

State of Wisconsin – Privacy Assessment

April 14, 2008



Table of Contents

1. Executive Summary.....	1
Scope and Approach.....	1
Key Strengths.....	1
Key Recommendations.....	2
2. Detailed Report.....	3
Scope.....	3
Review Objectives.....	3
Approach.....	4
Assessment Criteria.....	4
Conclusions.....	6
Strengths and Opportunities.....	6
Observations and Recommendations.....	10
3. Additional Recommendations.....	12



We are pleased to present to you our observations and recommendations identified during our review of the State of Wisconsin's practices for securing and handling sensitive information. This review required strong collaboration between our professionals and numerous personnel in cabinet level State Agencies. This effort could not have been completed without the immense support and dedication of those State of Wisconsin (State) personnel who assisted us throughout this process.

1. Executive Summary

Scope and Approach

Our review was designed to be a high level overall assessment of the program, policies and practices that are in place to protect sensitive information. This review was not intended to modify or implement revised or new practices, systems or controls, but rather to provide the State with observations and recommendations for planning and potential adoption into their program to safeguard sensitive information.

We compared the State's practices for safeguarding sensitive information against accepted industry practices, specifically controls and requirements specified within the Gramm-Leach-Bliley Act (GLBA), Health Information Portability and Accountability Act (HIPAA) and the FTC Safeguarding rules. To complete this comparison we performed the following steps:

- Reviewed results of the State of Wisconsin Confidential Information Audit for those State Agencies in scope.
- Obtained and reviewed documentation supporting policies, procedures and controls.
- Conducted interviews with personnel from seven State Agencies.
- Performed site visits and observations at three State Agencies.
- Assessed observations and documentation obtained in comparison to applicable regulatory frameworks.

The information identified within this report is based solely on the steps above. No control testing was performed to assess the existence, adequacy or operating effectiveness of controls and observations.

Key Strengths

During our assessment we identified numerous strengths within current practices deployed by State Agencies for the protection of sensitive information. The top strengths are listed below along with opportunities for leveraging those strengths. See section two of this report for detailed information relating to identified strengths and opportunities.

Program Definition

One State Agency out of those we reviewed has developed a formalized privacy office that includes definitions of responsibility and accountability for the direction and oversight of the program to protect sensitive information. Additionally, it was noted that the majority of State Agencies reviewed have developed privacy policies and procedures.

These elements of privacy program definition can be expanded and customized for State Agencies that have not developed, or do not have as robust of a privacy management program. Further, the State could utilize this program definition as the basis for an overall centralized privacy program and standard for all State Agencies.

Information Technology (IT) Server Consolidation

IT server consolidation initiatives were identified that can facilitate the implementation of strong controls and allow the State to take advantage of economies of scale and efficiencies of operation. Initiatives include:

- Several State Agencies are in the process of migrating their IT infrastructure to a state of the art centralized data center that utilizes robust policies and processes for infrastructure and security management.
- The State network is centrally controlled, monitored and protected.

These initiatives give the State the opportunity to review existing data center operations each time incremental expenditures are required for a specific State Agency infrastructure or data center modernization and to assess the most cost effective path for moving forward between function centralization and maintaining existing functions in place. Further, beyond this potential economic benefit these centralized functions maintain strong controls which can enhance the overall protection of sensitive information and potential reduction in the amount of replicated data between State Agencies by facilitating the use of common databases where allowed by law.

Risk Assessment

In 2007 – 2008 the State performed a Confidential Information Audit (overall risk-self assessment) designed to capture information about the protection of sensitive information within State Agencies and to baseline the adequacy of controls to protect sensitive information.

The process deployed by the State in 2007 – 2008 can be utilized as the foundation for the development of an ongoing privacy program risk assessment process that helps to ensure emerging threats to sensitive data are considered and that safeguarding practices are in place to meet the privacy program expectations.

Key Recommendations

The State has implemented many effective practices for the protection of sensitive information as stated in the 'Key Strength' section above. We see these efforts as a foundation to build upon to continue maturing a process that will provide sound policies, standards and controls across State Agencies. The following key recommendations represent the next layer of the building process toward enhancing the program for safeguarding sensitive information.

