PRIVACY PLAN

TABLE OF CONTENTS

FIGURES

TABLES

1. EXECUTIVE SUMMARY

1. EXECUTIVE SUMMARY

A review of the State's Privacy Program by the Office of Information and Management Technology (OIMT) concluded that there is currently insufficient funding and staff support to meet today's Privacy requirements. Most agencies do not have a dedicated privacy officer, and consistent methods are not used across the State to protect personally identifiable information (PII) as defined in HRS §487(N), HRS §487(R) and in the Federal standards as required.

This document describes the structure and method of the establishment of an Executive Branch Privacy Office and program organization. This document is a living document that will be kept current throughout the course of the program. The intended audience for this document is currently all Executive Branch Agencies.

The OIMT maintains the information technology (IT) infrastructure for a large portion of the state agencies under the Officer of the Governor of the State of Hawai`i.

In addition to guidance and directives regarding IT infrastructure, the Chief Privacy Officer (CPO), under the Chief Information Officer (CIO), also provides guidance, oversight, and assistance regarding privacy.

The CPO is responsible for formulating overarching State privacy policy and overseeing agency/office implementation and achieving the State's strategic goals in support of the OIMT vision for enterprise IT privacy performance. Value to both the customer and the public is promoted through the use of State-approved standards and industry best practices. The CPO will also interface with the Information Privacy and Security Council (IPSC) and assist them with development of their deliverables as well as act as a subject matter expert (SME) when needed.

2. INTRODUCTION

2. INTRODUCTION

2.1 PURPOSE

Protecting privacy is a core need for every State agency, and it is best attained when it is an integral part of the agencies' business operations. Privacy must be considered as part of the up-front appraisal of policy and programmatic decision-making as well as business operations, application development, and associated activities; it should not be an afterthought. Privacy stewardship and governance are keys to a successful privacy program and can reduce the risk that government programs erode privacy protections and ultimately lose the public's trust.

Privacy is a broad and complex concept that arises in a variety of contexts: information privacy (rules that govern collection, handling, and use of PII), bodily privacy (protection against assault of a person's physical being), territorial privacy (limits on the ability to encroach into another person's environment), and communications privacy (protection of mail, telephone, and email). Laws and regulations tend to focus primarily on information privacy issues, particularly as organizations increasingly use technology to collect, process, and store PII on employees and the public. However, information privacy is only one of many privacy issues that agencies must manage.

This document will provide a framework to improve how the State protects PII it is responsible for and also defines the major steps needed to build a consistent and comprehensive privacy program.

Examples of the proposed privacy program requirements include the following:

- Ensure that data at rest and in motion adhere to best practices and federal regulations.
- Ensure success throughout the State with reviews, protection, and reporting requirements under privacy elements including the Federal Information Security Management Act (FISMA) and State of Hawai`i Act 10.
- Oversee privacy training programs and other types of outreach for both agency Privacy Officers and for all departmental personnel.
- Promote analysis, expertise, and remediation efforts for breaches, and partner with security staff in the development of breach prevention measures.
- Monitor all agencies' website PII content and verify their privacy notices for statutory compliance.
- Coordinate with others in promoting adherence to sound privacy practices and procedures, both within and beyond the Executive Branch.
- Establish standards and guidelines for systems logging, cookies, web beacons, statistical aggregation, inclusion, disclaimers for external links, and sharing of information between agencies.
- Serve as chief privacy advisory to senior agency personnel.
- Partner and serve as advisory to the IPSC on privacy subject matters.

2.2 SCOPE

This document will define scope and structure for the privacy program for all Executive Branch agencies. In the future, this program may extend to other State of Hawai`i branches ensuring consistency of privacy protections across the State.

This document relies on the structure and processes detailed in the following OIMT plan documents:

- The State of Hawai`i Information Assurance Plan provides the security plan, phasing, and framework, including security tools and training.
- The State of Hawai`i Policy Plan provides the framework and policies, including structure for classification, protection, transport, and storage of data.

2.3 ASSOCIATED DOCUMENTS

- State of Hawai`i Business Transformation Strategy and IT/IRM Strategic Plan, 2012 (referred to as the Plan)
- Baseline of Information Management and Technology and Comprehensive View of State Services (referred to as the Final Report) prepared for the State by SAIC
- Federal Segment Architecture Methodology (FSAM)

2.4 THE THREAT

There has been growing public concern over identity theft and fraud, and employers are a tempting target for criminals seeking precisely the kinds of data needed to open, access, or change a financial account—such as information combining a name with the associated SSN, driver's license or passport number, current employer, home address, home telephone number, and date of birth.

In 2005, at least 14 large U.S. employers reported security breaches of PII data concerning thousands of current and former employees and dependents. The incidents involved Bank of America, Science Applications International Corporation (SAIC), Adecco Employment Services, Time

Warner, MCI, Purdue University, the U.S. Justice Department, the U.S. Air Force, Motorola, the Federal Deposit Insurance Corporation (FDIC), Eastman Kodak, San Diego County, Boeing, and Ford Motor Company. In early 2006, Ameriprise Financial and Honeywell reported similar security breaches involving employee data. In February 2006, computer security firm McAfee notified employees that a Deloitte & Touche auditor had left an unencrypted compact disc containing their names and social security numbers on an airplane. In March 2006, Fidelity Investments lost data on nearly 200,000 Hewlett-Packard employees on a stolen laptop computer containing retirement fund details. These last two incidents illustrate how a reputable third-party service provider may jeopardize the security of personal data held by an employer.

Notably, most of these data losses were not targeted hacks but simply lost tapes and stolen laptops, which in most cases did not demonstrably lead to instances of identity theft. Nevertheless, the incidents were made public, and in most cases, the affected employees were given free

credit-monitoring services for one to three years and other forms of assistance (such as letters to their financial institutions) to minimize their exposure to theft.

The landscape of the losses continues to change and has shifted away from simple loss of physical media or laptops common ten years ago to more recently the remote hacking of systems. Starting with the 2005 IBM Security Index Reports, there have been strengthening statements that cybercrime will continue to shift away from complex hacking and mass disruption through malware to smaller, more targeted attacks on organizations as a prelude to extortion demands. The reports warn that criminals will increasingly take aim at the most vulnerable point of access to an organization: its own personnel—authorized users who may be tricked or, less frequently, bribed. They state that in some cases, thieves have taken jobs in a target organization for the purpose of gaining access to valuable data. IBM concludes that computer users must be educated to recognize that they may be targeted either as intended victims or as a means of gaining access to their employer's systems and data. Successful efforts to assume the identity of an employee may be designed for fraud or extortion of the employer. This is another instance in which personal privacy and organizational security are corresponding interests—a point that should be emphasized throughout the organization.

2.5 PROGRAM MISSION

The OIMT Privacy Program's mission is to ensure the protection of the privacy information the State holds about individuals, to oversee privacy compliance by the Executive Branch, and to fulfill all State and Federal legal requirements associated with privacy matters.

