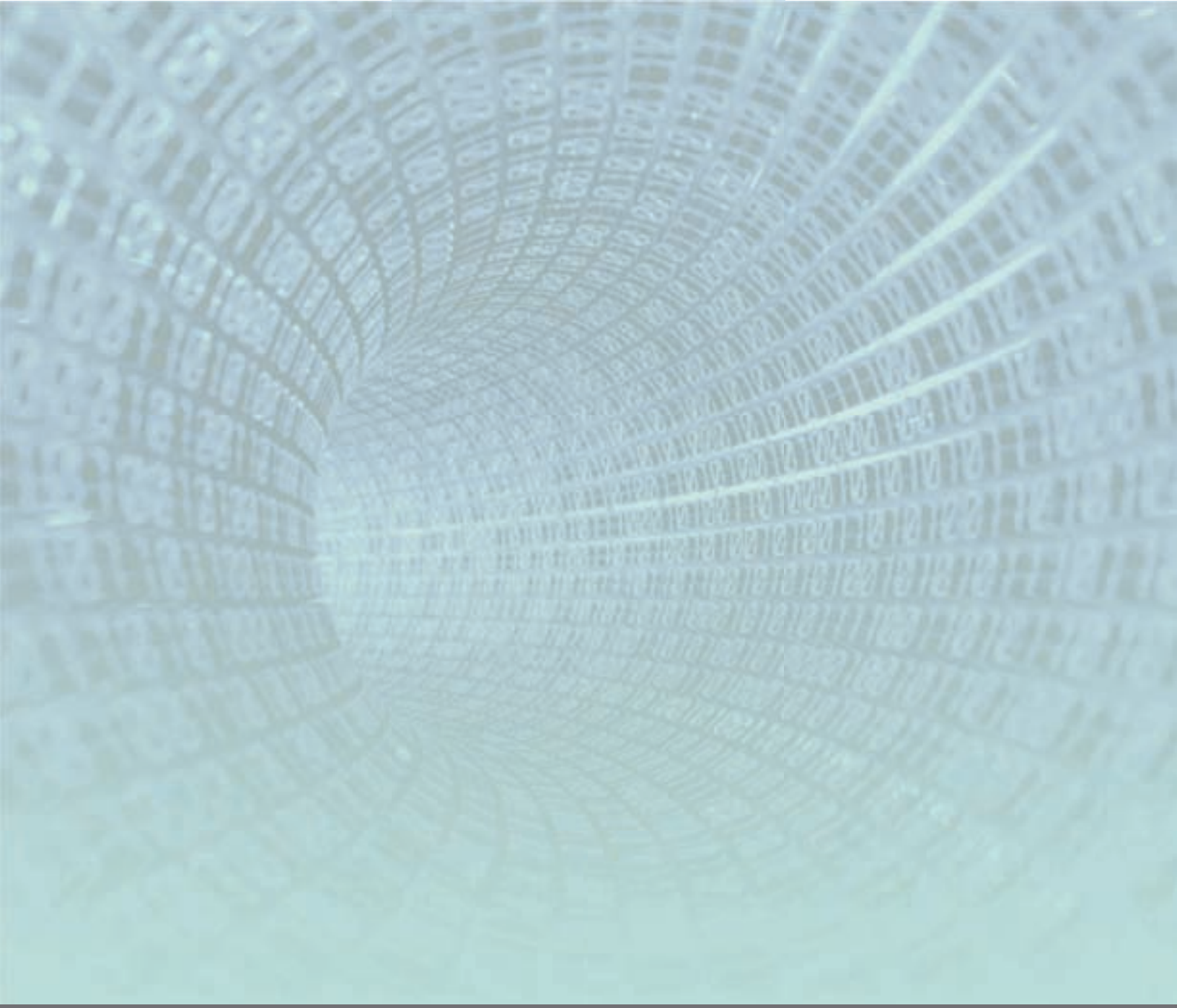
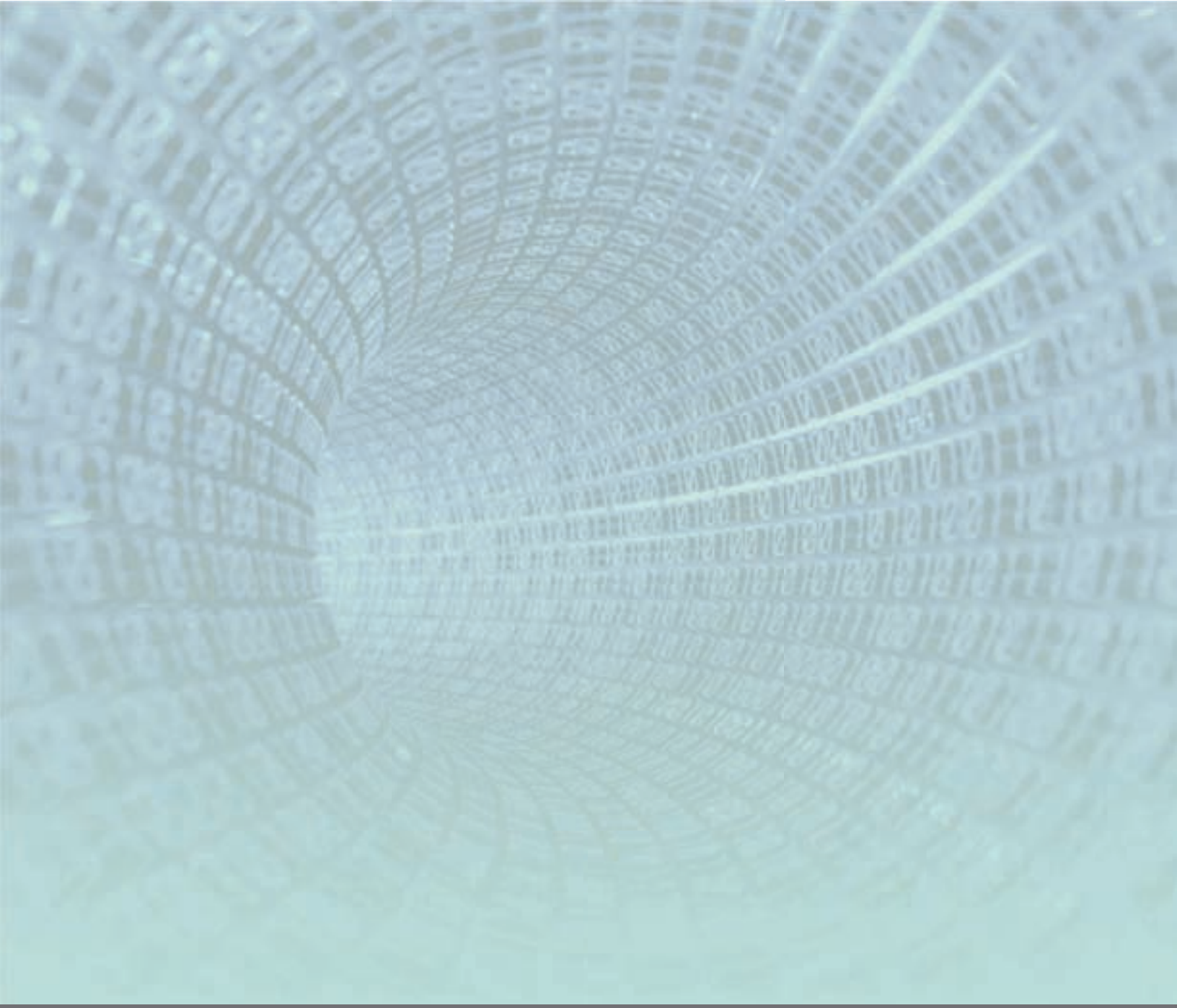


POLICY PLAN

TABLE OF CONTENTS

FIGURES

TABLES



1. EXECUTIVE SUMMARY

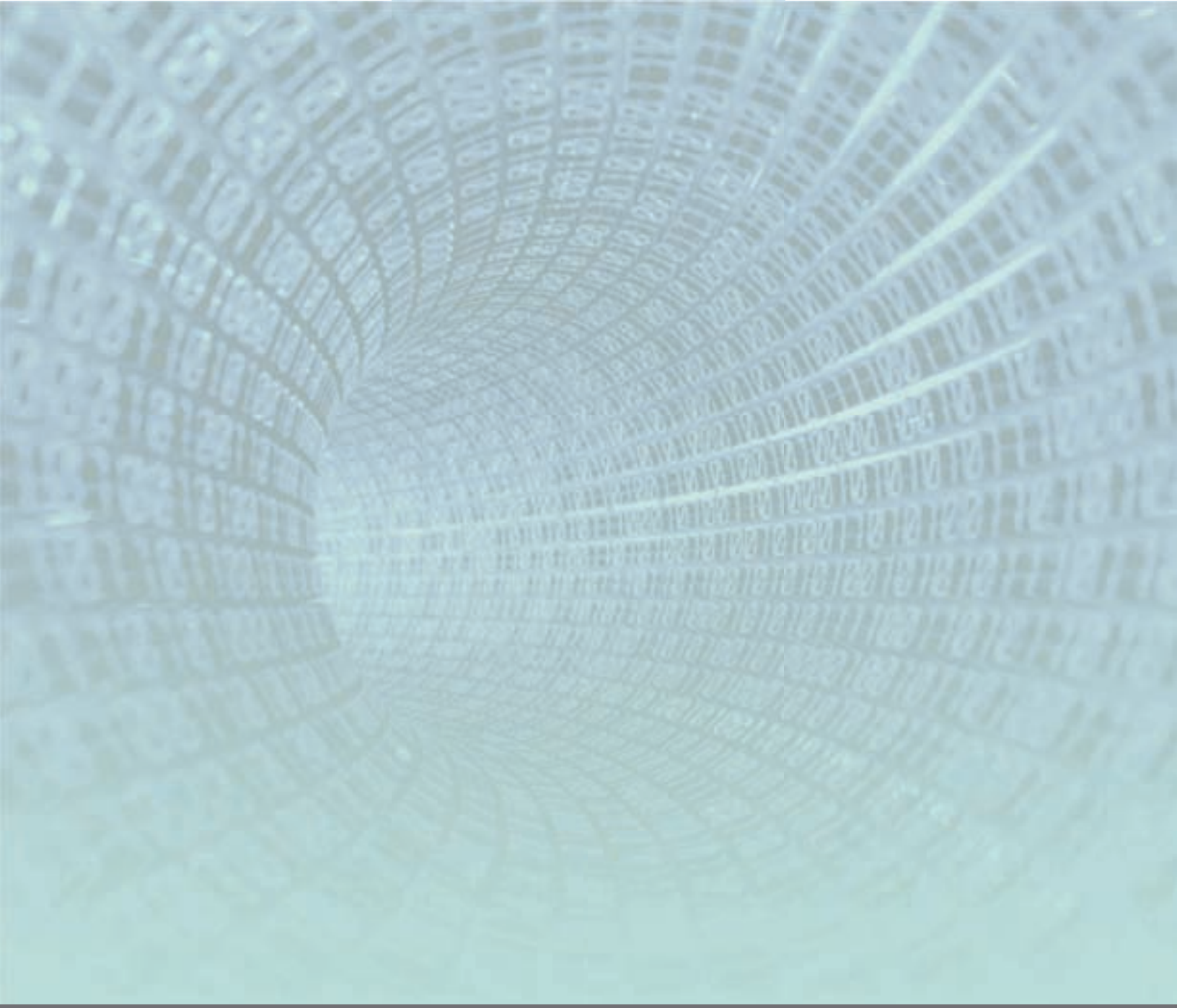
1. EXECUTIVE SUMMARY

A review of the State's fragmented Information Technology (IT) Policy Program by the Office of Information and Management Technology (OIMT) concluded that there is currently insufficient funding and staff support to meet today's policy requirements. Most agencies do not have a dedicated policy officer, nor are there consistent sets of policies used across the state.