Develop a Centralized Privacy Management Charter

In order to provide a sound program infrastructure, it is recommended that Privacy Program(s) be established either at the State level or at the State Agency level. The program should be charged with the establishment and oversight of privacy policies, responsibilities and oversight of privacy initiatives, risk assessment and mitigation and effectiveness of implemented information protection controls. This would provide for a cohesive and consistent implementation of required security controls, and foster enterprise wide monitoring and reporting on effectiveness of those controls.

Establish an Annual Privacy Program Risk Assessment Process

The recent Confidential Information Audits that were completed by the State Agencies represent a significant effort towards establishing a baseline for the State Agencies that collect, process, store and transmit sensitive information. This could be expanded into a formal risk assessment process that considers threats and scenarios that could result in a compromise of sensitive information and that assess required controls and practices against a minimum standard for controls. The minimum standard for controls that is utilized in the risk assessment should be based upon accepted industry practices and regulatory frameworks.

Establish Global Privacy Education Program

State employees are required to sign a confidentiality agreement when they are hired. In order to ensure consistency, standardization and adequate dissemination of current privacy practices it is recommended that this initial awareness be expanded into a formalized education program that is performed on a periodic basis. Development of an education program detailing the need for protection of sensitive information and related controls will foster a better understanding by employees of the requirements and commitment the State has towards safeguarding information.

Centralize Vendor Management

Many of the large contractual relationships the State has with select providers are controlled by the Department of Administration. If existing vendors, approved by the Department, cannot provide the needed service to a State Agency, current practice allows for individual State Agencies to broker their own contracts. We recommend that the State enhance the current central vendor management program to ensure all relationships are governed through a single standard. In addition, standardized due diligence processes, vendor assessments and contractual language regarding privacy concerns and expectations would be achieved.

2. Detailed Report

Scope

The scope of the privacy review was designed to be a high level overall assessment of the program, policies and practices that are in place for protecting sensitive information across the various State Agencies. Our review of current practices for securing and handling sensitive information (defined as consumer based (state resident) information held by the State) was conducted in comparison to applicable regulatory guidelines, frameworks and industry best practices. Our review was not intended to modify or implement revised or new practices, systems or controls, but rather to provide the State with options and recommendations for planning and adoption into their ongoing efforts to safeguard sensitive information. Our review included no control testing to assess the existence, adequacy or operating effectiveness of controls and observations.

Our overall level of effort to achieve the objectives outlined was provided on a limited basis. Therefore our efforts needed to be performed on a scope basis within the various State Agencies and we had to rely upon the overall assertions and guidance provided by State personnel. The level of cooperation and assistance we received from the State was immense and without which we would have been unable to complete our assessment.

Review Objectives

The goals, activities and deliverables of this review were designed to assist the State of Wisconsin in meeting the following objectives (see our approach section for activities performed to meet these objectives):

1. Assess the cause(s) of the recent disclosures of sensitive information and identify potential methods to improve practices to help prevent a reoccurrence.
2. Assess the overall program, policies and rules in place to govern practices to protect sensitive data (privacy program) and identify potential program, policy and rule enhancements.
3. Assess the State's governance model and practices in regard to program, policy and rule communication and enforcement and identify potential program, policy and rule enhancements.
4. Review the risk assessment practices utilized by the State to identify the locations and protections for sensitive information and identify potential enhancements.
5. Review incident response and investigation practices in place to assess known or suspected disclosures of sensitive data and identify potential improvements to correct practices in a timely fashion.
6. Review the practices in place to assess third party (vendor) controls and define data that will be shared based upon need and identify potential improvements to reduce the risk of disclosure of sensitive data.

Approach

Our efforts consisted of comparing the State's practices for safeguarding sensitive information against accepted practices within our industry in relation to the established objectives for the review. Controls and practices detailed within the GLBA, HIPAA and the FTC Safeguard Rules were used to benchmark our observations and guide our overall evaluation of the State's practices. These control practices and guidelines are provided in a summary format below in the Assessment Criteria section of the detailed report. To accomplish our objectives we performed the following activities:

- Reviewed results of the State of Wisconsin Confidential Information Audit (Audit) for those State Agencies in scope. The Audit details current State Agency practices for protecting sensitive information. Additional supporting information was also reviewed where applicable.
- Obtained and reviewed State policy, procedure, control or other supporting information (e.g. specific policies, unauthorized disclosure post event analysis) as necessary to support our overall review objectives (detailed above).
- Conducted interviews with key State personnel from the selected State Agencies to verify practices for protecting sensitive information and to verify or further probe results that were documented in the Audit. The State Agencies in scope for the review included:
 - Department of Administration (DOA)
 - Department of Revenue (DOR)
 - Department of Health and Family Services (DHFS)
 - Department of Workforce Development (DWD)
 - Department of Transportation (DOT)
 - Department of Natural Resources (DNR)
 - Department of Regulation and Licensing (DRL)

The targets for our assessment were chosen in cooperation with members from the DOA, based on size and overall amount of sensitive data that is maintained by the respective State Agency above.