This protection must occur in conjunction with the government's legitimate need to collect appropriate information about individuals in order to carry out its diverse missions.

As the government strives to increase transparency, improve communications both across government and with the public, and enhance efficiency through the use of new technologies, balancing these imperatives with vigilant privacy protection becomes increasingly difficult. Paired with the explosion of new technologies that support instantaneous communications between people and across continents, the potential for privacy breaches has also increased exponentially.

The State needs to develop and adopt a comprehensive strategy to limit the government's collection, use, and dissemination of personal information, and privacy protection is now more challenging than ever:

- There is increased computerization of records permitting new levels of analysis.
- There is a dramatic increase in the sheer volume of privacy information and in the number of systems containing such information maintained by agencies, including privacy data arising from other agencies as the vision of shared services in the State is realized.
- There are increased opportunities for breaches to occur in both electronic and paper records
- There are increased compliance and reporting requirements from oversight agencies.

We are governed by numerous laws, regulations, and policies that we must comply with in order to fulfill both our privacy protection responsibility and our privacy reporting and related requirements.

2.6 PROGRAM VISION

The OIMT must proactively implement policy that will provide a statewide standard to ensure uniformity in technology standards, process, methods, and system. The OIMT must ensure that these policies are implemented to include recommendations and requirements associated with FISMA, the National Institute of Standards and Technology (NIST), the Federal Bureau of Investigation (FBI), the Criminal Justice Information Services (CJIS) Security Policy, Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (PCI DSS), Americans with Disabilities Act (ADA), Internal Revenue Service Publication 1075, and other standards, agency audit requirements, guidelines, and best practices to comply with numerous laws and reporting requirements concerning policy. The Privacy Policy vision is a lofty one that will take concentrated effort and cooperation across the State for many years. Substantial parts of the vision will require not only funding, but also dedicated staff and ongoing training for employees. By putting solid and consistent privacy policies in place, we will build trust in government by the public in being good and secure stewards of their information, make it easier for staff to understand and meet expatiations, and develop standardized procedures streamlining processes.

2.7 PROGRAM GOALS

The OIMT Privacy Program's goal is to achieve excellence in privacy compliance and protection while reducing the risks to the public, OIMT, and State employees regarding privacy information. A cycle of continuous assessment and improvement will be put in place to not only ensure that we design and build systems and processes with privacy in mind, but also to ensure staff awareness of privacy requirements and put in place automated monitoring to assist them in meeting privacy goals. These risks include civil and criminal penalties: employees can be individually sued or prosecuted, and the department also has civil liability vulnerability. These risks involve general compliance issues with wide-ranging and very serious ramifications. We must work to ensure public trust, to ensure the minimization of negative media exposure, and to guarantee compliance with State and Federal requirements in order to prevent funding issues, additional scrutiny, and loss of State or public confidence.

Privacy Assessment and Compliance: Periodic privacy impact assessments are a vital tool for establishing and maintaining privacy compliance. A privacy impact assessment should be part of the System Life Cycle Development (SLDC) Plan triggered when new personal or PII information is implicated.

A privacy impact assessment provides information about how well policies are understood and followed and identifies areas where policy should be updated to reflect changes in law, regulation, best practices, or organizational business objectives. Periodic assessments demonstrate a strong commitment to a privacy culture and are excellent evidence of compliance efforts. Assessments take into account three perspectives:

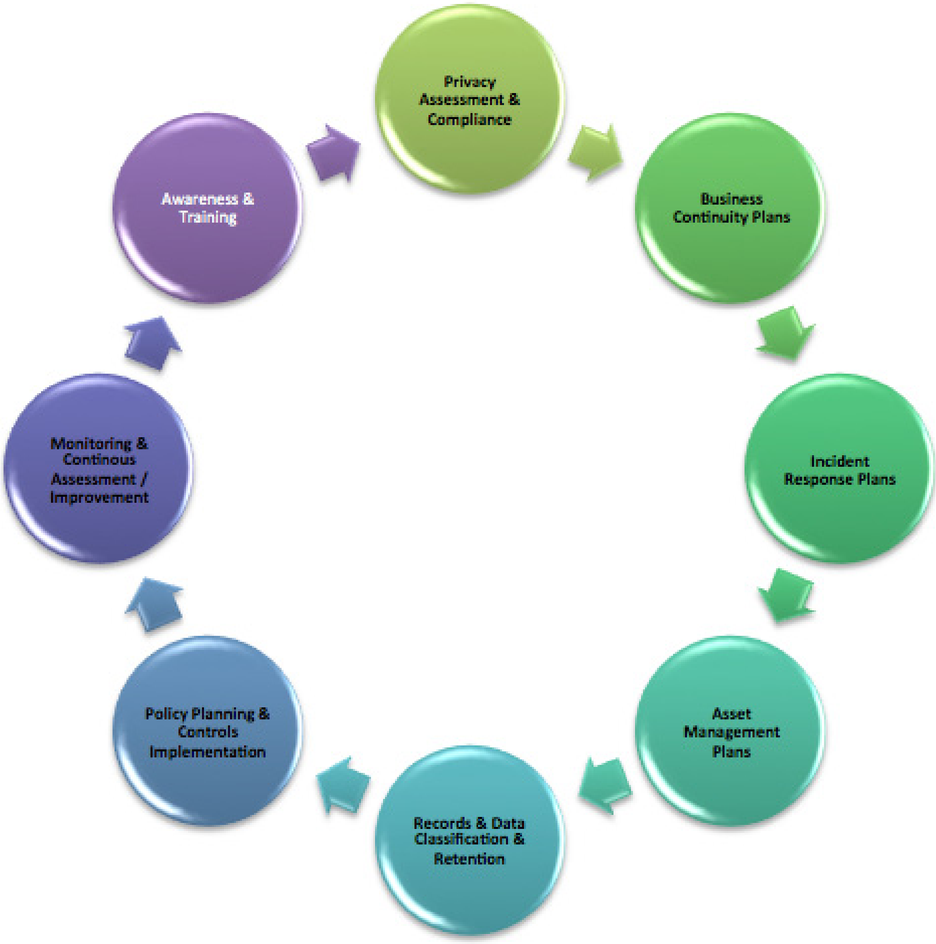
Privacy Assessment & Compliance
Business Continuity Plans
Incident Response Plans
Asset Management Plans
Records & Data Classification & Retention
Policy Planning & Controls Implementation
Monitoring & Continous Assessment / Improvement
Awareness & Training

Figure 1: Privacy Assessment Cycle

- Risks—what are the exposures and what can be done to minimize the effects?
- Readiness—what privacy controls are in place and how effective are they in preventing or detecting privacy breaches?
- Compliance—how well privacy obligations are met and is existing documentation sufficient?