The OIMT will soon provide governance and oversight for the IT infrastructure for a large portion of the state agencies as described in the Plan. In addition to guidance and directives regarding IT infrastructure the acting Chief Policy Officer (CPO), under the Chief Information Officer (CIO), also provides guidance, development, oversight, and assistance regarding policy.

The CPO is responsible for partnering with the Policy Working Group in formulating overarching State IT policy and overseeing agency/office implementation and achieving the State's strategic goals in support of the OIMT vision for enterprise IT policy. Policy will heavily rely on subject matter experts (SMEs) across the State as well as OIMT Working Groups to provide assistance with development and structure. Value to both the customer and the public is promoted through the use of State-approved standards, compliance requirements, and industry best practices.

It is envisioned that all enforcement and audit functionality will be defined as part of the governance development process contained in other sections of the Plan and will not be addressed in this document.



2. INTRODUCTION

2. INTRODUCTION

2.1 PURPOSE

Entities rely on policy to provide operating guidelines, and beyond that the business requires actual operating instructions. These instructions are delivered in the form of implementations of policy. It is imperative that a means of tying policy to its implementations be found, as well as measuring both policy and its implementations for effectiveness, so that the entity does not perceive its operating instructions as detached, irrelevant, contradictory, and ineffective. Policy governance ties policy and implementation formulation to measurements of usefulness to achieve better results for the State.

Policy governance, by definition, is a cyclic process that not only creates policy and its implementation but also measures policy and implementations for efficacy. It is the intention of the State of Hawai`i to provide proper attention to the measurement aspects of policy governance, ensuring its effectiveness. Furthermore, it is the objective of the State to be consistent in the mapping of policy and its implementations and enable enterprise transparency initiatives while increasing enterprise institutional knowledge. Policy governance is both applicable and needed in identity management and privacy settings.

This document will define the future requirements that will strengthen the framework on how the State develops, articulates, and implements IT policy for the Executive Branch and also defines the steps needed to build a consistent and comprehensive policy program.

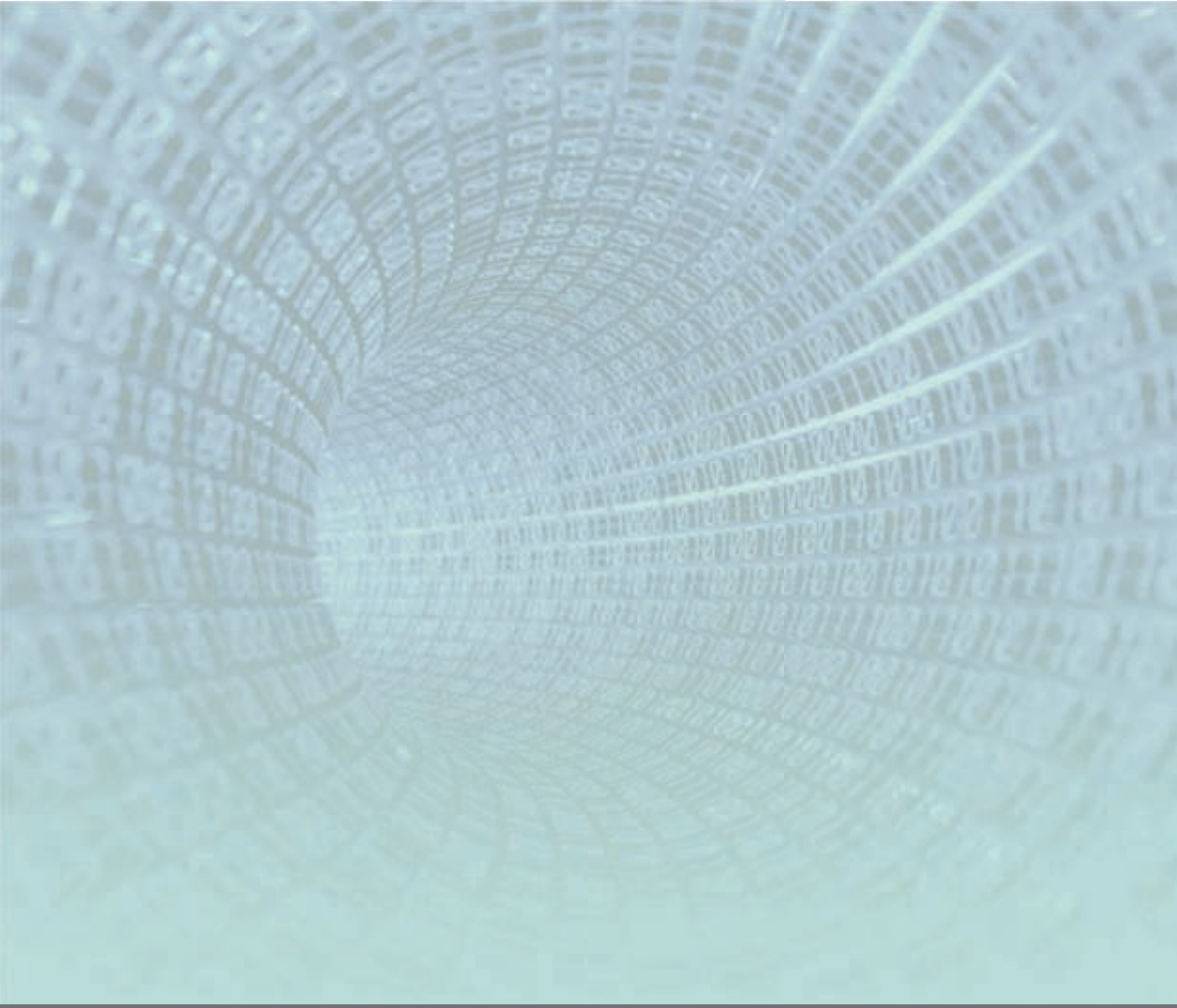
This document is a living document that will be kept current throughout the course of the program.

2.2 SCOPE

This document will define the scope and structure for the policy program for all Executive Branch agencies. In the future, this program may extend to other branches ensuring consistency of IT policies across the State.

In concert with the Policy Working Group, the Policy Specialists identified to be hired FY-2014 will accomplish the following in FY-2015:

- Better synchronization between the Policy Working Group, State Agencies, and the CIO Council (CIOC) in the development, provisioning, and implementation among the agencies in support of consistent and clear enterprise policies
- Proactive and relationship-building steps with auditing agencies
- Develop and update a policy program to educate staff on the policies and make an easily navigable web page where they can be housed to ensure both understanding and compliance
- Develop common nomenclature to be used across all policies and procedures
- Review agency/office additional requirements for accuracy and validity and incorporate them into the main policy library
- Updating of the OIMT Policy manuals and handbooks and writing new policy and templates where needed
- Provide oversight and reviews ensuring Agency Policy Officers utilize best practices and standards in their work with systems documentation, policy reporting, and other policy concerns
- Conduct policy technical evaluation and compliance reviews for agencies and offices
- Develop role-based policy training
- Develop and conduct policy workshops and policy awareness campaigns
- Creation of a centralized policy website for use across the Executive Branch
- Vigilantly keeping current with new policy 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 policy policies, initiatives, and matters
- Adoption of a very pro-active stance regarding policy guidance and implementation throughout the State to promote best practices and minimize risk while coordinating with other key programs
- Availability for providing ongoing policy subject matter expertise for the highest offices within the State, as well as increased ongoing support for Agencies including their Policy Officers
- Development of non-agency specific templates and guidelines for procedures, supply of best standards for application of policies



3. BASIC PROGRAM ELEMENTS

3. BASIC PROGRAM ELEMENTS

This section defines the mission, vision, goals, and objectives of the policy program.

3.1 MISSION

The Policy Working Group shall define and execute the process for establishing enterprise IT standards for Hawai`i State government entities. Enterprise IT standards provide several benefits to the State. These benefits include reduced costs, increased productivity, increased shared solutions, simplification of processes, and increased employee understanding and compliance. Standards may define or limit the tools, proprietary product offerings, or technical solutions which may be used, developed, or deployed by state government entities and their service providers. They may also define limitations, structure, methods, operational restrictions or processes, and obsolescence.

The policies developed will be ever-evolving—developed and maintained in such a way that they can be nimble and responsive to changes in Federal regulations and requirements as well as the requirements of Hawai`i State law.

The policies recommended and roughed by subject matter experts and the OIMT Working Groups with final development by the Policy Specialists will ensure:

- The State deploys and operates systems and technical solutions with uniformity in technology standards, process, methods, and protection of information
- The OIMT lays a solid policy framework to be used by agencies to successfully meet or exceed audit requirements
- The CIO maintains oversight in the development of the State policy structure
- That technology standards and systems reflect the collective input, technical knowledge, and programmatic expertise of State government entities
- A solid framework ensuring protection of confidential and personal information instills public confidence in government
- There is promotion of opportunities and standards for more seamless intra-agency common solutions
- A process of continuous improvement is in place and has a direct effect on the implementation of policy

3.2 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 Federal Information Security Management Act (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 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 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 expectations, and develop standardized procedures that streamline processes.

Establishment of a consistent policy governance structure is critical to streamlining policy development and implementation. Policy must also be differentiated from standards and procedures. Policy documents will contain the overarching governance concepts whereas standards and procedure documents contain the operational practices. As an example, a Password Policy defines the high level goals to build and sustain strong passwords. It would refer to a Password Standards document that defines the detailed rules and controls that make up a strong password such as password length, complexity, and history. Policy documents are intended to change less frequently than procedure documents that would be updated more frequently in response to rapid changes in technology.