- Conducted limited site visits to observe practices in place to protect and handle sensitive information. The sites visited included the following State Agencies:
 - Department of Administration
 - Division of Enterprise Technologies
 - Department of Administration – Printing Facility
 - Department of Revenue

These State Agency sites were selected at random or due to the fact that a previous unauthorized disclosure of sensitive information occurred at that State Agency.

- Assessed and compared the information obtained against applicable control frameworks, regulatory guidelines and best practices.

Metavante Corporation has provided leadership, subject matter experts and personnel to complete this review. We have worked with State personnel throughout the engagement to help ensure that applicable knowledge transfer of State activities has occurred.

Assessment Criteria

In performing our assessment we utilized the following privacy program characteristics and looked for evidence of the following key program characteristics within the State's overall program definition, policies, procedures and practices. Our assessment of the State's practices against these characteristics was limited to a sample based review of the documentation provided by the State and interviews with State Agency personnel to validate observations noted in the review of documentation. The information provided below is included to help establish the context for our expectations of a robust privacy program,

to provide insight to the types of questions we asked and to note some of the criteria that we reviewed to assess the assertions made by the State.

Program Definition – Existence of a formalized privacy program that includes overall accountability for its implementation and oversight, definition of roles and responsibilities for management, and policies and procedures to help ensure the program is consistently communicated and executed.

- Elements for program existence include but are not limited to: Formalized program charter, appointment of a Privacy Officer, privacy policies and procedures, clearly defined reporting framework and documented program assessments detailing effectiveness.

Risk Assessment – Activities designed to identify threats that could result in an unauthorized disclosure or compromise of sensitive information. The risk assessment process also includes mechanisms to identify gaps that could result in a compromise and ongoing monitoring to help ensure identified gaps are resolved to reduce the potential exposure.

- Elements for the risk assessment process include, but are not limited to: Defined list of potential threat/risks including likely scenarios of possible compromises, established framework and methodology for identifying areas of exposure and definition of necessary control objectives/types.

Program Implementation – Formalized policies, procedures and controls in alignment with applicable regulatory guidelines and best practices designed to mitigate the threats that could result in unauthorized disclosures of sensitive information. Further, these controls are assessed periodically to verify they are in place and operating effectively through independent testing or other control verification.

- Elements that indicate the program has been implemented include, but are not limited to: Controls that are in place meet the same objectives as regulatory mandates and guidelines, testing to validate that controls exist and are effective, a process is in place to identify and resolve control issues and an independent audit of program for overall adequacy and effectiveness.

Training and Communication – Processes and procedures to ensure that employees are aware of the program to protect sensitive information and are trained on its importance and their responsibilities.

- Elements of training and communication include but not limited to: Documented education program materials, requirements to certify that policies are read and understood by employees and periodic assessment of awareness effectiveness.

Vendor Management – Activities designed to help ensure any vendors or contractors that receive or handle sensitive information maintain protections that are consistent with the sensitivity or risk of compromise for that information.

- Elements of a vendor management program include, but are not limited to: Policies and procedures for selection and due diligence of prospective vendors, documented methodology for assessing vendor performance and contractual agreements that include appropriate privacy language.

Program Assessment – Periodic assessment of effectiveness of the program to protect sensitive information designed to identify any potential gaps and foster continuous improvement. Results of these periodic assessments are communicated to appropriate levels of management and action plans are developed as necessary.

- Elements of program assessment include, but are not limited to: Documented independent review of the program for soundness and effectiveness, documented improvements or adjustments to the program for continued maturity, documented issues and remediation plans and management reports on status and posture of program.