Business Continuity Plan: Identifies exposure to internal and external threats and integrates hard and soft assets to provide effective prevention and recovery for an agency. This document will not go in depth on this subject in that it is covered as a primary subject in other parts of the Plan.

Incident Response Plan: An organized approach to addressing and managing the aftermath of a security breach or attack. The goal is to handle the situation in a way that limits damage, prevents additional exposure of data, and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. Because it is covered as a primary subject in other parts of the Plan, this document will not go in depth on the subject (specifically, it is in the sections on policy and Information Assurance [IA]).

Asset Management Plan: The International Infrastructure Management Manual (2011 edition) defines an Asset Management Plan as "a plan developed for the management of one or more infrastructure assets that combines multi-disciplinary management techniques (including technical and financial) over the life cycle of the asset in the most cost effective manner to provide a specific level of service." As part of this plan, methods to protect data must be tightly integrated. As new systems are put in place, only obfuscated or highly redacted data should be utilized. For systems that are coming out of production, procedures must be put in place to protect and promptly remove any latent data. Because it is covered as a primary subject in other parts of the Plan, this document does not go in depth on this subject.

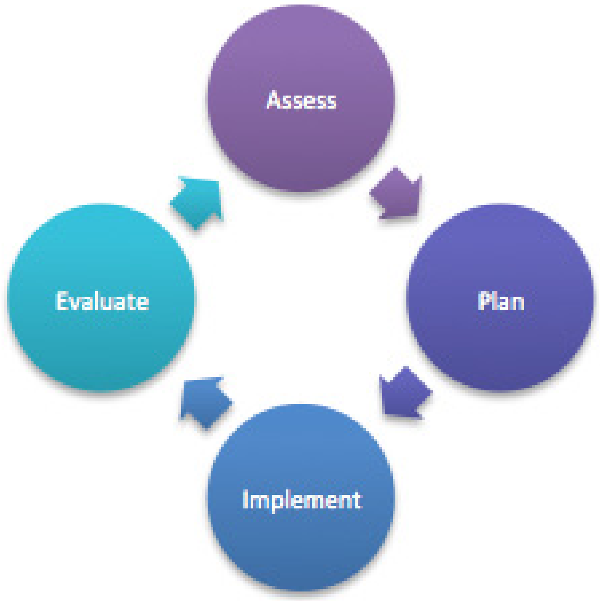

Figure 2: Kaizen Continuous Improvement

Records and Data Classification and Retention: There must be a documented plan put in place for each system and data element defining the need to collect, process, store, and dispose of PII data. Similar to tracking the physical assets you have, you must also keep vigilant track of the data elements you are also entrusted with. Data in a system should also be properly classified. Data classification needs to be coupled as a part of the Information Lifecycle Management (ILM) process—defined as tool for categorization of data to enable agencies to effectively answer following questions:

- What data types are available?
- Where are certain data located?
- What access levels are implemented?
- What protection level is implemented and does it adhere to compliance regulations?

When implemented, it provides a conduit between IT specialists and process or application owners. IT staff is informed about the data value by application owners who better understand the relationships of the data and if it needs to be more securely protected.

Policy Planning and Controls Implementation: Policies are put in place to not only regulate the administration of systems, but how data is handled, what types of logs are required, separation of duties, and many other controls. This is done not only to ensure that a system performs the functions it was built for, but that the data that it depends on is handled and with appropriate care and security.

Monitoring and Continuous Assessment/Improvement: Once privacy controls and policies are put in place, they need to be cared for and adjusted.

First you would need to assess how well things are doing. When the assessment is completed, you would need to plan the changes to be made to ensure the intended outcome. Implementation of the planned changes then takes place, followed by an evaluation of how well those changes faired. This process, illustrated in Figure 2, is commonly known as Kaizen, which can be roughly translated from Japanese to mean "good change." The philosophy behind kaizen is often credited to Dr. W. Edward Deming, resulting in the process sometimes referred to as a Deming Circle. This process may take place in the Privacy Assessment Cycle, shown in Figure 1, to improve the each step in the cycle.

Awareness and Training: If staff is not aware of and do not understand privacy concerns and the elements of data they work with that comprise PII, you cannot expect them to be vigilant in carrying out their duties as intended. Reliance on the coconut wireless is even worse in that as the message moves along, slight changes are made, and if not promptly corrected, result in becoming incorrect institutional knowledge. When privacy best practices, guidelines, or policies are issued, a comprehensive communications and training plan must be at the ready to ensure a successful outcome.

2.8 FAIR INFORMATION PRACTICES

There are many new laws in the U.S. that affect data security obligations, particularly for securing and protecting the kinds of data that potentially place employees and the public at risk of identity theft or fraud (such as SSNs, driver's licenses, and bank account and credit card information) or that touch on the medical and financial aspects of their private lives. This legislation is partly driven by publicity of the growth and cost of identity theft and several substantial security breaches involving employee data. In addition, U.S. state and federal legislators (and occasionally the courts) are increasingly focusing on the privacy of medical and financial information and certain common employer practices that impact privacy interests, such as criminal background and credit checks, alcohol and drug testing, genetic profiling, and employee monitoring and surveillance.

Despite differences in terminology and detail, the typical definition of personal information or personal data is set broadly as any information that is identifiable with a person, and within Hawai`i it is in the Hawai`i Revised Statutes §487(N), HRS §487(R). There are a few collective principles of fair information practices which could be summarized as follows:

- **Purpose and collection limitation:** Personal information should be gathered by fair and lawful means, preferably with the awareness of the individual, and it should be used and disclosed only for legitimate, specified purposes.

- **Data quality and retention:** The personal information collected should be relevant, complete, and not excessive for the intended purpose. The information should come from reliable sources. The information should be kept as accurate and up-to-date as needed for the intended purposes, and it should be retained no longer than needed for those purposes.

- **Notice and awareness:** Individuals normally have a right to know when personal information about them is being collected, saved, used, or revealed to others. They should be told what kind of information is collected, who has access to it, how it will be used, how it will be protected, and the options they have regarding its collection and use.

- **Choice and consent:** Individuals should be given choices, whenever feasible, about the personal information collected and how it is used. For example, legal and business requirements specify the information that must be collected, stored, and disclosed to banks or intermediaries when persons order a service and pay for it by credit card, but additional use of some of those personal details (e.g., to create a marketing mailing list) should be subject to an opt-in or opt-out choice.

- **Security:** Personal information should be protected at all times by appropriate technical and organizational security safeguards to avert loss, misuse, destruction, modification, or unauthorized access or release.

- **Accountability, enforcement, and recourse:** Agencies that handle personal information should appoint staff to be responsible to develop privacy and security policies, train relevant staff and contractors, and take proper steps to ensure that privacy and security policies are effective and enforced. Agencies should provide contact points for questions.

