.00
2016	N/A	3- Planning, 4 - Requirements	$ 200,00.00

		Analysis	
2017	N/A	6 – Development, 7 - Integration and Test	$ TBD
2018	N/A	8 - Implementation	$ TBD
2019	N/A	9 - Operations and Maintenance (O&M) – Year 1	$ TBD
2020	N/A	9 - Operations and Maintenance (O&M) – Year 1	$TBD
		Total Estimated Cost	**$**

1.2.1.4 Single-Sign on (Use Word Style Heading 3 for each project)

Project Name	Network Single-Sign on
Brief Description	Provide authentication and access control of multiple related, but independent software systems.

Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	N/A	1 - Initiation, 2 - Concept Development	$ 125,000.00
2016	N/A	3- Planning, 4 - Requirements Analysis	$ 100,000.00
2017	N/A	6 – Development, 7 - Integration and Test	$ 100,000.00
2018	N/A	8 - Implementation	$ 250,000.00
2019	N/A	9 - Operations and Maintenance (O&M) – Year 1	$ TBD
2020	N/A	9 - Operations and Maintenance (O&M) – Year 1	$TBD
		Total Estimated Cost	**$**

1.2.1.5 Example Project 1

Project Name	Example Project 1
Brief	Replace existing legacy system with COTS budgeting software.

Description	Assumes that only SDLC phases 1-4 are identified (corresponds to MITDP Project Planning Request (PPR))		
Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase(s) *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	RF	1 - Initiation, 2 - Concept Development, 3- Planning, 4 - Requirements Analysis	$ 1,000,000
2016	RF	5 - Design, 6 - Development	$ TBD
2017	RF	6 – Development, 7 - Integration and Test	$ TBD
2018	RF	8 - Implementation	$ TBD
2019	RF	9 - Operations and Maintenance (O&M) – Year 1	$ TBD
2020	RF	9 - Operations and Maintenance (O&M)	$ TBD
		Total Estimated Cost	**$ 1,000,000**

1.2.1.6 Example Project 2

Project Name	Example Project 2		
Brief Description	Replace existing legacy system with COTS budgeting software. Assumes that only SDLC phases 1-9 are identified (corresponds to an MITDP that has progressed to the Project Implementation Request (PIR))		
Fiscal Year	Funding Source *(one line per source per FY; GF, RF, SF, FF, MITDPF or N/A)*	Estimated SDLC Phase(s) *(See* Table 1 - State SDLC Phases*)*	Estimated Expenditures *(Dollars)*
2015	RF	1 - Initiation, 2 - Concept Development, 3- Planning, 4 - Requirements Analysis	$ 1,000,000
2016	RF	5 - Design, 6 - Development	$ 1,500,000
2017	RF	6 – Development, 7 - Integration and Test	$ 1,500,000
2018	RF	8 - Implementation	$ 1,500,000
2019	RF	9 - Operations and Maintenance (O&M)	$ 1,000,000
2020	N/A	N/A	$ N/A
		Total Estimated Cost	**$ 6,500,000**

1.3 Section 6 - Maryland IT Security Policy Compliance

1.3.1 Objective

The objective for ITMP Section 6, Maryland IT Security Policy Compliance, is to ensure each agency has a documented security plan and procedures to comply with the Maryland Information Security Policy (MD ISP) and current legislation.

For the 2015 FY ITMP, the State is most concerned with information systems containing personally identifiable information (PII). In future years, the system inventory and security compliance matrix will be expanded to meet all requirements defined within the MD ISP.

1.3.2 Background

DoIT requires each State agency under its jurisdiction to annually submit an IT security plan or documented security procedures that address key areas of the State ISP. This requirement is instituted in response to the Data Security Performance Audit (conducted from May 2011 to February 2012), and recent legislation (Senate Bill 676 – Government Procedures – Security and Protection of Information).

The current MD ISP. is located online at :
http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf .

1.3.3 Definitions

- PII – Personally identifiable information is defined as data elements such as an individual's name combined with any one of the following; social security number, driver's license number, financial, tax or health records.

- Information System containing PII data – any State of Maryland automated system that processes, stores, or transmits PII data via any means.