Conclusions

Strengths and Opportunities

During our assessment we identified numerous strengths within current practices deployed by State Agencies' for the protection of sensitive information. These strengths not only provide a basis for the protection of sensitive information, but are also assets that the State can leverage for use throughout each State Agency. Within this section we have listed several noted strengths along with opportunities to capitalize on these strengths to further enhance sensitive information protection.

Program Definition

Formalized Privacy Office in State Agencies

Strength – One State Agency out of those we reviewed has developed a formalized privacy office and has appointed a privacy officer with responsibility and accountability for the direction and oversight of the program to protect sensitive information.

Benefits – Centralized leadership and assignment of responsibilities is an essential mechanism to help ensure that required policies, practices and processes are developed and deployed as part of an overall privacy program. Additionally, centralized oversight and management helps to ensure a consistent direction is established for the privacy program and that consistent controls are put in place. Further, centralized accountability and oversight helps to ensure the required practices are completed, as a specific task of the centralized management is to obtain reporting from each responsible party relative to their implementation of a privacy program.

Opportunity – The structure that has been developed and deployed for this State Agency could be expanded to be either an overall centralized program for the entire state or it could be administered in a distributed fashion for each of the State Agencies. Either way the concepts and practices that are maintained as part of a centralized program definition can help ensure that the privacy practices within each State Agency meet one prescribed standard.

Policies

Strength – It was noted that the majority of State Agencies reviewed have begun developing or have developed privacy policies and procedures to address the needs and requirements for safeguarding sensitive information.

Benefit – Sound policy language is the foundation for establishing a viable privacy program initiative. Policies set the tone for commitment and direction as well as establishing common objectives for securing sensitive information. Development of a statement of policy regarding privacy requirements helps to ensure controls and programs meet the overall objectives for protecting sensitive information.

Opportunity – These elements of privacy program definition can be expanded and customized for other State Agencies that have not developed a program or could be utilized as the baseline framework for a centralized privacy program and standard that State Agencies must adhere. Further, the State could review all policies that have been developed by the respective State Agencies to identify the best policies for adoption across all State Agencies.

Risk Assessment

Confidential Information Audits (Risk Assessment)

Strength – In 2007-2008 the State performed an overall self assessment process designed to capture information about the protection of sensitive information within State Agencies. Further, this assessment was designed to baseline the adequacy of controls to protect sensitive information. This was completed through the Confidential Information Audits that were performed by the State Agencies providing pertinent information on the status of protection of sensitive information.

Benefits – Periodic risk assessments and controls baselines are critical elements to continually assess the quality of practices to protect sensitive information. In completing these self assessments valuable information detailing the status of how information is being protected has been collected and will serve as a benchmark for evaluating the controls on sensitive information protection.

Opportunity – The process deployed by the State in 2007-2008 can be utilized as the foundation for the development of an ongoing privacy program risk assessment program that can help to ensure that protections are in place to meet overall State expectations. The results of this process can be used by the State to identify areas for potential improvement and to mandate improvements, if necessary. Further, if performed on a periodic basis it will provide the State a mechanism to assess the effectiveness of each of its State Agencies on implementing any mandated improvements over time. Lastly, as threats to sensitive information protection emerge the overall process can be adjusted to consider those threats and to continually challenge State Agencies to adapt controls to emerging threats.

Program Implementation

IT Server Consolidation

Strength – The State has an initiative underway to centralize many of its' processing functions centrally. Several State Agencies are in the process of migrating their IT infrastructure to a state of the art centralized data center operated by the DET. Visiting the Data Center provided some insight to the initiatives underway. We observed several high quality controls in operation within the data center and data center management processes including:

- Well managed computer room operations
- Management appropriately oversees operations with sufficient experienced personnel
- Satisfactory policies and standards
- Reporting that indicated adequate system capacity, performance and availability
- Evidence of sufficient controls and tools in place for capacity planning, processing, job execution, and patch and incident management
- Appropriate data and file backup practices are followed and environmental protections exist
- The State network is also centrally controlled, monitored and protected by firewalls with robust rule sets to detect any foreign anomalies that may be deemed as alleged attacks on the environment

The above controls meet control obligations and requirements defined for infrastructure and data center management as specified within regulatory requirements to support an overall privacy program.