As a result of these trends and needs, system architects and owners are faced with the task of reconciling privacy requirements with systems and applications that were designed for organizational efficiency and security. Privacy policies usually result in new or modified system requirements, such as:

- Displaying privacy notices and options online and in printed forms and reports

- Recording and implementing individual opt-in or opt-out choices

- Creating and enforcing fine-grained internal access controls and authentication procedures designed to protect privacy

- Using spiders or other software to find all the instances in which the organization collects personal data online or stores personal data on its systems

- Scrambling or abstracting personal data in certain applications and reports. This could be done in such a manner to suppress the display of all but the last four digits of identifier. Note that due to privacy concerns in Hawai`i, it is not recommended to use the last four digits of an SSN on documents or reports.

- Logging or tracking the use of personal information and its disclosure to third parties

- Monitoring the interfaces with outsourced service providers that handle personal information from the organization, and establishing the capability to assess their compliance with privacy and security requirements

- Applying legal or contractual restrictions on personal information transmitted from other organizations or jurisdictions (such as credit reports and background checks, health insurance enrollment and claims records, and HR data transmitted from Europe subject to Safe Harbor Privacy Principles or model data-protection contracts)

- Establishing mechanisms to identify personal information compromised in security breaches and to comply with security breach notice requirements

- Ensuring compliance with applicable data retention and data destruction requirements for sensitive personal data

As is true for information security in general, privacy solutions tend to be lower in cost and more effective when they are designed into a system from its inception rather than bolted on later. For example, encrypting or redacting SSNs or replacing them with a randomly assigned identifier in an existing application or report is notoriously costly and time-consuming if the application was not designed with this prospect in mind. Self-service access to personal data, with automated means of making or requesting options and alterations, is much more efficient over the long term than responding manually to every such request. The ability to tag data originating from a particular party or jurisdiction may be a critical feature for compliance with a law or contract that is very difficult to add to an established database.

Ideally, system designers should identify privacy requirements as early as possible in the development or procurement cycle, as well as when revising existing systems. Architects may have to prompt the agencies to help delineate requirements when new or modified systems are envisioned. To do this, it helps to have a basic understanding of trends in privacy norms and regulations and the kinds of functionality that may be required to comply with the State's current and near-future privacy requirements.

There are many more data flows than ever before between the State and third parties (often crossing jurisdictional borders), and many of these include personal information. The reality is that information is rarely an in-house affair in its entirety. Outsiders such as business partners, vendors, auditors, insurance underwriting, and claims personnel, and a variety of technical and management consultants have at least limited or intermittent access to some of the State's data. As a result, we must manage the operational, security, and liability risks that follow from multiple data flows and distributed access to personal information collected and used by the State. Ultimately, this complicates the job of the architects and owners of enterprise systems.

2.9 HEALTH DATA

In 2001, the Federal Department of Health and Human Services (HHS) finalized medical information privacy and security regulations required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 USC §1301 et seq. The HIPAA Privacy Rule, 45 CFR Parts 160 and 164, took effect in 2003 (it is available, along with related materials, on the HHS HIPAA website). A separate HIPAA Security Rule was later adopted, and it specifies much more detailed security standards effective in 2005 or 2006, depending on the size of the health plans involved.

Due to the complexity and expertise required in the proper execution and compliance of required HIPAA privacy elements, the development of privacy policy for HIPAA data elements within the State are intended to remain the primary responsibility of the privacy SMEs in the agencies that collect and/or process HIPAA data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.10 CRIMINAL JUSTICE DATA

Due to the complexity and expertise required in the proper execution and compliance of required Criminal Justice Information Services (CJIS) privacy elements, the development of privacy policy for CJIS data elements within the State are intended to remain the primary responsibility of the privacy SMEs in the agencies that collect and/or process CJIS data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.11 PROTECTION OF DATA BELONGING TO MINORS

The proper protection for data associated with minors (persons under the age of 18) is very nuanced and best left under the direct input from those who interact and manage the data on a daily basis. The *Privacy Plan* will place the primary responsibility for the development of specialized privacy protections for these data elements with the privacy SMEs in the agencies that collect and/or process this type of data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.12 PRIVACY TRAINING AND AWARENESS

Privacy training and awareness programs are key elements of building a culture of privacy. Training programs reinforce the implementation of a privacy policy and reduce the risk of privacy incidents throughout the State. Training and awareness are critical elements of an effective privacy program. One project goal is to put in place the requirement that all employees and contractors receive mandatory annual privacy training. Successful completion must be documented (and on file) at least once per year.

A best practice is that all personnel must successfully complete privacy training before permitted access to State information and information systems. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties. Another best practice is to require those personnel who cause or commit a PII breach to take PII refresher training with documented completion for every reportable breach. Both the annual and PII refresher training should include acceptable rules of behavior and the consequences when the rules are not followed. For areas that have authorized telework and other remote access programs, training should also include the rules of those programs.

2.13 PRIVACY RISK MANAGEMENT AND COMPLIANCE DOCUMENTATION

The Federal government Privacy Impact Assessment (PIA) and System of Records Notice (SORN) are the primary tools to identify holdings of PII, assess privacy risks, and implement privacy protections in their systems and programs. Currently in the State, the Information Privacy and Security Council collects yearly information about PII systems. This manual process is envisioned to be transformed into an automated system and aligned following best practices of the proven Federal system. Requirements for a PIA for all IT systems, whether or not they collect PII, would be established as well as a blanket or adapted PIA for third-party social media. This would not only assist staff awareness of the need for additional protection of systems, but would also streamline systems administration processes and raise overall staff awareness of privacy requirements and concerns.

The Privacy Act requires Federal agencies to issue SORNs for every system of record under their control that collects PII and from which a person's records are retrieved by a unique identifier. A SORN is a legal document used by the Federal government to promote transparency and provide notice to the public regarding their rights and procedures for accessing and correcting PII maintained by the agency. This process can also be adopted for State use as part of the Privacy program.

Another Federal PII tool is the Privacy Act Statement (PAS). A PAS is required on all Federal official forms (paper and electronic) that an organization uses to collect PII from members of the public or Federal employees. These statements inform individuals at the time their information is collected what the legal authority for and purpose of the collection is, and how the organization will use the information. Privacy Act Statements also notify individuals whether providing the information requested is mandatory or voluntary and the consequences of failing to provide the information. Implementation of a similar program in the State can help to instill confidence and provide transparency to the public in the data that we collect.

3. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

3. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

The Privacy FTE and resources will be utilized to provide coordination, oversight, and comprehensive privacy program direction for privacy matters across the Executive Branch. This will support OIMT mission goals by increasing accountability, and enhancing functional integration; the results orientation to be utilized will also permit increased alignment between OIMT privacy across the Executive Branch with OIMT enterprise initiatives. We will utilize this FTE to assist in the updating of procedures and training. The FTE will conduct improved oversight of the new procedures and training, which will decrease the State's risk. It will provide support to all the Executive Branch agencies for successfully complying with the various FISMA reviews. Efforts can be undertaken to promote greater privacy and security awareness throughout the State. Providing the required FTE and resources as well as implementing recommendations in the Security and Privacy programs can be expected to reduce not only the number, but also the severity of the privacy breaches.