1.3.4 ITMP Section 6 Submission Requirements

DoIT requires each Agency to submit the following as part of its annual ITMP:

1. Agency inventory of any information systems containing personally identifiable information (PII). See Appendix B for inventory format.
    a. If your agency does not maintain or control any systems with PII, provide a statement indicating that fact.
    b. The inventory shall be created and maintained as a separate document from the ITMP.
    c. The inventory shall be updated annually.
    d. The inventory shall be certified as accurate within 60 days of ITMP submission by an Agency Point of Contact (see Section 6.7.6).
2. Evidence of measures to demonstrate compliance with IT security common controls as defined in MD ISP Sections 3, 5 & 6. This can be accomplished by one of two methods :

a. An existing, approved IT security plan meeting the following requirements:
    i. Plan clearly indicates the agency's name and point of contact,
    ii. Plan clearly indicates the authorizing authority who approved the security plan,
    iii. Plan has been reviewed and revised within the past year,
    iv. Plan addresses all common controls listed in MD ISP Sections 3, 5, & 6.
    v. If such documentation is not complete, not current, or not approved, the compliance matrix must be fully completed.

b. A completed "IT Security Policy Common Controls Compliance Matrix" (Common Controls Matrix, as defined in section 6.7.7.

1.3.5 Agency Exemptions

Any agency with no systems containing confidential data as defined above must still provide a statement indicating that fact.

1.3.6 Agency Security Plan Point of Contact

Insert the name of the individual who is the Agency's point of contact for security-related matters. This individual is responsible for ensuring the accuracy of the security-related information submitted with the ITMP.

Name	Reginald Shorter
Role	Deputy CIO
Title	Deputy CIO
Agency	Maryland State Archives
Email address	Reginald.shorter@maryland.gov
Phone number	410 260 6456

1.3.7 Common Controls Compliance Matrix

This matrix is a compiled list of selected "common controls" identified in the MD ISP.

These common controls consist of management and operational controls mandated by State policy to be implemented in all Maryland IT solutions or systems containing data classified as PII.

The scope of the common controls compliance matrix is as defined in section 6.7.3.

	Common Control	Agency Response
	Section 3 Inventory of	

	Assets	
	Does your agency have a documented inventory of IT systems that contain confidential or PII data? *A complete inventory shall include a unique system name, a system owner, a security classification and a description of the physical location of the system.* See Section 2Appendix B – Complete System Security Inventory of PII Systems [For more clarifying information refer to Section 3.0 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [X] Yes [ ] No If Yes, does this inventory contain the required data elements (a unique system name, a system owner, a security classification and a description of the physical location)? [X] Yes [ ] No
	Section 3.1 Information Classification	
	Does your agency clearly identify Confidential information (PII, Privileged, or Sensitive) as "Confidential"? [For more clarifying information refer to Section 3.1 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [X] Yes [ ] No If Yes, describe here how this "confidential" information is clearly identified or labeled: Data deemed "restricted" is based upon approved retention schedules. Restrictions are substantiated by state or federal law, government regulations or court rule. Information subject to such restrictions are not displayed publicly in web applications. The *Guide to Government Records* contains fielded data which alerts staff to the existence of restrictions. In addition, the Maryland General Assembly has given the Archives the authority to redact from public view certain

		specifically designated information based on a petition from the person in interest.
	Section 3.1.1 Information Marking & Handling	
	If portable devices are approved for use within your agency and contained "Confidential" information, is encryption used for protection? [For more clarifying information refer to Section 3.1.1 of the MD ISP.]	*Check one* [X] N/A (No IT systems that contain confidential or PII) [ ] Yes [ ] No
	Section 5 Management Level Controls	
	For IT systems that contain "Confidential" information, does your agency have an ongoing risk management review and evaluation process? [For more clarifying information refer to Section 5.0 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [X] Yes [ ] No If Yes, describe how your organization incorporates a risk management program and the schedule for defining on-going risk. The Archives' Appraisal and Description department routinely meets with senior management of the agency to discuss access issues to archival material. In addition, that department conducts ongoing appraisal of historic government records and incorporates their findings in the *Guide to Government Records.* Finally, MSA Standards committee utilizes best practices with directions from the State Archivist to evaluate workflow and process.
	Section 5.1 Security Assessment & Authorization	