Benefits – Besides providing a basis to meet control obligations dictated by overall privacy requirements the server consolidation initiative is a positive step to gain economy of scales, maintain high quality control over the processing, storage and transmission of sensitive information and provide a suitable environment for the logical and physical protection of information. In addition tighter security controls over who has access to sensitive information and a potential reduction in the amount of replicated data throughout the environment could be realized.

Opportunity – Currently each State Agency has a choice to either maintain their own data center operations, co-locate at the centralized data center or be hosted by the DET. This current structure gives the State the opportunity to review existing State Agency data center operations each time incremental expenditures are required for specific infrastructure or data center modernization, and to assess the most cost effective path for moving forward between function centralization and maintaining existing functions in place. Further, the quality of the control structures in place at the DET data center give the State opportunities to remediate control deficiencies identified at a State Agency through infrastructure consolidation.

Event Logging

Strength – Logging of events, which is an activity important for maintaining audit trails of authorized and unauthorized access attempts is centrally monitored and maintained. Management is currently

evaluating enhancements to the existing logging and monitoring process through the implementation of an automated consolidated logging system. This consolidated logging system will allow the automated correlation of events between multiple State Agencies and the identification of anomalous activities across agencies. This is a positive step on the road to ensuring data access is being appropriately scrutinized for misuse.

Benefits – Implementation of a centralized logging and monitoring system including a consolidated logging system could provide automated early warning to vulnerabilities and unauthorized attempts to gain access to sensitive information. In addition the ability to correlate information from multiple State Agencies in one report could identify sophisticated systematic attacks across State Agencies more quickly.

Opportunity – It is important that event logs continue to be reviewed by appropriate personnel on a regular basis. Implementation of an automated log consolidation and monitoring system not only reduces the manual process of reviewing multiple reports but allows for automated trending and immediate alerts of potential unauthorized attempts to access sensitive information. This can create a significant overall enhancement to the existing control structure for the State.

Data Protection

Strength – Efforts are currently underway by at least one State Agency to replace Social Security Numbers (SSN) with a randomly generated customer ID number. This targeted approach to securing an extremely sensitive data element enhances the overall protection of end consumers. However by law, many State Agencies must keep and maintain sensitive information, such as the SSN for reporting purposes.

Benefits – The generation of random customer numbers to replace SSN information where possible promotes sound security over sensitive data and is clearly a proactive move to protect the identity of individuals. Further the SSN is an example of a specific data element that if compromised even without any other sensitive data element related to it (e.g. name) could be used for identity theft or consumer fraud.

Opportunity – One State Agency we observed has a data protection project underway to assess where sensitive data elements exist. Expanding such efforts across State Agencies with intent to discover where sensitive information elements are stored can provide valuable insight on how the information is protected. This will assist in determining whether stronger controls need to be applied, determine if data is adequately protected or identify if enhancements such as data masking or truncation should be utilized to reduce the risk of compromise.

Data Destruction

Strength – Several State Agencies have policies and procedures in place regarding the destruction and disposal of documents and information when it is no longer needed. We noted through discussion and observation that employees are aware of the importance to shred or render sensitive information unusable when no longer required.

Benefits – Documented requirements on how sensitive information must be destroyed when no longer needed is important to be sure that information cannot be reconstructed and used in an unauthorized manner. Procedures detailing the appropriate methods of destruction based on type of media will help ensure that adequate steps are taken to render the data unusable.

Opportunity – It was noted during the review process that possible inconsistencies in policy language and enforcement across State Agencies may exist. This could cause an inadvertent disclosure of sensitive information if it is not properly destroyed when no longer needed. Standardized destruction methodologies across the State Agencies would greatly reduce the possibility of data compromise resulting from inadequate disposal.

Change Management

Strength – We observed through document review and interviews established change management processes in place across many of the State Agencies that perform application modifications, system upgrades and general maintenance fixes. These established procedures supported key control objectives related to effective change management including requiring changes to be documented, authorized, tested and approved before migration into production. Further, we identified source code management tools, such as ChangeMan, were in place to provide security over source code to prevent unauthorized changes and help to ensure that change practices are followed.

Benefits – An automated change process helps to ensure sound and consistent practices for modifications being made to system or application environments. Source code management tools, such as ChangeMan, are used to help enforce these restrictions as a change cannot be migrated without approval. This process promotes the dual control concept and ensures that no modifications can be erroneously placed into the production environment. This helps ensure changes do not compromise the integrity of the production environment as it prevents unwanted changes that could compromise the security of the overall environment are not made. Furthermore, rigid control over changes aligns the controls to the objectives set by regulatory mandates and guidelines.