3.1 PRIVACY PROGRAM MILESTONES (NON-STAFFING)

Table 1: Milestones (Non-staffing)

Milestones	Person or Team Responsible	Planned Completion Date
OIMT Directive on Administration Policy	Privacy Officer, Information Management Chief, OIMT	
FY15 Annual Privacy Report (recurring)	Privacy Officer	FY-2015 (need FTE on board)
Annual Review of Privacy websites for compliance	Privacy Officer	Continuing; Annually (need FTE on board)
Agency/Office Quarterly/Annual PII Assurance Report	Agency and Departmental Privacy Officers, OIMT	
Complete and deploy computer-based training (CBT) for all OIMT employees, contractors, etc.	Privacy Officer	FY-2015 (need FTE on board)
Develop and deploy at least nine role-based training modules (CBT)	Privacy Officer, Contractors	FY-2015 (need FTE on board)
Employee awareness and outreach to agencies/offices	Privacy Officer	FY-2015 (need FTE on board)
Monitoring/oversight of agency/office Privacy implementation	Departmental Privacy Officers	FY-2015 (need FTE on board)
Certification and Accreditation for Privacy Officers and specialists	Agency/Departmental Privacy Officers	FY-2015 (need funding)
Update OIMT Privacy regulations/Privacy Manual sections	Privacy Officer	FY-2015 (need FTE on board)
Full training program for all staff	Privacy Officer	FY-2015 (need FTE on board)

3.2 PRIVACY PROGRAM MILESTONES (STAFFING)

Table 2: Milestones (Staffing)

Milestones	Person or Team Responsible	Planned Completion Date
Meet with Human Resources	Privacy Office, Information Management Chief, OIMT Business Manager	
Write PDs	Privacy Officer	
Classify PD	OIMT HR	
Advertise vacancies (open continuously)	OIMT HR, OIMT Business Manager, DHRD	
Pull first set of applicants (SR 22-26)	DHRD, OIMT HR	
Set up interviews	CIO Business Manager, Privacy Officer	
Finalize interviews; give cert and recommendations to CIO for approval	Privacy Officer	
Pull second set of applicants	OIMT HR	
Approval from CIO	Information Management Division Chief, Dept CIO, CIO	
Provide cert to OIMT HR for processing	OIMT Business Manager	
Set up Interviews for second set of applicants	OIMT Business Manager, Privacy Officer	
Make first offer	OIMT HR	
Finalize interviews (second Group); give cert and recommendations to CIO for approval	Privacy Officer	
Pull third set of applicants (if needed to fill two FY-2014 vacancies)	OIMT HR	
Hire first applicant (on-board)	OIMT HR	
Make second offer	OIMT HR	
Set up interviews for third set of applicants	OIMT Business Manager, Privacy Officer	
Finalize interviews (third group); give cert and recommendations to CIO for approval	Privacy Officer	
Make third offer	OIMT HR	
Hire second applicant (on-board)	OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2015 to cover shortfalls in hiring in FY-2014, up to two positions	OIMT Business Manager, Privacy Officer, CIO, Information Management Div. Chief, OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2015 = one additional position	OIMT Business Manager, Privacy Officer, Deputy CIO, Information Management Div. Chief, OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2016 = one additional position	OIMT Business Manager, Privacy Officer, Deputy CIO, Information Management Div. Chief, OIMT HR	

4. COSTS

4. COSTS

4.1 IDENTIFY PROGRAM COSTS (INCLUDING COSTS APPROVED BY THE OIMT)

Table 3: Estimated Program Costs

Description	Estimated FY-2014 Costs (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Meet with Human Resources	Pending Review	Based on existing union contract wages
Contractor support for development of up to nine Privacy role-based training modules[1]	Pending Review	Based on estimate for CBT development
Total	Pending Review	

In addition to the program costs summarized above, the annual operational costs in Table 4 below are expected for each subsequent fiscal year starting in FY-2014, with an increase of one FTE SR-22/24 in FY-2015 and an additional one in FY-2016, which brings the total Privacy staff to three FTEs SR-22/26. These annual costs will be used as the basis for Total Cost of Ownership.

Table 4: Annual FY-2014 Operating Costs

Description	Estimated Annual Budget (Starting in FY-2014 – 4 % Increase for Each Out Year) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Ongoing FTE expenses for two Privacy Specialists	Pending Review	Estimate of salaries
Travel:		
Travel to Agency locations for Privacy Compliance and Training	Pending Review	Based on contractual expenses for no less than four trips/annually (includes transporting supporting documentation)
Other Services:		Based on estimates from the International Association of Privacy Professionals, OPM security clearance estimates, and professional insurance
IAPP membership	Pending Review	
IAPP cert exams	Pending Review	
IAPP cert courses	Pending Review	
Bookmarks, monuments	Pending Review	
Training for Privacy staff	Pending Review	

[1] *Cost assumes that a statewide CBT system is procured as noted in "The Plan" that these modules can be installed in.*

Description	Estimated Annual Budget (Starting in FY-2014 – 4 % Increase for Each Out Year) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Update/new security clearances	Pending Review	
Professional insurance	Pending Review	
Equipment:		
Scanners, printers, laptops, docking stations, monitors, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Communications:		
BlackBerries, teleconference lines, etc.	Pending Review	
Print pamphlets, supplies, and minor contracts for updating CBTs	Pending Review	Based on estimates from OIMT, current supply expenditures, and privacy pamphlets
Total	**Pending Review**	

Table 5: Estimated Additional Funding Requirement (FY-2015)

Description	Estimated Annual Budget (FY-2015 and FY-2016) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Develop performance metrics, analytics, investigation, and compliance tools	Pending Review	Based on contractor support estimates
Personnel Costs:		
Ongoing FTE expenses for one additional Privacy Specialists	Pending Review	Estimate of salaries
Travel to agency locations for Privacy Compliance and Training	Pending Review	Based on contractual expenses for no less than 4 trips/annually. (Includes transporting supporting documentation)
Other Services:		Based on estimates from the International Association of Privacy Professionals, OPM security clearance estimates, and professional insurance
IAPP membership	Pending Review	
IAPP cert exams	Pending Review	
IAPP cert courses	Pending Review	
Training for Privacy staff	Pending Review	
Update/new security clearances	Pending Review	
Professional insurance	Pending Review	
Contractor assistance	Pending Review	

Description	Estimated Annual Budget (FY-2015 and FY-2016) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Equipment:		
Scanners, printers, laptops, docking stations, monitors, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Communications:		
BlackBerries, teleconference lines, etc	Pending Review	
Total	**Pending Review**	

4.2 CRITICAL SUCCESS FACTORS

Critical Success Factors (CSFs) increase the probability of success when management focuses attention in these areas. This program's CSFs are:

