

Sunset Public Hearing Questions for
Information Systems Council
Created by Section 4-3-5501, *Tennessee Code Annotated*
(Sunset termination June 2015)

1. Provide a brief introduction to the council, including information about its purpose, statutory duties, staff, and administrative attachment.

Introduction

The Information Systems Council (ISC) was established by law in May, 1994 when the *Tennessee Code Annotated* was amended to enact the organization, membership, and duties of the Information Systems Council. Prior to this, Governor McWherter established the ISC by Executive Order Number 18. The concept of the Council was first initiated by Governor Dunn, when he issued Executive Order Number 18 on January 20, 1972, and similar Executive Orders were issued by each succeeding Governor.

Purpose

The ISC is to set policy in the overall direction of Information Technology. (See Attachment A.)

Statutory Duties

The ISC develops policy for the overall management of the State's information systems to assure:

- Appropriate hardware and software for the State's Data Center;
- Appropriate security and disaster recovery policies and procedures for the State's information systems environment;
- Cost effective use of departmental computer systems, which shall, for the purpose of this policy, include the appropriate use and integration of microcomputers and minicomputers into the State's information management systems;
- Appropriate and cost effective telecommunication policies;
- Make recommendations to the Governor and General Assembly regarding amendments to the purchasing laws which would be beneficial in the establishment and operation of information systems;
- Establishment of guidelines for the acquisition and maintenance of both hardware and software;
- Establishment of effective long-range planning for the State's information management systems; and
- Priorities are set for the development and deployment of new information systems.

Staff

The Office for Information Resources (OIR) serves as staff.

Administrative Attachment

None.

2. Provide a list of current members of the council. For each member please indicate who appointed the member and how member's presence on the council complies with Section 4-3-5501, *Tennessee Code Annotated*. Please indicate each member's race and gender and which members, if any, are 60 years of age or older. Are there any vacancies on the council? If so, what is being done to fill those vacancies?

Based upon Section 4-3-5501, Tennessee Code Annotated, the current members of the ISC include:

VOTING MEMBERS

MEMBERS BY OFFICE – Appointed by Statute:

Commissioner of the Dept. of Finance & Administration, Larry Martin, Chairman
Commissioner of the Dept. of General Services, Bob Oglesby
Comptroller of the Treasury, Justin Wilson

LEGISLATURE

Information Systems Director, Vinay Dattu

SENATORS—Appointed by the Lieutenant Governor

Senator Thelma Harper
Senator Brian Kelsey
Senator Ken Yager

REPRESENTATIVES—Appointed by the Speaker of the House

Representative Mike Harrison
Representative Ryan Haynes
Representative Steve McDaniel

SUPREME COURT DESIGNEEE

Administrative Office of the Courts, Ann Lynn Walker, Assistant Director, Technology

PRIVATE SECTOR—Appointed by the Governor

The Bank of New York Mellon, Mr. Donald Enfinger

TENNESSEE REGULATORY AUTHORITY—Appointed by TRA

NON-VOTING MEMBERS—Appointed by Statute

Information Technology Management Assoc., Ken Bernhardt, Dept. of Environment & Conservation

TSEA Rep., Martha Wettemann, Depart. of Labor & Workforce Development

STAFF

Chief Information Officer, Dept. of Finance & Administration, Mark Bengel

3. How many times did the council meet in fiscal year 2013 and to date in fiscal year 2014? How many members were present at each meeting?

Meetings in the July 2012-April 2014 Timeframe

July 30, 2012 = 8 (2 non-voting)	July 29, 2013=7 (2 non-voting)
November 19, 2012 =7 (2 non-voting)	October 28, 2013=6 (2 non-voting) No Quorum
February 1, 2013= 8 (2 non-voting)	
April 29, 2013=8 (2 non-voting)	February 24, 2014=5 (2 non-voting) No Quorum

4. What per diem or travel reimbursement do members receive? How much was paid to council members during fiscal years 2013 and to date in calendar year 2014?

None of the ISC Legislative members have requested per diem or travel reimbursement during FY 2013 or thus far in FY 2014. No other member is paid or reimbursed.

5. What were the council's revenues (by source) and expenditures (by object) for fiscal year 2013 and to date in 2014? Does the council carry a fund balance and, if so, what is the total of that fund balance? If expenditures exceeded revenues, and the council does not carry a fund balance, what was the source of the revenue for the excess expenditures?

There was no revenue for the ISC in the past two years. There were no expenditures for travel and meals in Fiscal Year 2013 and no expenditures are estimated for Fiscal Year 2014.

6. In addition to the disclosure requirements placed on individual members of the council at Section 8-50-501, *Tennessee Code Annotated*, how does the council ensure that its members and staff are operating in an impartial manner and that there are no conflicts of interest? If the council operates under a formal conflict of interest policy, please attach a copy of that policy.