Opportunity –The State should compare each State Agencies practice against this identified strength and bring each State Agencies control environment to this level.

Training and Communication

Employee Awareness

Strength – Confidentiality agreements are in place with State employees and a majority of the State Agencies have mandated that confidentiality agreements are read, understood and signed by State employees upon hiring. This helps to ensure that employees understand their responsibilities for securing sensitive information and therefore better complete those responsibilities.

Benefits – Communicating and enforcing policy and confidentiality agreements sets the tone for understanding the seriousness of protecting sensitive information. These agreements can also create positive re-enforcement that State employees who have access to sensitive information understand their responsibility to protect information and help to ensure that privacy requirements are known and understood across the employee base. In some cases this provides the basis to enforce disciplinary action against an employee in the event of misconduct.

Opportunity – The development of a privacy education program on an enterprise wide basis would promote standardization, eliminate some of the noted inconsistencies, and provide assurance that State employees were receiving the same message as it pertains to their responsibilities toward the safeguarding of sensitive information. Consideration should be given to utilizing the confidentiality agreements as a starting point for building a privacy education program and further evolving the requirement to a periodic formalized employee verification of understanding of privacy related policies on an annual basis.

Vendor Management

Vendor Due Diligence

Strength – The DOA is responsible for the oversight of large state contracts and to help State Agencies with vendor sourcing needs. Vendors sign confidentiality agreements and go through relevant background screening prior to establishing a working relationship with the State. Controls and due diligence efforts appear to be adequate for those vendors that the DOA controls to help ensure that vendors have and maintain adequate controls to meet the State's standards for protecting sensitive information.

Benefits – Vendor management oversight is important and having a function dedicated to managing the multitude of relationships the State has with vendors is a sound practice. Ensuring consistent

standards are enforced and that vendors meet the overall requirements for data protection mandated by the State is a critical component in the process requiring contracted vendors to uphold the State's overall security standards. A single DOA point of contact for contract negotiations, agreement specifications, due diligence, and assessment activities helps ensure viable, cost effective and secure relationships are established.

Opportunity – Under the current process, the Bureau of Procurement in DOA oversees enterprise-wide contracts with approved vendors. However, several agencies have been delegated the authority to perform their own procurements and can therefore select vendors that may not have an established relationship with the State. This could result in a State Agency not completing all of the defined requirements in place that help to ensure that vendors maintain adequate security standards. A centralized approach to sourcing requirements or at a minimum a centralized standard that requires certain activities to be completed would strengthen the overall posture and ensure vendors meet the expectations from a privacy perspective before an agreement is completed.

Observations and Recommendations

The State has implemented many effective practices for the protection of sensitive information as stated in the Strengths and Opportunities section above. We see these efforts as a foundation to build upon to continue maturing a process that will provide sound policies, standards and controls across State Agencies. The following represents a list of observations made during our assessment and recommendations that we believe will enhance efforts for the ongoing protection of sensitive information within the State. These observations and recommendations are based upon trends and observations noted amongst State Agencies we reviewed.

Program Definition

Develop a Centralized Privacy Management Charter

Observation – Specific formalized Privacy initiatives were not present in many of the State Agencies we reviewed. Many State Agencies lack the function, roles and responsibilities associated with a Privacy initiative. This could lead to inconsistent execution of proper controls over the safeguarding of sensitive information, monitoring activities and reporting.

Recommendation – In order to provide a sound program infrastructure it is recommended that a State level or State Agency level Privacy Program be established. The program should be charged with the oversight of privacy initiatives, policy setting and governance pertaining to the establishment and monitoring of information security controls to protect sensitive information. This would provide for cohesive implementation of required security controls, and foster enterprise wide monitoring and reporting on effectiveness of those controls. Further, it would help to ensure that all State Agencies meet one centralized standard for sensitive information protection, would provide a universal benchmark to assess the effectiveness of each State Agencies' activities and would help ensure the benefits described above in the Strengths and Opportunities section can be achieved.