	For each system that contain "PII" , has your agency produced an Authorization to Operate (ATO) document that verifies security controls have been adequately implemented (or plan to be implemented) to protect confidential information? [For more clarifying information refer to Section 5.1 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [X] Yes [ ] No If Yes, is the ATO updated every three years or upon a significant change and signed by a senior agency official? [X] Yes [ ] No If you answered "No" to any of the questions above, your agency is not compliant with this section of the MD ISP. Indicate here what steps your agency plans to take to become compliant and indicate when your agency expects to become compliant. Steps: 1.
	Does your agency conduct annual formal assessments of the IT security controls of information systems that contain PII to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome? [For more clarifying information refer to Section 5.1 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [ ] Yes [X] No Steps: 1. MSA will conduct annual formal assessments when resources are available.
	Are Plan of Action & Milestones (POA&M) documentation in place, for agencies with IT systems, that identifies any deficiencies related to the processing of "Confidential"	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [ ] Yes [X] No Steps: **1.** MSA will investigate the (POA&M) documentation

	information? [For more clarifying information refer to Section 5.1 of the MD ISP.]	process when resources are available.
	Section 5.3 Service Interface Agreements (SIA)	
	Are agencies IT systems with Service Interface Agreement in place for non-networkMaryland connections permitted only after all approvals are obtained consistent with the MD ISP? [For more clarifying information refer to Section 5.3 of the MD ISP.]	*Check one* [X] N/A (No IT systems that contain confidential or PII) [ ] Yes [ ] No
	Section 6 Operational Level Controls	
	Does your agency ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to systems? [For more clarifying information refer to Section 6.0 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [X] Yes [ ] No
	Does your agency identify personnel with information system security roles and	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes

	responsibilities? [For more clarifying information refer to Section 6.0 of the MD ISP.]	☐ No Senior Management - Senior management is charged with IT security programs and its overall program goals, objectives, and priorities in order to support the mission of the organization. Computer System Managers – IT system mangers directs the organization's day-to-day management of its computer security program. These individuals are also responsible for coordinating all security related interactions within MSA. **1.**
	Section 6.1 Configuration Management	
	For agencies with IT systems, are application and operating system hardening procedures created, maintained and up-to-date security? [For more clarifying information refer to Section 6.1 of the MD ISP.]	*Check one* ☐ N/A (No IT systems that contain confidential or PII) ☒ Yes ☐ No MSA IT management believes their planning and preparation activities on a secure baseline configuration for the information systems is developed, reviewed, approved, and implemented utilizing CM best practices. If No, your agency is not compliant with this section of the MD ISP. Indicate here what steps your agency plans to take to become compliant and indicate when your agency expects to become compliant. Steps: 1.
	For agencies with IT systems, have all default system administrator passwords been changed? [For more clarifying information refer to Section 6.1 of the MD	*Check one* ☐ N/A (No IT systems that contain confidential or PII) ☒ Yes ☐ No

	ISP.]	1.
	For agencies with IT systems, have appropriate change management processes been implemented? [For more clarifying information refer to Section 6.1 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No
	Section 6.2 Contingency Planning	
	For agencies with IT systems, has the IT Disaster Recovery Plan been tested? [For more clarifying information refer to Section 6.2 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, identify here the date of the last test for disaster recovery conducted by your organization. <8/7/2013> If No, your agency is not compliant with this section of the MD ISP. Indicate here what steps your agency plans to take to become compliant and indicate when your agency expects to become compliant. Steps: **1.**
	Section 6.3 Incident Response	
	For agencies with IT systems that have experienced a successful Category 1, Category 2, and/or Category 3 security incident in this calendar year, has the incident been reported to	*Check one* [x] N/A (No successful Category 1, Category 2, and/or Category 3 security incidents have been identified in this calendar year) [ ] Yes [ ] No

	DoIT in accordance with the MD ISP? [For more clarifying information refer to Section 6.3 of the MD ISP.]	
	Section 6.4 Maintenance	
	For agencies with IT systems, is system maintenance scheduled, performed, and documented in accordance with manufacturer or vendor specifications? [For more clarifying information refer to Section 6.4 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, identify here the unit within your organization responsible for scheduled IT maintenance. If multiple units are responsible, describe the management process implemented to track such maintenance activities. IT Technical Support
	Section 6.5 Media Protection	
	For agencies with IT systems, has access to system media containing "Confidential" information been restricted to authorized individuals? [For more clarifying information refer to Section 6.5 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, describe here the process or mechanism that enforces this access restriction on IT systems. MSA best practices authorization and authentication concepts consists of username and password along with IP address and / or hostname.
	For agencies with IT systems that have	*Check one*