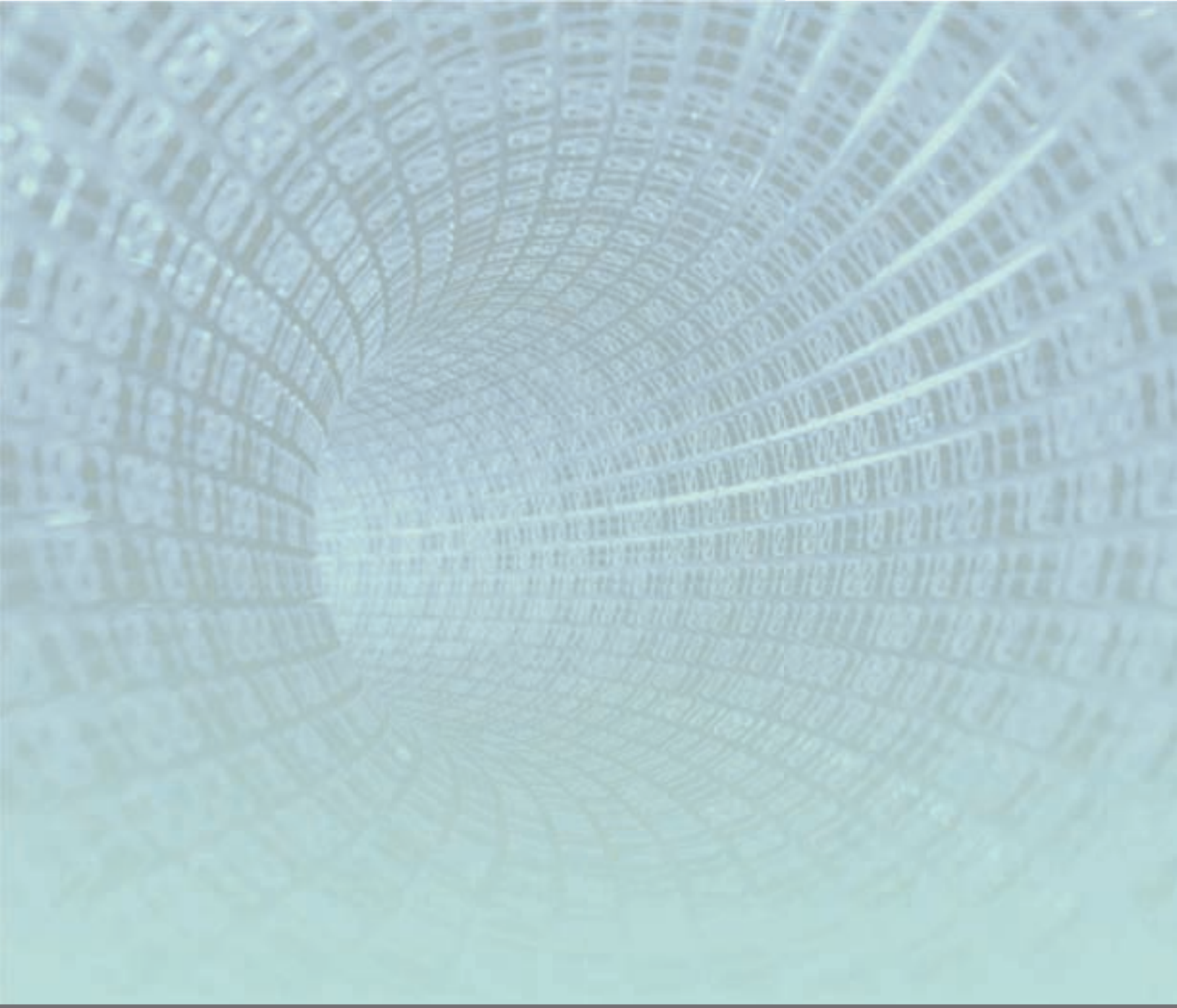
3.3 GOALS

The goal of the OIMT Policy Program is to achieve excellence in IT policy establishment and compliance. Risks of not having a comprehensive policy structure in place can result in adverse findings during a Federal audit potentially resulting in fines or the loss of federal funds. Such 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; continuity of government, and to guarantee compliance with State and Federal requirements in order to prevent funding issues, additional scrutiny, and loss of State or public confidence.

3.4 OBJECTIVES

Program staff will be utilized to provide coordination, oversight, and comprehensive policy program direction for policy matters across the Executive Branch. This will support OIMT mission goals by increasing accountability, and enhancing functional integration. This will result in increased alignment between OIMT policies across the Executive Branch with OIMT enterprise initiatives. We will also utilize program staff to assist in updating procedures and training. Staff will conduct improved oversight of the new procedures and training, which will decrease State risk and provide support in conjunction with privacy and security staff to Executive Branch agencies for successfully passing audit and swift and comprehensive resolution of any adverse policy or procedural findings. Efforts can be undertaken to promote greater policy and security awareness throughout the State.



4. PROGRAM DELIVERABLES

4. PROGRAM DELIVERABLES

This section will outline the steps that will be taken, processes to be used, documentation to be developed, and procedure that will be put in place in the delivery of the Policy Program.

4.1 FOUNDATIONAL POLICY CATEGORIES

The Policy Working Group has established the following major policy categories in which the individual specific policies will be aligned with:

- Access Control
- Configuration Management
- Contingency Planning
- Incident Response
- Media Protection
- Physical and Environmental Protection
- Security and Privacy Awareness Training
- System and Information Integrity
- System and Services Acquisition

In addition to the above, a common set of terms and definitions will be developed and used across all policies as well as a standard set of classification labels.

4.2 WRITTEN DOCUMENTS WITH VERSION CONTROL

Even though it seems apparent, nearly every security standard and framework explicitly requires information security policies to be written. Since policies define management's expectations and stated goals for protecting information, policies cannot be implied, but must be documented. Having a written policy document helps to ensure standards are clear and concise, as well as ensures consistency and fairness. A written policy is the first key control established within the international standard ISO/IEC 1-7799:2005 which is currently the globally accepted best practice standard for information security, and is essential to performing both internal and external audits as it standardizes operations for conformity.

Policy documents need to be written in plain and simple language ensuring it is easy for both IT professionals and end-users to read, understand, and comply with. Since user education and training is a key component of all information security frameworks, clear, user-oriented language is critical.

Development of a standard template and format to be used across the State is essential so that policies can be effectively managed and updated. The standard format not only imposes consistency among documents, it ensures that each document contains key components that facilitate the overall management of the information security policies, such as the owner/author, title, scope, and effective dates of the policy. Each policy shall contain the following critical elements:

Title: The name of the policy should be as specific as possible—not more than six words.

Reference number: A reference number or code to assist with filing and identification.

Summary: Including a one or two-line summary of the policy is particularly useful when an index of policies is to be posted on the intranet.

Policy objective: This states the objective of the policy. It should also briefly explain the intent, making it clear despite potential complexities of detail later in the document.

Intended audience: A brief statement of the roles and/or locations chiefly targeted by this policy.

Exceptions: A brief statement if exceptions to the policy will be allowed and for what reasons and length of time.

Policy statement: The main content of the policy. This may have several subsections. It may also include diagrams and charts to promote better understanding.

Background material and references to other documents: References to other material that is essential to understanding the policy. It is important to ensure that these references are kept up to date, particularly when the policy is on an intranet and the references are hyperlinks that may change. This also helps to avoid too much background material into the policy document itself.

Compliance statement or reference to compliance framework: Each policy should contain, or be associated with a compliance statement saying who it affects and how (compulsory, advisory, or indicative). If the compliance statement is complex or will change frequently, it should be kept separate from the policy itself for reasons of simplicity and focus.

Roles and responsibilities for the policy: This section includes the job titles, names, and contact details of the people or group who have specific roles within the policy (for example, the people who have data protection and data privacy responsibilities).

Contact names for further information: This may be the author of the policy or others who can give explanations or guidance on what it means or how to apply it.

Policy dates, version number and change history: This includes

the date the policy was approved and issued. It may include the date it comes into force if different from the issue date. There may also be an expiry date if the policy is intended to be of finite duration (for example, a special limit on hardware purchase while changing suppliers). Include a change history with dates and references to previous versions. Not only is this helpful for understanding what policy was in force at some specific time in the past, but it may be essential for legal or regulatory reasons to maintain such an audit trail. It must include a version number, following the enterprise standard.

Review timetable: This says when and by whom the policy will be reviewed or if the policy will remain in force without time limit and without review.

Policy owner: This is the job title, name, and contact details of the person or group responsible for the implementation and enforcement of the policy.

Change authority: This includes the job title, name and contact details of the person or group who has authority to change the policy or give exception waivers to it. If appropriate, also include a summary of the process for requesting and authorizing changes

References: Optionally, include references to related documents (as paper documents or hyperlinks) both internally and externally (for example, to ISO, NIST, COBIT, or ITIL documents).

4.3 DEFINED MANAGEMENT STRUCTURE

To help keep IT policies understandable and manageable, it is important to keep the information level steady among the various document types. In other words, it is not advisable to mix policies, procedures, standards, and guidelines into policy documents.

A policy governance structure will be developed which breaks information into separate documents for policies, standards, and procedures. For example, a Password Policy would state the high-level organizational goals to build and sustain strong passwords. It can refer to a Password Standard document, which defines the detailed controls that make up strong passwords, such as password length, complexity, and history. Keeping these structural elements separate will allow updating of standards and procedures as new technologies or processes are introduced, while updating higher-level policy documents less frequently.

Documents will be placed into groups based on subject matter. Since many agencies are subject to Federal audits as a requirement of them receiving federal program funds, the choice has been made to structure policy elements under the NIST/FISMA control numbers. This same structure will be used in the organizing of documents on the OIMT Web Portal.

The Policy Working Group is a standing investigative group that will act as an ongoing advisory body to the policy staff as well as to take input from the CIOC and other councils and boards. They will assist in the development and final editing of policy, ensuring that input from agencies and SMEs is incorporated as needed.

4.4 TARGET USER GROUPS

Not all IT policies are suitable for every role in the state. Therefore, written IT policy documents will be based on the lowest common need as an example defined by NIST or FISMA concepts. Some agencies (such as Health, Labor, Tax, and Welfare) will be able to add appendices specific to their agencies to strengthen policy where required, with those added requirements being applicable to their staff or those in possession of their data or access to their systems.

For example, all users might need to review and acknowledge Internet Acceptable Use policies. However, perhaps only a subset of users would be required to read and acknowledge a Mobile Computing Policy that defines the obligatory controls for working at home or on the road. It is felt that most employees are already faced with information overload, so the goal is to organize the framework in such a way where it is easy for staff to determine what is applicable to them.

4.5 POLICY COMMUNICATIONS AND EDUCATION PLAN

Communications will follow the Communications Strategy outlined in the Governance section of the Plan. For policy communications, the following would be emphasized:

- The policy framework
- How the specific policy fits in to the framework
- If the policy has been revised, a simple way to tell what has been changed
- Clear definition of individual responsibilities as a result of the policy
- A method for simply and easily providing feedback

4.6 VERIFIED AUDIT TRAIL

Policy documents will not be effective unless they are read and understood by all members of the target audience. It is envisioned that a working group specializing in training will develop an overall IT education program that will assist in this process.