- Timely commitment of funds and processing of required acquisitions
- Availability of appropriately skilled staff and contractors to complete program tasks and deliverables
- Participation and commitment of program team to complete their tasks and deliverables on schedule

4.3 PROGRAM STAFF DELIVERABLES

With a complement of two Privacy Specialists identified to be hired FY-2014, the OIMT Privacy Office will accomplish the following in FY-2015:

- Enhance agency oversight for FISMA (quarterly and annual) review and reports.
- Improve coordination with Cyber Security with the provision of coordination between the agencies in support of responding to PII Breaches.
- Provide greater oversight and guidance on handling Privacy information contained in systems being decommissioned, transferred or migrated.
- Review agency/office system notices for accuracy and validity. Correct notices where needed and provide guidance to agencies/offices.
- Provide oversight and reviews of the information classification documentation, ensuring Agency Privacy Officers utilize the correct data from these databases in their work with systems documentation, privacy reporting, and other privacy concerns.
- Review of System Privacy Impact Assessments (PIAs) as currently collected by the IPSC for Privacy requirements.
- Review of web pages for Privacy compliance through reports provided by the Access Hawaii Committee.
- Update the OIMT Privacy manuals and handbooks and write new policies, procedures, and templates where needed.
- Provide assistance to the Information Privacy and Security Council.
- Build the plan for incorporating SORN, PIA, and PAS within the State

With the hiring of one additional Privacy Specialist per year until the OIMT reaches the recommended three specialists, one Privacy Officer, and the purchase of automated PII assurance solutions, the Departmental Privacy Office will be able to accomplish:

- Enhanced agency oversight for FISMA (quarterly and annual) review and reports
- Better coordination with Cyber Security with the provision of coordination between the Department's and agency's Identity Theft Task Forces in support of responding to PII breaches
- Provide greater oversight and guidance on handling Privacy information contained in systems being decommissioned, transferred or migrated
- Develop and update Orientation to the Privacy CBT (mandatory for all employees, contractors, and volunteers)
- Review agency/office system notices for accuracy and validity. Correct notices where needed and provide guidance to agencies/offices.
- Provide oversight and reviews ensuring Agency Privacy Officers utilize best practices and standards in their work with systems documentation, privacy reporting, and other privacy concerns
- Review of System PIAs for Privacy requirements
- Review of web pages for Privacy compliance through reports provided by the Access Hawaii Committee

- Updating of the OIMT Privacy manuals and handbooks and writing new procedures and templates where needed
- Conduct Privacy technical evaluation and compliance reviews for the OS, agencies, and offices
- Develop role-based Privacy training
- Develop and conduct Privacy workshops and Privacy awareness campaigns
- Creation of a centralized risk assessment and PIA file collection across the Executive Branch
- Enterprise-wide examination of offices, in coordination with agencies, for PII coverage
- Enterprise-wide examination of offices, in coordination with Agencies, for PII Reviews
- Enterprise-wide examination of offices, in coordination with Agencies, for best practices in privacy protection in paper and electronic records
- Vigilantly keeping current with new privacy legislation and guidance, and promptly disseminating it and incorporating it into agency practices
- Increasing and stronger liaisons with external agencies, commissions, and working groups regarding government-wide privacy policies, initiatives, and matters
- Adoption of a very proactive stance regarding privacy guidance and implementation throughout the State to promote best practices and minimize risk while coordinating with other key programs
- Availability for providing ongoing privacy subject matter expertise for the highest offices within the State, as well as increased ongoing support for agencies including their Privacy Officers
- Provide assistance to the Information Privacy and Security Council

4.4 ASSUMPTIONS

Success is predicated on hiring requested staff, contractor support, fulfilling financial resources (e.g., procuring tools), implementing policies, authorities, and processes as requested.

4.5 TECHNICAL CONSTRAINTS

The Privacy Program will need new and more sophisticated tools to more effectively track, monitor, and analyze the outputs and performance of the program. It will be necessary to have these to better determine and analyze quantitative and qualitative measures for the effectiveness and overall performance of privacy compliance and quality at the department. To have this evaluative capability, there will need to be new metrics, analytics, and measures for privacy compliance and for privacy violations, as well as tools to assist in investigation of privacy performance. The data will provide value in measuring levels of compliance, quality assurance across the department, areas needing correction and enforcement, and provide for improved program management.

5. RISKS

5. RISKS

This section summarizes major program risks discovered at the start of the program. This program's risks will be monitored and reported as part of the Privacy Program Risk Register.

Table 6: Risks

ID	Description	Probability 1 = low 5 = high	Impact 1 = low 5 = high	Mitigation Plan
1	Personnel overcommitted due to other tasks, existing duties, illness, vacations, etc. may delay program	5	5	Ensure Agency/Office Privacy Officers have backups
2	Contracting delays for procurements may delay program or increase costs	4	4	Extend Program schedule, as necessary; keep CIO and OIMT Business Manager informed of anticipated cost issues
3	Failing to comply with State laws and the voluminous FISMA review and reporting requirements would be devastating to the Department.	5	5	Ensure Senior Managers are aware of potential fallout from non-compliance; and recommend personal liability insurance be required for all Privacy Officers
4	Failure to publish a PIA prior to collection of information covered by the Privacy Act	5	5	Use annual PII reviews to warn delinquent Agencies/offices about potential costs; ensure employee awareness of requirements
5	Failure to draft a PIA for a system included in an agency's IT investment portfolio can subject the agency to non-approval by OIMT of its investment.	5	5	Ensure PIAs are conducted as regular part of annual review process
6	Failure to protect PII or SSNs could result in identify theft, Legislature inquiry, bad media coverage, loss of public confidence in the State government, financial loss to the individual and the State government, and may result in official Departmental reprimands or termination and may have budget consequences for the affected program.	5	5	Acquire software to capture unencrypted PII to prevent breaches; conduct annual survey/review for use of PII in conducting business to minimize use/risk
7	Remediating a major breach, for example, the loss of a laptop with unencrypted SSNs or PII of numerous citizens, could cost the State millions of dollars and thousands of work hours	5	5	Get PLMS approved and ensure agencies commit to it; consider methods for determining where money to pay costs will come from, and control use of laptops