	electronic media storage for disposal or re-use, is the electronic media appropriately sanitized or destroyed? [For more clarifying information refer to Section 6.5 of the MD ISP Options 1 and 2 for applicable media overwriting techniques.]	[ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, describe here the media sanitation/destruction processes. MSA has adopted the best practice of destruction of electronic media process, so the physically damaged media is not usable by any device.
	For agencies with IT systems that transfer "Confidential" information outside of the agency, is the confidential information securely protected from unauthorized disclosure or use? [For more clarifying information refer to Section 6.5 of the MD ISP]	*Check one* [x] N/A (No IT systems that contain confidential or PII) [ ] Yes [ ] No If Yes, describe here the procedures in place to protect information for such transferred media.
	Section 6.6 Physical & Personnel Security	
	For agencies with IT systems, is physical access implemented to control access to processing equipment, media storage areas, media storage devices, supporting infrastructure (communications, power, and environmental) to prevent, detect, and minimize the effects of	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, describe here how physical access security controls are managed for storage devices, facility, and media storage areas. Physical MSA access controls permits entry to individuals with

	unauthorized or unintended access to these areas? [For more clarifying information refer to Section 6.6 of the MD ISP.]	appropriate authorization and denies entry to individuals lacking appropriate authorization.
	For agencies with IT systems that required security clearances for personnel, are appropriate background investigation (e.g., CJIS, State Police) being conducted? [For more clarifying information refer to Section 6.6 of the MD ISP.]	*Check one* [x] N/A (No security clearances are required for our agency's systems) [ ] Yes [ ] No
	Section 6.7 System & Information Integrity	
	For agencies with IT systems, are systems protected against malicious code (e.g. viruses, worms, Trojan horses, etc.)? [For more clarifying information refer to Section 6.7 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, identify here the anti-virus solution in place for your organization. Symantec Endpoint Security application
	For agencies with IT systems, what Intrusion detection/prevention tools and techniques are deployed?	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No

	[For more clarifying information refer to Section 6.7 of the MD ISP.]	If Yes, identify here the intrusion detection prevention solution in place for your organization what unit within your organization is responsible for daily management of the IDP. Cisco Systems IPS managed by IT System Support
	For agencies with IT systems, are information system security alerts/advisories for critical software being received and reviewed to take appropriate actions? [For more clarifying information refer to Section 6.7 of the MD ISP.]	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [x] Yes [ ] No If Yes, describe here the process that is implemented within your organization, i.e. vendor subscriptions, patched management alerts, industry watch dog lists, etc. MSA complies with the security practice of distributing alerts and notifications to IT system support for review acknowledgment.
	For agencies with IT systems, are systems managed to protect system output during the entire system lifecycle in accordance with applicable federal laws, Executive Orders, directives, data retention policies, regulations, standards, and operational requirements? [For more clarifying information refer to	*Check one* [ ] N/A (No IT systems that contain confidential or PII) [ ] Yes [X] No If Yes, describe here how your organization ensures compliance with applicable laws, policies, directives, etc. If No, your agency is not compliant with this section of the MD ISP. Indicate here what steps your agency plans to take to become compliant and indicate when your agency expects to become compliant. Steps:

	Section 6.7 of the MD ISP.]	MSA will investigate the process and possibility when resources are available.

2 Appendix B – Complete System Security Inventory of PII Systems

2.1 System Security Inventory Scope

The system security inventory documents all automated information systems associated with the agency that contains PII.

Examples of assets associated with automated information systems that contain PII include:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster recovery plans, archived information;
- Software assets: application software, system software, development tools and utilities
- Physical assets: computer equipment (processors, monitors, laptops, portable devices, tablets, smartphones, modems), communication equipment (routers, PBXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies, air conditioning units), furniture, accommodation; and
- Services: computing and communications services, general utilities, e.g. heating, lighting, power, air-conditioning

A complete inventory shall include a unique system name, a system owner, a security classification and a description of the physical location of the asset. See the MD ISP for all system security inventory requirements.

Num	Unique Name of information system containing PII	System Business Owner (Name and Title)	Security Classification *(Public, Confidential)*	Description of the Service the System Supports	Date of Most Recent System Authorization (ex. C&A, IV&V, Authorization to Operate, etc.)	Location of System *(Include externally hosted systems as well as assets containing system backups)*
1.	MDLANDREC.NET	MSA	Public	Land records of Maryland State		MSA
2.	Guide of MD Government Records	MSA	Public	Catalogue of Maryland Government Records Collections		MSA