Risk Assessment

Establish an Enterprise Risk Assessment Process

Observation – The recent Confidential Information Audits that were completed by the State Agencies represent a positive effort for establishing a baseline for who collects, processes, stores and transmits sensitive information. The State Agencies currently do not have a plan to continuously review and update these assessments to ensure the information collected is accurate. To help ensure the program continues to meet the overall needs of the organization it is important that risk assessments be executed to determine the status of security controls over sensitive information and to help measure the effectiveness of these programs over time.

Recommendation – A formal risk assessment process should be established consisting of a standard framework to be utilized State wide and performed on a periodic basis. This risk assessment methodology should consider threats and risks of compromise of sensitive data and

assessing the overall quality of the controls and practices to mitigate those risks. Further, the assessment methodology should utilize standardized control frameworks based upon regulatory minimum acceptable controls to compare current practices against acceptable targets. The State Agencies must also ensure the risk assessments are updated for changing threats, risks or minimum controls on a periodic basis.

Program Implementation

Establish a Formal Control Testing Program

Observation – The Confidential Information Audits completed by the State Agencies indicate there are reasonably sound security measures in place and efforts underway to ensure the protection of sensitive information. Standards, procedures and controls have been stated to be in place for many of the areas. The information provided on the self assessments is positive; however we were not able to conduct control testing to verify that controls actually exist in our scope of study. It is important to know that the controls implemented are adequate in providing the required safeguarding for sensitive information.

Recommendation – In order to validate the effectiveness of controls to protect sensitive information that have been implemented, a formal testing program should be established. Controls implemented to protect sensitive information may not necessarily be adequate or operating effectively to sufficiently reduce or mitigate the risk of unauthorized use. Testing or validating that controls and procedures are implemented and functioning at prescribed levels is warranted to evaluate overall exposure and determine where weaknesses exist. This will help the State to identify opportunities for improvement on a continuous basis and will help to ensure protections of sensitive information are adequate over time.

Sensitive Information Utilization

Observation – Application development and modifications to existing systems require testing to ensure proper functionality. Replications of live data containing sensitive information is often used in testing environments to recreate a pseudo production environment to thoroughly test changes being made. Security and controls in the test environments may not be at the same level as production environments. Creating an additional copy of the information without the proper access criteria could lead to unauthorized access. Further, additional dissemination of live data within the test environment increases the risk of compromise.

Access to sensitive information should always be managed on the principle of least privilege. Development personnel do not need access to sensitive records to perform their day to day jobs. Ideally, test data should never contain any sensitive information and should consist of fictitious or truncated data if copies of live data are to be utilized

Recommendation – It is recommended that if data containing sensitive information must be used in the testing environment, those data elements should be masked, scrambled or truncated as part of the replication process from the production environment to the testing environment.

Establish Global Data Classification Program

Observation – During our review we did not observe any evidence of an overall inventory of data, therefore classifying and ensuring proper protection exists can be difficult. Additionally, we suspect information could be transferred to or may be maintained on devices other than the traditional mainframe and server platforms. These range from laptop/desktop hard drives, USB sticks to mobile media (PDA's) and backup tapes. As more types of media are used to house information, the overall risk of potential data compromise increases.

Recommendation – The determination of where sensitive information resides is a daunting task. However, we recommend the development of a Data Classification Program to determine where sensitive data resides. Once the locations of sensitive data are identified this will enhance the State's overall program to review the protections in place for that data as they will be able to assess the specific controls and practices that protect sensitive information. Once controls and practices can be

linked with specific data elements the state can ensure, in a cost effective manner, that protections are appropriate for the type of information instead of needing to apply universal protections across all information and environments. In addition, clear and concise standards and procedures should be established depicting how sensitive information is handled including but not limited to transmission, storage and destruction, to help reduce the risk of compromise by reducing the overall number of locations and replications of data.

Internal Policies and Procedures

Observation – Based on our discussions there appeared to be many versions or variants of policies and procedures implemented throughout the various State Agencies. These variants can result in inconsistent standards and procedures being utilized or controls that are not in line with regulatory expectations.

Recommendation – The State should centralize policy making for Information Security and Privacy or ensure that policies are consistent and tied to the same regulatory practices. Individual State Agencies should continue to formalize internal standards and procedures based on the State policies to ensure consistent security and privacy practices are being implemented and are in line with each State Agencies specific needs. The policies should be fully disseminated throughout the State Agencies allowing employees to review the policies that impact their day-to-day operations with an on-going process to communicate new or revised policies and procedures.