6. STAFFING PLAN

6. STAFFING PLAN

6.1 FY 2014-15 TEAM STRUCTURE (NOTIONAL)

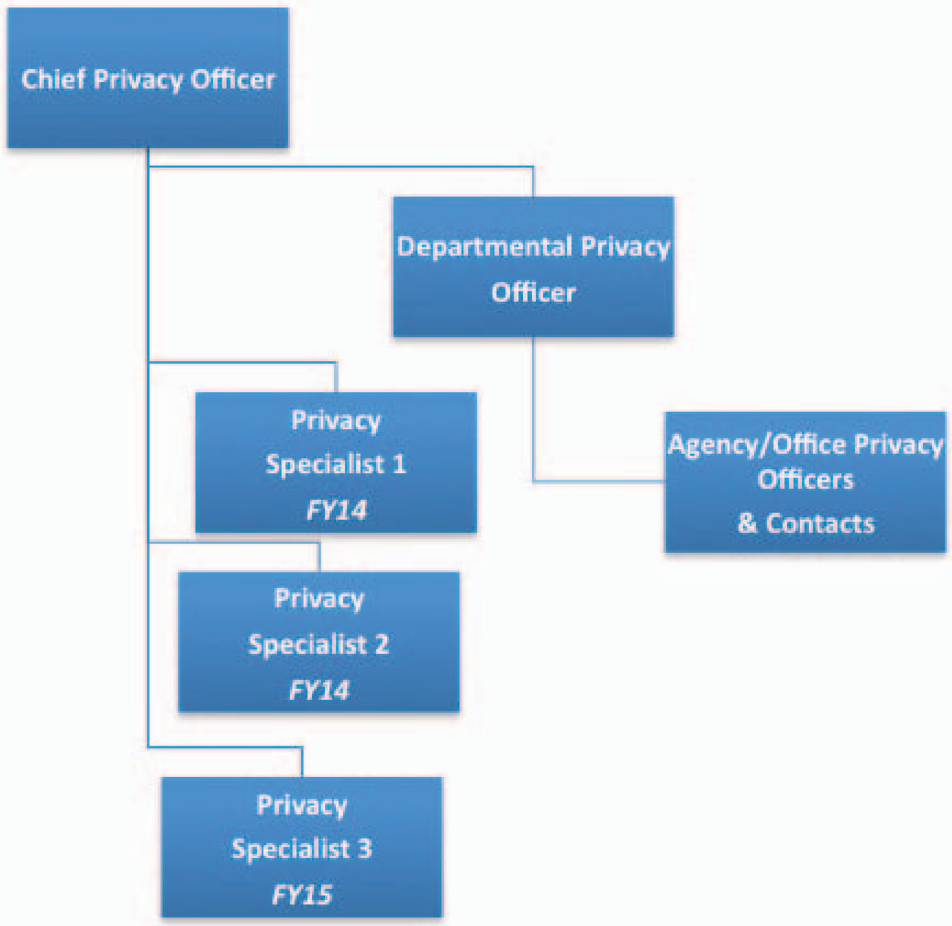
Chief Privacy Officer
Departmental Privacy Officer
Privacy Specialist 1 FY14
Agency/Office Privacy Officers & Contacts
Privacy Specialist 2 FY14
Privacy Specialist 3 FY15

Figure 3: Privacy Program Team Organization Fiscal Year 2014-15

7. RESOURCE REQUIREMENTS

7. RESOURCE REQUIREMENTS

7.1 ROLES AND RESPONSIBILITIES

Table 7: Roles and Responsibilities

Role	Responsibilities
Sponsor(s): Senior Agency Official for Privacy/Chief Information Office Assistant Secretaries, Agency/Office heads, and Budget Officers	• Commit to the scope of this Plan • Authorize program funding/resources required to successfully meet objectives of this Plan, including full compliance with State privacy laws and policies • Be accountable for the success/failure of agency/office compliance • Participate in Identity Theft Task Force meetings, as appropriate • Ensure acquisitions comply with State privacy requirements • Facilitate resolution of OIMT and OIMT Privacy Office PII breaches and other issues outside of the program • Actively participate in progress reviews to ensure critical program information is communicated to Agency/office organizations • Facilitate resolution of program issues in agency/office organizations
OIMT Privacy Officer–Program Manager/Team Leader	• Manage the day-to-day work of the program • Provide program oversight and monitoring of agency privacy programs for compliance • Define and manage program risks • Lead, coordinate, and facilitate Program team's planning and execution of tasks and deliverables • Accountable for the success/failure of program/team tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Prepare and present program reports to appropriate levels of management • Facilitate resolution of issues and elevated risks • Manage acquisitions
OIMT Privacy Specialists	• Provide leadership, expert technical assistance and training for agency/office SMEs and Privacy Officers • Attend all scheduled meetings • Assist OIMT Privacy Officer in providing program oversight/monitoring of agency/office privacy programs for compliance • Actively participate in progress reviews to ensure critical program information is communicated to all agency/office organizations • Facilitate resolution of program issues, elevated risks, e.g., PII breach investigations, in agency/office organizations • Be accountable for the success/failure of OIMT program tasks and deliverables

Role	Responsibilities
	• Ensure appropriately skilled program participants are available when needed • Complete assigned tasks and deliverables based on agreed schedule. • Provide status updates including issues and risks • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
Agency/Office Privacy Officers–Team Leaders	• Participate in agency/office process to ensure compliance with applicable privacy requirements, e.g., preparation of PIAs, etc. • Anticipate/prepare to mitigate privacy risks within the agency/office • Present program results to senior agency/office management and others • Be accountable for the success/failure of agency/office compliance • Attend all scheduled meetings • Prepare and present agency/office reports to appropriate levels of management • Designate/train back-up personnel • Ensure appropriately skilled program participants are available when needed • Develop/issue agency/office-specific procedures for compliance, as appropriate • Investigate/report on PII breaches within the agency/office • Keep OIMT Privacy Officer informed of status/outcomes of breach investigations • Provide technical assistance/training to agency/office personnel • Ensure all employees are aware of statutory/regulatory/policy responsibilities • Complete assigned tasks and deliverables based on agreed schedule • Act as SME for appropriate organizational function • Be prepared to take some responsibility to educate others • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
OIMT Finance and Procurement Staff	• Oversee contracts • Manage task order solicitation • Administer contracts • Administer competitive procurements • Facilitate OIMT Privacy Program Procurement staff processing of acquisitions

Role	Responsibilities
Internal Stakeholders: Program Team Agency/Office Privacy Officers Agency/Office CIOs Sponsors All Other OIMT Employees **External Stakeholders:** The Public Legislature	• Understand legal, regulatory, and policy requirements for handling data as covered in HRS §487(N), HRS §487(R), and federal standards where required • Ensure compliance with privacy laws, regulations, and policies • Report potential and actual breaches to appropriate officials • Take annual privacy training • Provide feedback regarding OIMT implementation of privacy laws, regulations, and policies via audits, reports, Legislature inquiries, correspondence, appeals/litigation, etc. • Legislature amends the law and State policies to improve privacy safeguards and compliance

7.2 PROGRAM STAFFING PLAN

OIMT is investing 4.83 Full-time Equivalents (FTEs) of effort by FY-2014 via employees and contractors to complete this program's tasks and deliverables. The breakdown by organization is as follows:

Table 8: Program Staffing Plan by OIMT Entity

OIMT Entity	FTEs
Privacy Officer	1
Business Manager	0.125
Business Staff	0.25
Privacy Specialist (first/third FTE)	0.33
Privacy Specialist (FY-2014)	3
Program Total	4.83

This table shows an estimated percentage of scheduled work hours needed for the program to be successful.