A deliverable of the Policy Team with assistance from the other working groups will be defining a proposed audit mechanism which will indicate that users have read and acknowledged specific versions of policy documents, including the date of acknowledgement with our goal to be able to verify that each person handling information within our organization has read and understood the IT policies that apply to them.

4.7 WRITTEN EXCEPTION PROCESS

It may be impossible for every part of an agency to completely follow all of the IT policies at all times due to funding constraints or other circumstance. Rather than assuming there will be no exceptions to policy, a documented process for requesting and approving exceptions to policy and clearly documenting the associated risks will be developed. Written exception requests will require the approval of senior management within the organization and also at OIMT, and have a defined time frame after which the exceptions will be reviewed again.

Policy exceptions will be managed within the same framework as the policy documents themselves. In other words, exception will be documented, have a clear owner, and can be organized by topic area.

4.8 ENVISIONED PROCESS

The process of operationalizing privacy is analogous to the enterprise policy governance in which policies are formulated, implemented, measured, and then refined and re-implemented. Although the previous statement is recognizable as a governance process (specifically a Boyd cycle), there are common behaviors that prevent this process from being continuous and thus prevent it from becoming a true governance process.

It is to be understood that policy revision and creation stem largely from influencing factors including, but not limited to: business initiatives, emerging technologies, paradigm shifts, and mandated governmental changes. It is also important to recognize that in some cases the State may need to act quickly to create or revise items within the governance framework to facilitate and expedite the process of compliance.

Ideally, the goal is that the framework that is constructed for enterprise policy governance processes follows the flow illustrated in Figure 1 and reflects the anticipated regular methodology for new IT policy development. OIMT and the CIO may abbreviate and/or expedite the process when operationally required.

Initiation: At the Information Technology Steering Committee (ITSC), the CIO will table the goal and objective for proposed new IT policies and recommended updates to existing policies or additions. Subject matter experts or OIMT Working Groups may also submit changes for consideration to the policy team.

Initial Draft: The designated individual/group will conduct sufficient research and consultation with stakeholders and technical experts to craft an initial draft and suggest a classification as IT policy, standard, or guideline. The CIO will table the initial draft for review and comment by the ITSC, prior to publishing and circulating to the State at large.

Circulation and Comment: Subsequent to comments and recommended revisions to the initial draft, the draft document will be circulated among a larger group comprised of selected

Figure 1: Policy Governance Process

individuals in the affected units/departments/communities. Comments are to be returned to the development team for review within the specified deadline.

Refinement: Based on comments gained during the circulation phase, modifications will be made to the policy. If significant or potentially controversial changes are made, another round of circulation and comment will occur. Further development of this process will further define when another round of circulation and comment is needed.

Final Draft: The CIO will liaise with affected stakeholders and the community at large as necessary and prior to submission of a final draft to the leadership of the affected unit/department/community for information and comment. Final drafts will be posted for information on the CIO's web site. Final drafts will include clear accountabilities, monitoring provisions, and any required reporting for compliance. A suggested timeline for review/updating will be included.

Approval: The finalized document will be submitted for approval. Following approval, the document will be posted on the CIO's website and clearly show the date it will become active.

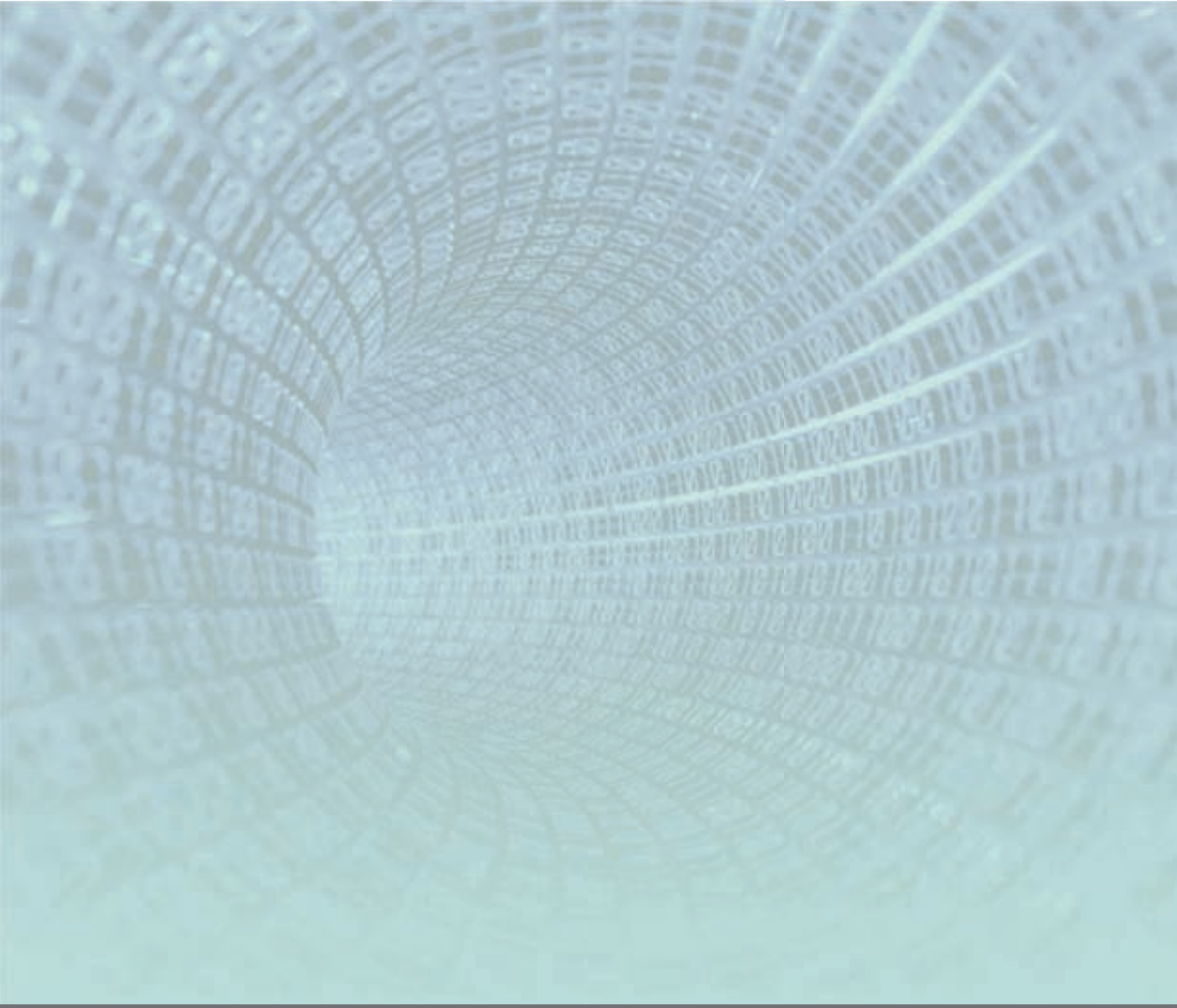
Communications: The policy will be suitably advertised/promoted ensuring affected staff is informed of and understands the policy. Multiple communication methods should be considered when promulgating any new or revised policy. Communications should include written notification (email, websites, paper memos, etc.) and face-to-face meetings of constituency groups to allow for clarification and responses to any questions. As an example, policies affecting personnel officers would be presented at meetings of personnel officers.

Implementation: A policy will become effective on the date stated in the policy document. The date shall allow at least thirty days for communication to staff and allow for any temporary exemptions to be applied for and vetted for approval or denial.

Periodic Review: Each policy should be reviewed at least bi-annually to ensure that it is still relevant with current technology, follows established best practices, and is compliant with audit requirements. Review may also take place as part of an agency Federal audit ensuring compliance.

Training: As each new policy is approved or existing one revised, each agency will be encouraged to participate in a training process that ensures that the policy is properly understood and adequately followed by procedures and guidelines, while expediting the targeted compliance.

The Continuous Improvement process will be employed as defined in the Service Management section of the Plan as elements of the policy development and review cycles.



5. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

5. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

5.1 POLICY PROGRAM MILESTONES (NON-STAFFING)

Table 1: Milestones (Non-staffing)

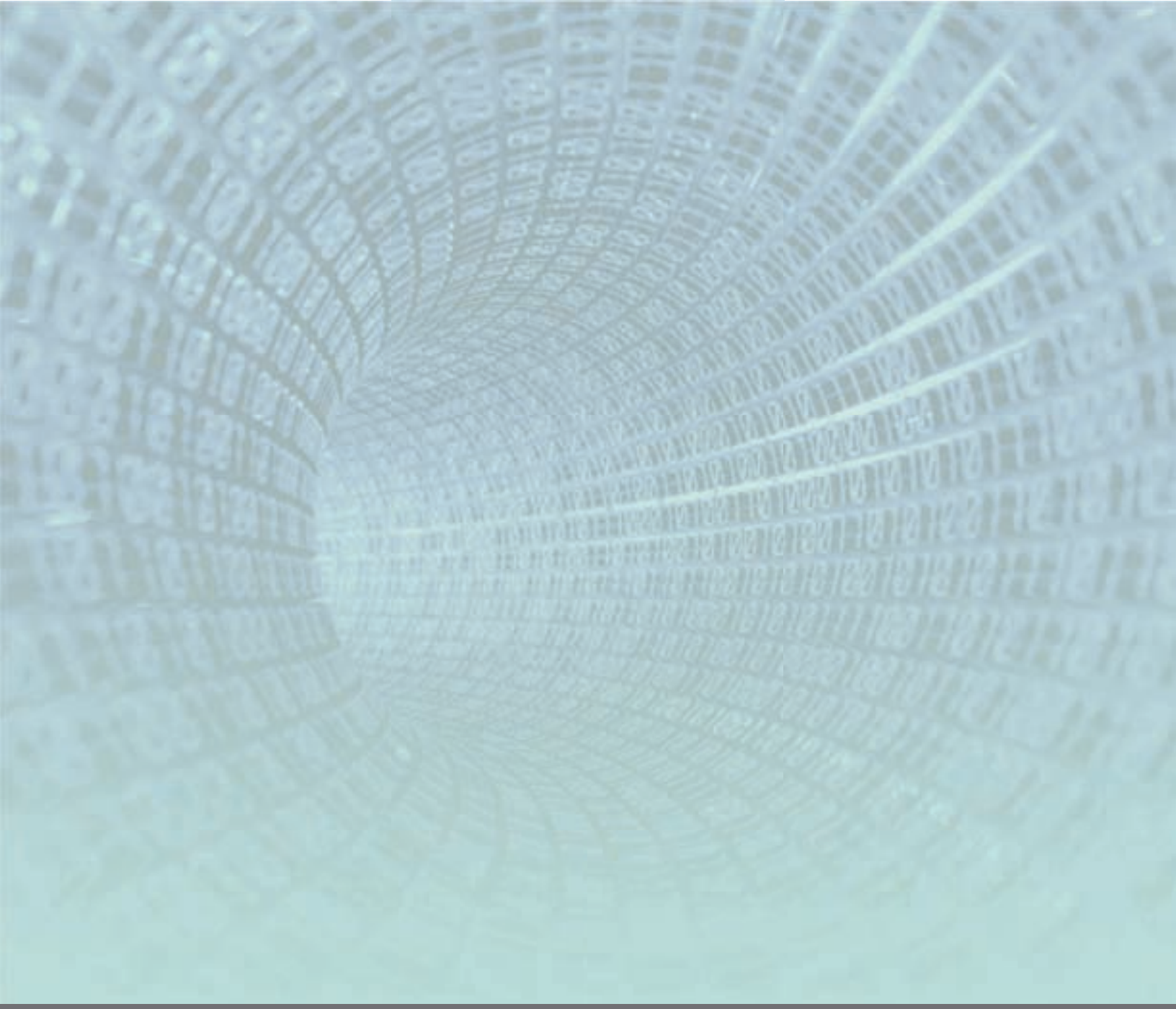
Milestones	Person or Team Responsible	Planned Completion Date
OIMT Directive on Administration Policy	Policy Officer, Information Management Chief, OIMT	FY-2015 (need FTE on board)
Complete and deploy Executive Branch policy website	Policy Officer	FY-2015 (need FTE on board)
Employee awareness and outreach to Agencies/Offices	Policy Officer	FY-2015 (need FTE on board)
Monitoring/oversight of Agency/Office Policy implementation	Departmental Policy Officers	FY-2015 (need FTE on board)
Update OIMT Policy Sections	Policy Officer and Policy Working Group	FY-2015 (need FTE on board)
Definition of training program requirements for all staff	Policy Officer and Policy Working Group	FY-2015 (need FTE on board)