Training and Communication

Establish Global Privacy Education Program

Observation – State employees are required to sign a confidentiality agreement when they are hired during the new-hire orientation process. Other than the initial employee acknowledgement we did not observe any additional ongoing requirements for employees to participate in established awareness or privacy education programs. Threats, vulnerabilities and security requirements are constantly changing and it is important that employees understand how these changes effect there responsibilities toward safeguarding sensitive information.

Recommendation – In order to ensure consistency, standardization and adequate dissemination of current privacy practices it is recommended that an enterprise wide training initiative be established. Development of a training program detailing the need for privacy and related controls to protect sensitive information will foster a better understanding by employees of the requirements and commitment the State has towards safeguarding sensitive information. In addition, employees will be made more aware of changes in the day to day practices that require implementation and remain current on the threats and vulnerabilities that could result in a compromise of sensitive information.

3. Additional Recommendations

The observations and recommendations below are additional items the State should consider as part of an overall program towards the safeguarding of sensitive information. State Agencies possessed many strengths which were noted above, the items detailed below were somewhat unique in comparison to our overall recommendations and we felt it was warranted to document them as part of the report.

Security & Quality Control

Observation – The printing facility visited is secured by perimeter access controls for the building (badge readers) and logical access controls for the printers. Additionally, many quality control mechanisms are in place to limit human error during the printing process, such as job check off lists and post-print inspections of mail. Though manual controls existed, they were not reviewed or tested for accuracy by appropriate management at the facility.

Risk – Due to the complexity and volume of printing sensitive information for mailing, human error could occur leading to compromise of sensitive information.

Recommendation – We recommend that State printing facilities further examine their current quality controls when dealing with sensitive information and develop a dual review process (on a sample basis) for mailings or other distributions that contain sensitive information.

Physical Security

Observation – Through observation at the sites visited and conversations with key personnel, it was noted that State locations appeared to have adequate physical security controls in place, such as card access systems, locked doors and security personnel. However, it was also pointed out that information is collected through hard copy forms received at many distributed State offices. Our review did not verify the physical security controls at distributed State field offices.

Risk – Since sensitive information exists at numerous locations throughout the State, a lack of robust physical security controls could lead to information compromise.

Recommendation – We recommend that State Agencies perform as part of an overall privacy program, an assessment of practices at State locations/offices to verify adequate controls are in place to prevent data compromise. Physical security assessments should be conducted on an annual basis to ensure that field personnel are aware of the importance of physical security as it relates to the protection of sensitive information.

Incident Response

Observation – In some instances informal security incident response processes exist to support timely response and investigation of unauthorized activities.

Risk – Not having formal incident response plans in place to timely address security breaches if they occur could lead to inconsistent actions being taken by staff hindering resolution efforts.

Recommendation – We recommend that State Agencies as part of an overall privacy program review and consider developing formal incident response plans to address necessary actions and steps to be taken for any potential breaches.

Information Access

Observation – User access to information and changes made to user access criteria must be properly approved by appropriate State Agency personnel prior to being implemented. However, no ongoing formal access review occurs within State Agencies.

Risk – Job responsibilities for State Agency personnel may change over time and as such their initial authorized access may no longer be appropriate for current job responsibilities. This can result in inappropriate personnel having access to sensitive data due to a lack of a formal access review process.

Recommendation – We recommend that the State Agencies implement a formal access review process to ensure access levels are reviewed and validated for appropriateness including removal of inappropriate access.

Mobile Security

Observation – During the review we noted the absence of formal policies regarding how sensitive data on mobile devices, such as laptops, PDA's and flash drives was to be protected.

Risk – If portable devices are lost or stolen, sensitive data on these devices could be compromised.

Recommendation – We recommend that State Agencies develop policies to address the protection of data in the mobile environment and investigate options to enable mobile device encryption.

About Metavante:

Metavante (NYSE: MV) delivers banking and payments technologies to over 8,000 financial services firms and businesses worldwide. Metavante products and services drive account processing for deposit, loan and trust systems, image-based and conventional check processing, electronic funds transfer, consumer healthcare payments, electronic presentment and payment, business transformation services, and payment network solutions including the NYCE Network, a leading ATM/PIN debit network.

Metavante is headquartered in Milwaukee.