Table 9: Minimum Program Staffing Plan

Resource Name or Role (if not staffed)	Minimum Needed for this program (%)	OIMT Entity
EM05+	100	Privacy Officer
	0.125	Business Manager
	0.25	Business Staff
SR-24	0.33	Privacy/508/Quality Assurance Specialist
SR-22/24	100	Privacy Specialist
SR-22/24	100	Privacy Specialist
SR-22/24	100	Privacy Specialist

7.3 CONTRACT SERVICES REQUIREMENTS

Table 10: Contractor Requirements

Role	Skills	Experience	Duration
Develop Privacy role-based training modules and no less than six workshops	Planning, developing, and presenting computer-based and classroom training	Governmental Privacy experience, CIPP/G Certification	Greater than one year
Plan, develop compliance standards, conduct compliance audits and training to meet requirements	Planning, developing privacy compliance standards, and conducting compliance audits, evaluations, etc.	Governmental Privacy experience; CIPP/G Certification	Greater than one year

7.4 STAFFING PLAN FOR ONGOING OPERATIONS

In addition to the Staffing Plan for this program, the following the organizational OIMT roles, skills, and experience will be needed to operate and maintain the resulting solution.

Table 11: Operational Support Requirements

Role	Skills	Experience
Two Privacy Specialist (FY-2014) One Privacy Specialist (FY-2015) for all skills identified	Development of policy, procedures, manuals, handbooks, and directives to large organizations on the Privacy Program (e.g., PIAs, PII, SSN Reduction, DEAR, PLMS, Breach, etc.) Provision of oversight to Privacy Program Development/Presentation of Privacy training Privacy Compliance	One year at next lower grade

8. DELIVERABLES

8. DELIVERABLES

8.1 PROGRAM DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing.

Table 12: Program Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Agency/Office Identity Theft Task Force (ITTF) Charters	Codify roles and responsibilities of task force and task force members	Each Agency/Office	OIMT Privacy Officer/ Privacy Specialists Agency/Office Managers and CISOs	OIMT Privacy Officer
Scorecards; FISMA Annual Report; assist in compliance reviews use of SSNs/PII, DEAR, CSAM, and Privacy websites; and Privacy Impact Assessments	Comply with various laws and State privacy requirements	Public, OIMT Privacy Office	OIMT Privacy Specialists Agency/Office Managers	OIMT Privacy Officer

8.2 PROGRAM MANAGEMENT DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing.

Table 13: Program Management Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Program Plan	Acquire resources required for full OIMT compliance with privacy laws and State policies	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB Budget Officers
Update OIMT Privacy Manual and Handbook (need requested FTE to complete)	Provide guidance needed to ensure OIMT compliance with privacy laws and related State policies	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
Privacy Loss Mitigation Strategy (PLMS) (need requested FTE to complete)	Provide guidance to Agencies/ offices needed to ensure appropriate OIMT response/ handling of breaches of PII	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
OIMT Identity Theft Task Force (ITTF) Charter (need requested FTE to complete)	Codify roles and responsibilities of task force and task force members	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB

Deliverable	Objective	Primary Audience	Reviewers	Approvers
OIMT Privacy Policies and Procedures (in addition to Privacy Manual and Handbook) (need requested FTE to complete)	Enable awareness of scheduled tasks	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
Role-Based Trainings & Workshops (need requested FTE to complete)	Identify strengths, areas for improvement, and recommendations	All agencies and offices	OIMT Privacy Team	OIMT Privacy Officer
Technical Evaluations (need requested FTE to complete)	Ensure compliance with privacy requirements	All agencies and offices	OIMT Privacy Team	OIMT Privacy Officer

9. PROGRAM CONTROLS

9. PROGRAM CONTROLS

9.1 SCORECARDS (QUARTERLY AND ANNUALLY)

Agency/Office Privacy Officers are responsible for preparing quarterly PIA and annual PIA/PII reports to OIMT. These reports reflect level of agency/office/OIMT compliance with specified requirements.

9.2 FISMA PRIVACY ANNUAL REPORT (ANNUAL)

Agency/Office Privacy Officers are responsible for preparing their portion of the annual reports as set forth in the privacy plan. This report reflects level of agency/office/OIMT compliance with specified requirements.

9.3 ANNUAL REVIEW OF SYSTEM OF RECORDS NOTICES AND AUTOMATIC REQUIREMENT TO WRITE PIA FOR NEW SYSTEMS WITHIN 90 DAYS

The OIMT Privacy Office conducts an annual review of SRNs, in collaboration with the Agency/Office Privacy Officers, to ensure that existing PIAs are current and that all new Privacy Act systems have PIAs and any outdated PIAs must be revised as appropriate.

9.4 REVIEW AND PROCESSING OF PRIVACY IMPACT ASSESSMENTS (PIAS) FOR ALL ELECTRONIC SYSTEMS

As part of the review process, all systems that contain PII must have PIAs written and published. This step ensures that PIAs are incorporated into the system creation process.

9.5 ANNUAL SURVEY/REVIEW FOR REDUCING USE OF SSNS AND OTHER PII IN CONDUCTING OIMT BUSINESS

The OIMT Privacy Office conducts an annual survey and review of OIMT's use of SSNs and PII in conducting business, in collaboration with the agency/office Privacy Officers. This exercise ensures that the use of SSNs and PII in conducting OIMT business is minimal so that the risk of PII loss is as low as possible.

9.6 REVIEW DEPARTMENTAL ENTERPRISE ARCHITECTURE REPOSITORY (DEAR), CYBER SECURITY ASSESSMENT MANAGEMENT (CSAM) AND PRIVACY WEBSITES FOR COMPLIANCE ANNUALLY

These program controls are not currently being implemented due to lack of sufficient program resources. Implementation of controls will begin once staffing levels are reached.

9.7 PERFORM PRIVACY TECHNICAL EVALUATIONS ANNUALLY

These program controls are not currently being implemented due to lack of sufficient program resources. Implementation of controls will begin once staffing levels are reached.

9.8 PRIVACY AND SECURITY

All program documents will be labeled Sensitive But Unclassified - For Official Use Only in the header and footer. All Certification and Accreditation (C&A) tasks and deliverables required before this program's solution can be implemented in production are part of this program.

REFERENCES

REFERENCES

Major State Privacy statutes and authorities are located at:

http://ipsc.hawaii./gov

www.capitol.hawaii.gov/hrscurrent/

OIMT's Privacy website is located at:

http://oimt.hawaii.gov

For OIMT Privacy contacts:

See the listing maintained at http://oimt.hawaii.gov.

The OIMT Privacy Manual is located at:

http://oimt.hawaii.gov/Privacy

GLOSSARY OF ACRONYMS

GLOSSARY OF ACRONYMS

For definitions of terms and acronyms used in this document, see the OIMT Nomenclature Guide.