5.2 POLICY 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 PD	Privacy Officer	
Classify PD	OIMT HR	
Advertise vacancies (open continuously)	OIMT HR, OIMT Business Manager	
Pull first set of applicants (SR-24/26)	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 (if needed)	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 (if needed)	OIMT Business Manager, Privacy Officer	

Milestones	Person or Team Responsible	Planned Completion Date
Make first and second offers	OIMT HR	
Meet with Human Resources	Privacy Officer	
Hire first and second applicants (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 Division Chief, OIMT HR	



6. COSTS

6. COSTS

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

Table 3: Annual FY-2013 Estimated 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)
Personal Costs:		
Ongoing FTE expenses for two SR-26 Policy Specialists	Pending Review	Estimate of salaries
Travel:		
Travel to agency locations for Policy Compliance and training	Pending Review	Based on contractual expenses for no less than four trips/annually (includes transporting supporting documentation)
Training:		
Technical writing or focus area training	Pending Review	Based on estimates provided by previous procurement and contracts
Equipment:		
Scanners, printers, laptops, docking stations, monitors, projector, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Supplies/Printing/Minor Misc. Contracts:		
Print pamphlets, supplies, and minor contracts for updating CBTs	Pending Review	Based on estimates from OIMT, current supply expenditures, and policy pamphlets.
Total	**Pending Review**	

Note: Conferences are currently not included in these estimates. It is anticipated that SMEs will bring back injects to the policy team when they attend training or conferences as part of the continuous improvement cycle.

6.2 CRITICAL SUCCESS FACTORS

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

- Timely commitment of funds and processing of required acquisitions
- Hiring and 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
- Active agency participation on the Policy Working Group
- Active policy development participation by the OIMT Working Groups and SMEs

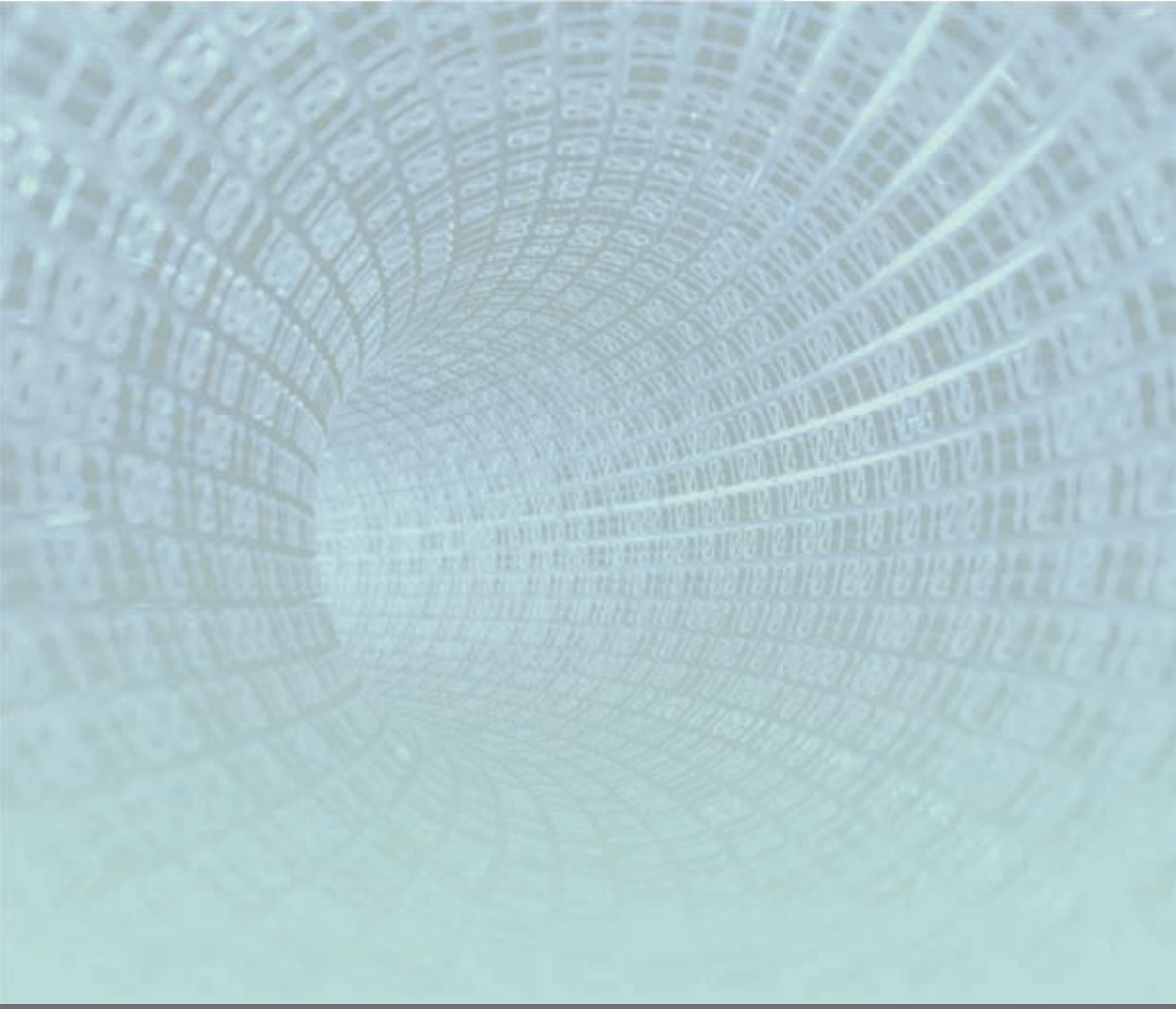
6.3 ASSUMPTIONS

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

Training tools and methodology will be developed and implemented by one of the other working groups that can implement the training needs developed.

6.4 TECHNICAL CONSTRAINTS

The Policy Program will need new and more sophisticated tools than the state currently has to more effectively track, monitor, and analyze the outputs and performance of the program. It will be necessary to have these tools to better determine and analyze quantitative and qualitative measures for the effectiveness and overall performance of policy compliance and quality at the Department. To have this evaluative capability, there will need to be new metrics, analytics, and measures for policy compliance and for policy violations, and tools to assist in investigation of policy 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.



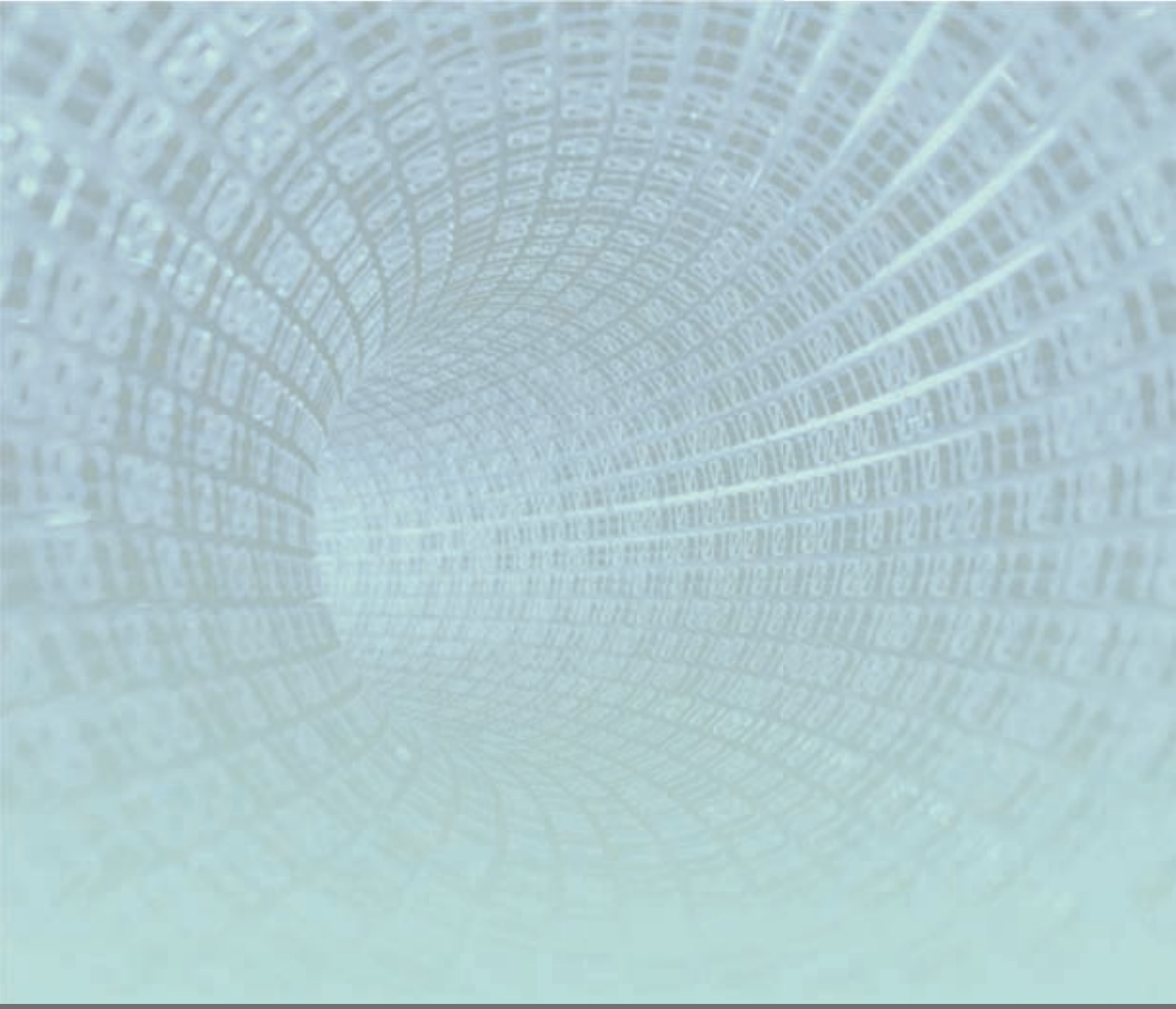
7. RISKS

7. 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 Policy Program Risk Register.

Table 4: 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	There are only two OIMT staff members with this function. Management will need to act as the backup.
2	Contracting delays for procurements may delay program or increase costs	4	4	Extend the Program schedule, as necessary, and keep the CIO and OIMT Business Manager informed of anticipated cost issues
3	Contradictory policies across the Executive Branch	4	3	Policies will need to be combined to ensure a single policy is in effect.
4	Staff knowledge of the policy in effect	5	5	Training and awareness programs must be put in place as well as an easy navigable website and log-in banners.
5	Training of staff ensuring new policies are well understood	5	5	A working group should be formed focusing on how an IT training program can be put in place and the costs of the equipment, software, and consultants required.
6	Operational procedures and processes are developed and documented by the SMEs and technical team members once policies are developed	3	5	Assistance will be provided by the two policy specialists to guide the development of the documents and to tie them back into the main policy framework.



8. RESOURCE REQUIREMENTS

8. RESOURCE REQUIREMENTS

8.1 FY-2014 TEAM STRUCTURE (NOTIONAL)

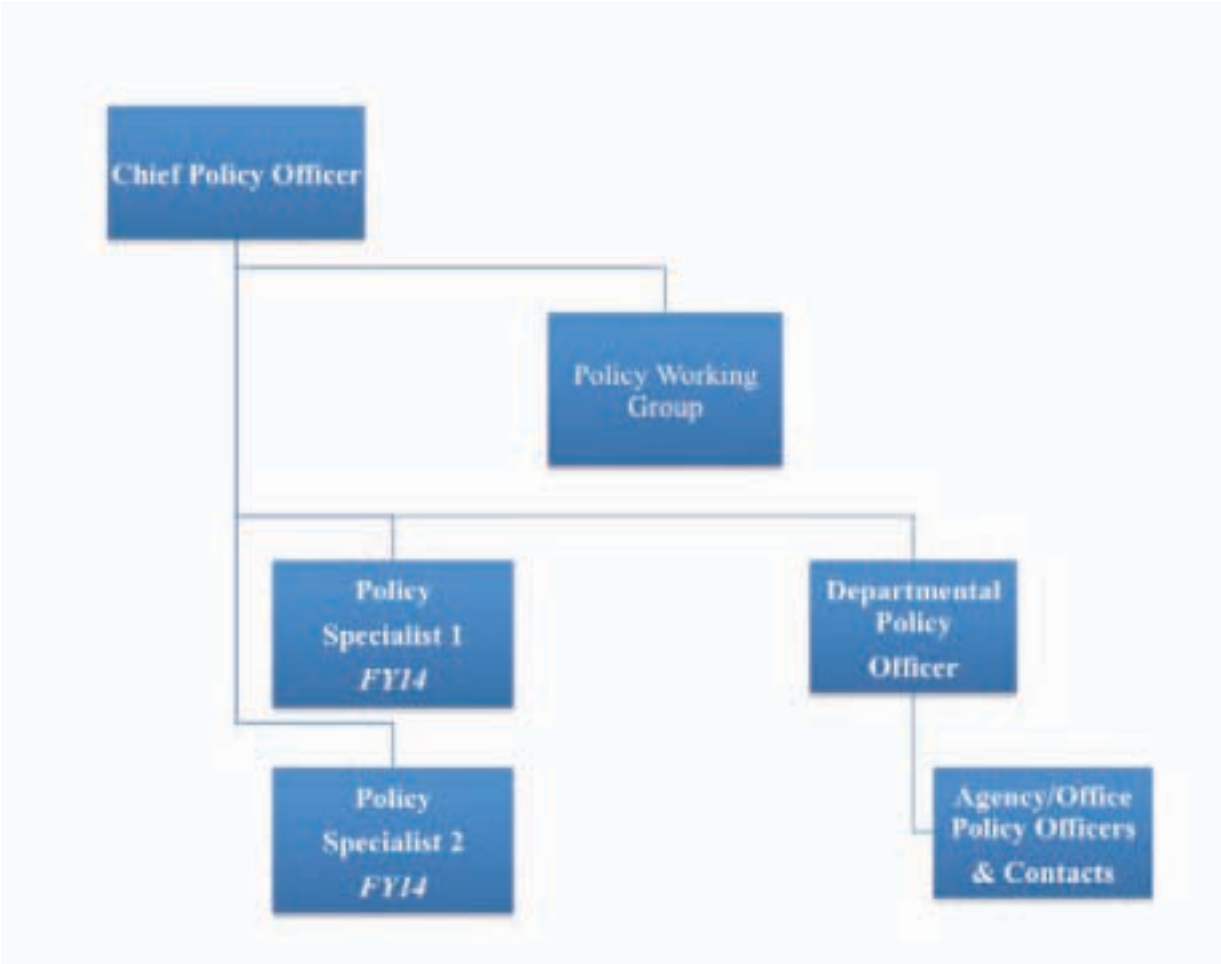
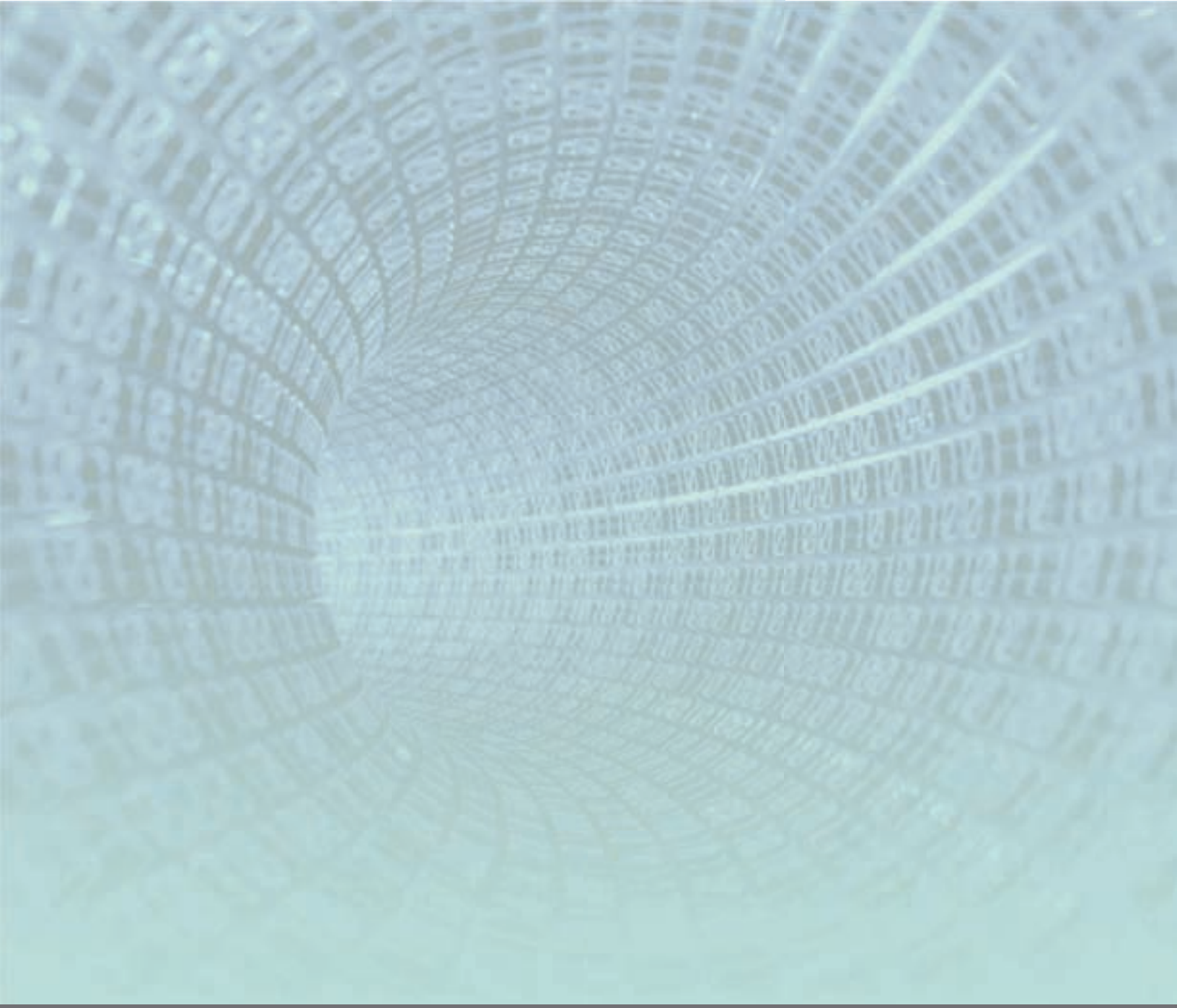


Figure 2: Policy Program Team Organization FY-2014



9. ROLES, RESPONSIBILITIES, AND STAFFING

9. ROLES, RESPONSIBILITIES, AND STAFFING

9.1 ROLES AND RESPONSIBILITIES

Table 5: Roles and Responsibilities

Role	Responsibilities
Sponsor(s): Senior Agency Official for Policy/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 policy laws and policies • Be accountable for the success of agency/office compliance • Ensure acquisitions comply with State policy requirements • 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 Policy Officer–Program Manager/Team Leader	• Manage the day-to-day work of the program • Provide program oversight and monitoring of agency policy 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 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 • Chair the OIMT Policy Working Group
OIMT Policy Specialist	• Provide leadership, expert technical assistance and training for agency/office SMEs and Policy Officers • Attend all scheduled meetings • Assist OIMT Policy Officer in providing program oversight/monitoring of Agency/office policy programs for compliance • Actively participate in progress reviews to ensure critical program information is communicated to all agency/office organizations • Develop and maintain a website containing all policies • Develop communications plan to educate staff of policies and changes • Be accountable for the success/failure of OIMT program tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Complete assigned tasks and deliverables based on agreed schedule.

Role	Responsibilities
	• Provide status updates including issues and risks • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
Agency/Office Policy Officers–Team Leaders	• Participate in agency/office process to ensure compliance with applicable policy requirements. • Present program results to senior agency/office management and others • Be accountable for the success 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 • 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 Policy Program Procurement staff processing of acquisitions
Internal Stakeholders: Program Team Agency/Office Policy Officers Agency/Office CIOs Sponsors All Other OIMT Employees	• Ensure compliance with policy laws, regulations, and policies • Report potential and actual breaches to appropriate officials • Take annual policy training • Provide feedback regarding OIMT implementation of policy laws, regulations and policies via audits, reports, Legislature inquiries, correspondence, appeals/litigation, etc.

9.2 PROGRAM STAFFING PLAN

OIMT is investing 1.5 Full-time Equivalents (FTEs) of effort by FY- 14 via employees and contractors to complete this program's tasks and deliverables. The breakdown by organization is as follows:

Table 6: Program Staffing Plan by OIMT Entity

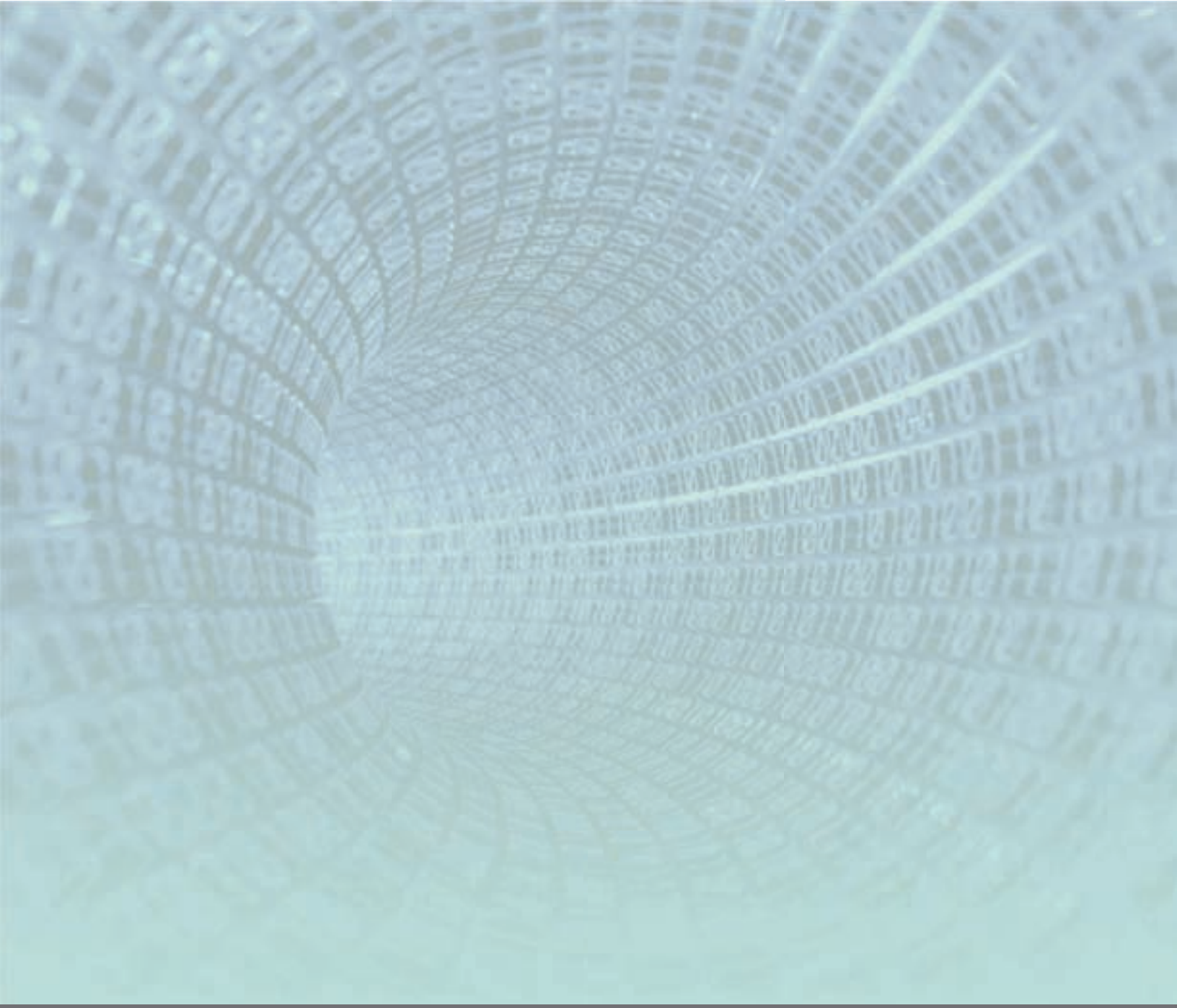
OIMT Entity	FTEs
Policy Officer	0.25
Other OIMT Staff	0.25
SMEs and OIMT WGs	1
Policy Specialist (second in FY-2014)	2
Program Total	3.5

Table 7 shows an estimated percentage of scheduled work hours need for the program to be successful.

Table 7: Minimum Program Staffing Plan

Resource Name or Role (if not staffed)	Minimum Needed for this Program (%)	OIMT Entity
EM05	0.25	Policy Officer
Other OIMT Staff assistance	0.25	
SR-24/26	2	Policy Specialist

Note that this does not take into account hours required within an agency or hours required for a successful Policy Working Group which the agencies participate in.



10. DELIVERABLES

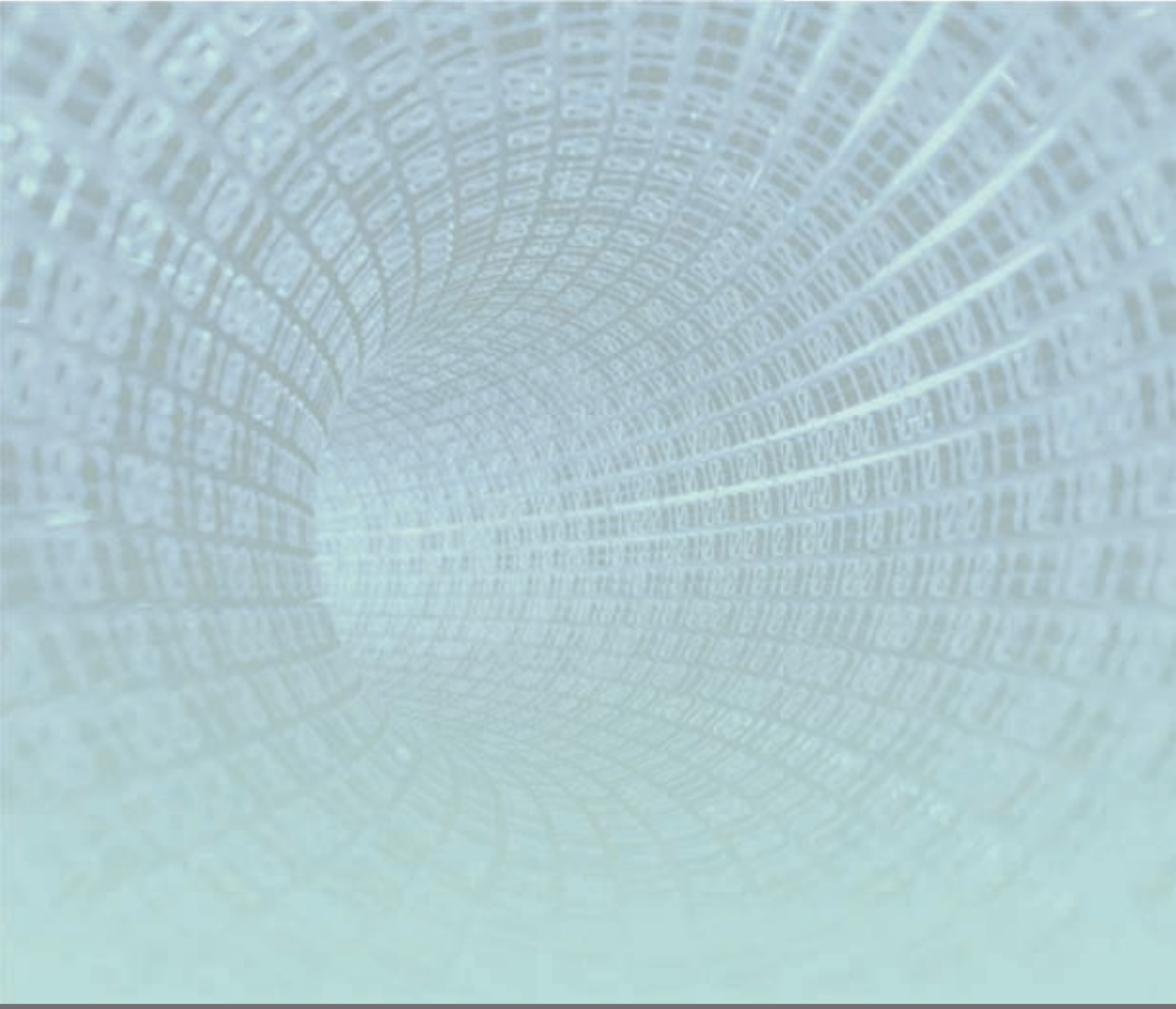
10. DELIVERABLES

10.1 PROGRAM DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing requirements. Governance over policy implementation and verification will be overseen by the Governance team, and thus is not included in this document.

Table 8: Program Management Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Program Plan	Acquire resources required for full OIMT compliance with policy laws and State policies	All agencies and offices	OIMT Policy Officer, CIO, Policy WG	CIO, Budget Officers
Update OIMT Policy set (need requested FTE to complete)	Provide guidance needed to ensure OIMT compliance with policy laws and related State policies	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
OIMT Policy Policies and Procedures (in addition to Policy Manual and Handbook) (need requested FTE to complete)	Enable awareness of scheduled tasks	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
Role-based Trainings and Workshops (need requested FTE to complete)	Identify strengths, areas for improvement, and recommendations	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
Technical Evaluations (need requested FTE to complete)	Ensure compliance with policy requirements	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO



11. PROGRAM CONTROLS

11.1 POLICY AND SECURITY

All program sensitive 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.

12. 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 by SAIC
- Internal Revenue Service Publication 1075
- National Institute of Standards Special Publications (800 Series)

13. WORKS CITED

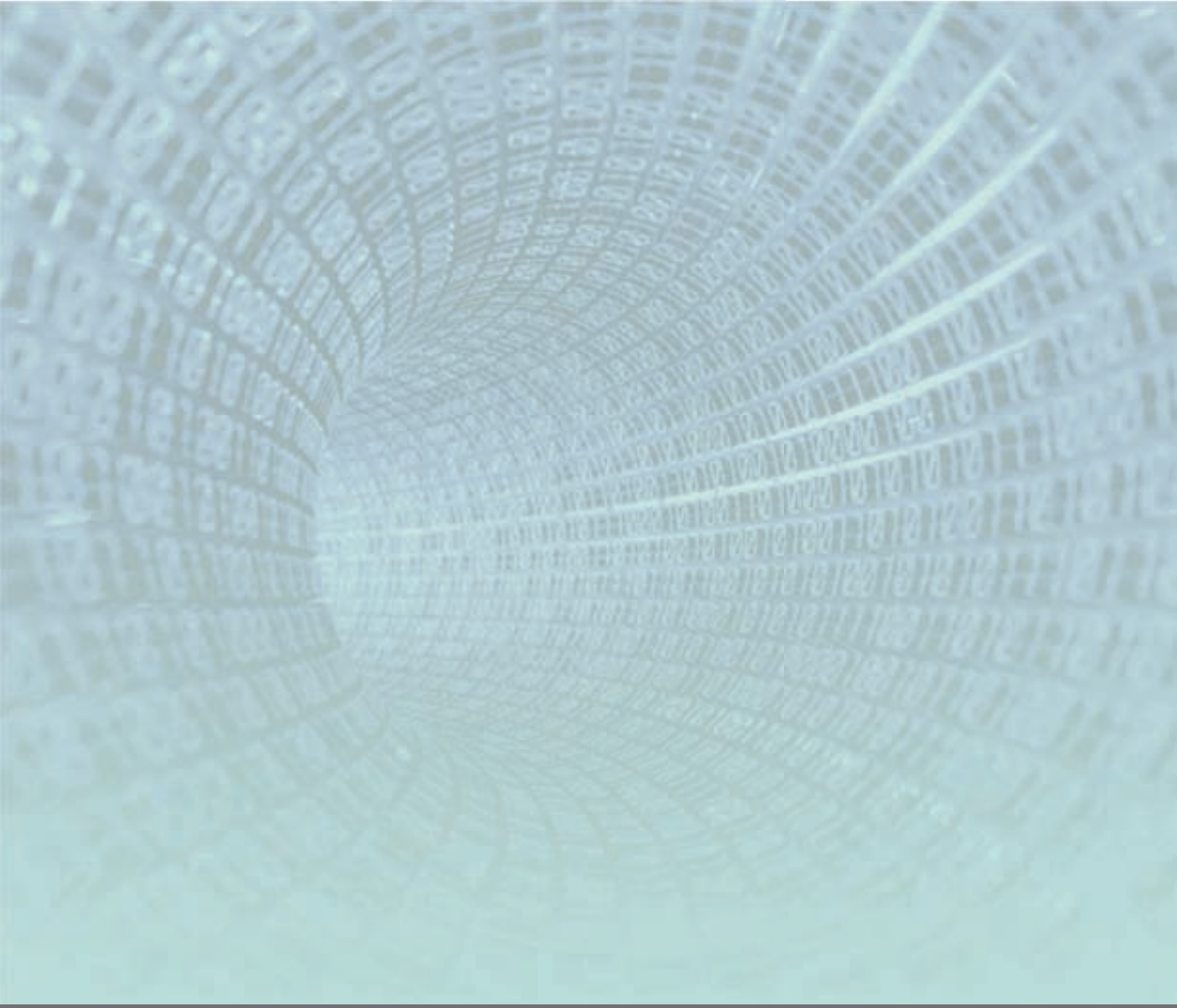
Gartner, Governance Processes to Support Effective Implementations of Policy. 2010.

14. REFERENCES

OIMT's Policy website is located at: http://oimt/higov.net

15. GLOSSARY OF ACRONYMS

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



APPENDIX A: CROSSWALK OF POLICIES

APPENDIX A: CROSSWALK OF POLICIES

The Tables that follow illustrate existing policies that were collected from State agencies and aligned into the new Policy Framework as devised by OIMT and the Policy Working Group. Policy will be developed for each on the coverage areas noted in the first column, incorporating existing Agency policy then aligning and incorporating established and proven Federal Policy or other best practices.

POLICY & PROCEDURE CROSSWALK

Key: Collateral exists | Good collateral example | P Procedure | O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH	Laws	Notes	Other State Collateral
RECORDS MANAGEMENT																		
Records Management Policy								P								Act 137	DCCA's Office of Information Practice's Records Reporting System	
Records Management Retention Schedule				O				P								487R	DAGS general record schedules (http://dlnri.higov.net/intranet/Documents/IT/Policies/GRS%202002%20-%20revised%205-06.pdf & http://dlnri.higov.net/intranet/Documents/IT/Policies/Comp%20Cir%202001-02.pdf)	
Digital/Paperless Environment																		
ACCESS																		
General				O													MFP_Security_FINAL.pdf	
Remote				O													HCJDC Remote Access Agreement	
Wireless				O													Wireless LAN Security Policy (authorized use/security)	
Revoking Privileges After Termination				O														
Consultant and Contractor Access																		
Policy for Interfacing with non State of Hawaii Entities (DOH)																		
Publicly Accessible Systems Policy																		Maryland
ACCEPTABLE USE																		
Acceptable Use				O													DHR Acknowledgement Form; ICSD Smartphone Agreement	Maryland (E Comm); New York
User-owned Device Mgmt																		
Use of State Telephones																		Ohio
Loss of physical asset																		
SECURITY																		
General Security																	UH Sys Admin rules (good); HCJDC LAN Workstation and Server Policy; CJIS Security Policy; Maryland Agency Self-Evaluation Tool; DHS Cyber Security Evaluation Tool	
Security Incident Management		P														487N, Act 10	ICSD Incident Response Cklist	

POLICY & PROCEDURE CROSSWALK

Key: Collateral exists | Good collateral example
P Procedure | O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCDC	DAGS	IPSC	Privacy	PID	UH			
Security Training and Awareness																	CSEA Policy on Employee Orientation	
Security Testing Policy																		
Password Policy and Guidance				O														Maryland
Physical Security				O														
Personal Identification Information (PII)								P				O				Act 10, Acts 135 - 137, 139 of 2006, HRS 487N, 487J and 487R (7/1/07)	Best practice from IPSC; UH General Confidentiality Notice (agreement)	
Classification																		Maryland (Standards for Security Categorization of Information Systems)
Screen Procedure																		
User-owned Device Mgmt																		
Risk Assessment		P																
HIPAA																		Connecticut
Certification and Accreditation																		
Internet Privacy Policy																		New York
Digital Signature Policy																		New York
Virus Software Policy				O														
Hard Drive Encryption Policy																		
SOCIAL MEDIA																		
Social Media Policy				O													DAGS April 2009 Cyber Security Tips Newsletter (http://hawaii.gov/dags/icsd/cst/newsletters/2009/april_social_networking); SOH Social Networking Policy.pdf; New York Social Media Legal Guidance Toolkit; New York Social Media Tutorial	Maine; New York
EMAIL/INTERNET/MOBILE																		
Email Usage				O		P												

POLICY & PROCEDURE CROSSWALK

Key: Collateral exists | Good collateral example | P Procedure | O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Homeland	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPAC	Private	PSD	UH			
Wireless Email				O													Wireless policy (address rogue access points and endure agencies have deployed full wireless solutions which meet security req'ts and monitoring for unauthorized access)	
Web site Mgmt																	EM 00-03, State Agency Website Common Template; need State Agency Website Deployment Policy (format, URL structure, domain names, advertisements, endorsements, etc.)	Connecticut; West Virginia
Wireless Communication																		Maryland
Electronic Communications																		Maryland
eCommerce Policy																		
Mobile Device Policy																Act 10	HCJDC Mobile Device Use Agreement; ICSD Smartphone Agreement	Maryland
Interfacing with non State Entities																		
Instant Messaging																		
SOFTWARE/HARDWARE																		
Development																		
Application Development																	ICSD System Requirements for Computer Application Systems; ICSD Standard Systems Development Methodology (SSDM)	
Database Development																	ICSD Database/Data Dictionary Overview (includes System Development Checklist for DB tasks)	
Change Management																		
Twgis																		
VM																	Cloud/Virtualization Policy	
Configuration Management																		
Software Maintenance				O														California 4846 (legally procured & used in compliance with licenses, copyright laws, etc., inventory, etc.)
OS																		
Power Management Policy				O														California 4819.31.13

POLICY & PROCEDURE CROSSWALK

Key: Collateral exists; Good collateral example; P Procedure; O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	SLC Hawaii Is	CSEA	DICCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCDC	DAGS	DPSC	Privacy	PSD	UH			
Hardware																		
Network																	ICSD 8.04 Network Security	
Monitoring																		
OUTAGE MANAGEMENT																		
Outage																	Centralized Support Priority Support Policy (DLIR)	
PROPERTY CONTROL																		
State IT Property Control				O														Connecticut
Inventory Policy																	DLIR uses a $600 inventory tool	
Disposal of IT Equipment				O														Ohio
CBA/ROI/Feasibility Planning																		California 4819.35
Cost Threshold																		California 4819.39
IT Equipment Depreciation																		
System Inventory and Modernization																		
POLICY DEVELOPMENT																		
Procedure and Process for Creating, Reviewing and Approving IT Policies, Procedures, and Guidelines																	Guidelines for Writing Standards http://hawaii.gov/dags/icsd/standards/pdf_standards/ITS_0101.pdf; DAGS Policy Exception Request Form	
Exception Management																		
Definitions																		California 4819.2
PROJECT MANAGEMENT																		
Project Management Policy																		Connecticut
PROCUREMENT																		
IT Procurement (including Technology Review)																	Executive Memorandum 94-08 8/31/94; B&F Memo 10/18/94; CS Circular 90-1 9/14/90; ICSD T-205 Approval Process; EM 08-05; AD 87.1; CM 2011-14 & 2011-05	New York
Service Contract Information Technology (SCIT) Certification Policy																		California 4819.31
DISASTER RECOVERY																		
Disaster Recovery Planning Policy				O														California 4819.31

POLICY & PROCEDURE CROSSWALK

Key: Collateral exists — Good collateral example
P Procedure — O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C moves to IT	CSEA	DCCA	DLNR	DOH	DOH	DHS	DOT	ICSD	HCJDC	DAGS	JPIC	Privacy	PSD	UH			
IT Business Continuity Planning Guideline																		
STORAGE/BACKUP																		
Storage/Backup Policy				O														
TELECOMMUTING																		
Telecommuting Policy																	DHR MOU	
STRATEGIC PLAN																		
Agency Strategic Plan																		California 4900.2
Information Management Strategic Planning Process																		California 4819.31
IT Capital/Portfolio Planning																		California 4819.31/4904
IT Performance Management																		
IT Project Oversight Framework (including reporting and project criticality classification)																		California 4819.31.10/4800
OTHER																		
Data Entry Policy																		

* Include social media, email, etc. (See Maryland's.)