The Information Systems Council operates under TCA 8-50-501. The Council does not have any additional policies in place.

7. Is the council subject to Sunshine law requirements (Section 8-44-101 et seq., *Tennessee Code Annotated*) for public notice of meetings, prompt and full recording of minutes, and public access to minutes? If so, what procedures does the council have for informing the public of its meetings and making its minutes available to the public?

Yes, the Council is subject to Sunshine law requirements. Notices of scheduled meetings are posted throughout State office buildings where the public would have access and are distributed via electronic mail to anyone who has requested notification of meetings. In addition, notices of meetings are posted on the State's Internet site:

<https://apps.tn.gov/pmn/detail/publicbody/252.html>. The minutes are formally approved at the following meeting, and are made available to the public once they are approved by the ISC. The meetings are attended by many suppliers of Information Technology. The meeting area has a section reserved for the public.

The provisions of Section 4-3-5509, *Tennessee Code Annotated*, which were enacted in 2005, allow the ISC to consider confidential security issues only in a session that is closed to the public.

The ISC is committed to functioning under the Sunshine Law. It is the intent of the Council to keep closed sessions to the minimum necessary. Only those portions of the meeting that deal with security issues are closed. The process that is followed is that the proposed agenda, with recommendation for closing the meeting (or portion of the meeting), is presented to the Department of Finance and Administration's Chief Counsel for review and concurrence.

8. Has the council developed policy guidelines for the overall management of the state's information systems, including the areas specified in Section 4-3-5502(1), *Tennessee Code Annotated*? Please describe the policy development process, including (for example), what types of information the council reviews and what types of input the council receives prior to developing a policy? How often are policies reviewed to ensure they are applicable given changes in information technology? How often has the council made recommendations to the Governor and the General Assembly regarding needed amendments to the purchasing laws (as they relate to information technology)?

Policy Guidelines

As of the 2002 Sunset Review, the ISC had approved twelve policies regarding information technology. They were:

- Policy 1 - Data Security;
- Policy 2 - Information Systems Review;
- Policy 3 - Ownership;
- Policy 4 - Information Systems Design & Programming;
- Policy 5 - Information Systems Management & Application Development Policy;
- Policy 6 - Architecture;
- Policy 7 - Information Systems Planning;

- Policy 8 - Systems Dial-Up Access Security;
- Policy 9 - Disaster Recovery;
- Policy 10 - Data Resource Management;
- Policy 11 - Surplus of State Computers;
- Policy 12 - Open Access to Electronic Information;

An Internet Information Privacy statement was approved by the ISC in its January 25, 2001 meeting.

ISC policies were reviewed and revamped in September 2004. The following actions have been taken:

- Policy 1 - Data Security; Revised September 2004
- Policy 2 - Information Systems Review; Deleted and merged into Policy 7, September 2004
- Policy 3 - Ownership; Deleted September 2004
- Policy 4 - Information Systems Design & Programming; Deleted September 2004
- Policy 5 - Information Systems Management & Application Development Policy; Revised December 2004
- Policy 6 - Architecture; Revised September 2004
- Policy 7 - Information Systems Planning; Revised September 2004
- Policy 8 - Systems Dial-Up Access Security; Deleted September 2004
- Policy 9 - Disaster Recovery; Revised September 2004
- Policy 10 - Data Resource Management; Revised September 2004
- Policy 11 - Surplus of State Computers; Deleted December 2004
- Policy 12 - Open Access to Electronic Information; Revised September 2004
- Policy 13 – Network Infrastructure Support and Maintenance, Adopted September 2003, Revised September 2004
- Policy 14 – Electronic and Digital Signatures, Adopted March 2007

ISC policies are reviewed periodically and revisions, additions, recommendations for deletions are presented to the Information Systems Council as needed. The following highlights the status of each policy since the previous Sunset review:

- Policy 1 - Data Security; Revised October 2011
- Policy 2 – Reserved for Future Use
- Policy 3 – Reserved for Future Use
- Policy 4 – Reserved for Future Use
- Policy 5 - Information Systems Management & Application Development Policy; Revised November 2012
- Policy 6 - Architecture; Revised September 2004
- Policy 7 - Information Systems Planning; Revised September 2004
- Policy 8 – Reserved for Future Use
- Policy 9 - Disaster Recovery; Revised September 2004
- Policy 10 - Data Resource Management; Revised December 2009

- Policy 11 – Reserved for Future Use
- Policy 12 - Open Access to Electronic Information; Revised December 2009
- Policy 13 – Network Infrastructure Support and Maintenance, Adopted September 2003, Revised October 2011
- Policy 14 – Electronic and Digital Signatures, Revised March 2007

Policy Development Process

The procedure for establishing new policies or modifying existing policies requires the Office for Information Resources (OIR) to develop policy recommendations identifying why the need for the change or new policy, and describing how information technology would be affected by the change. Then a presentation is made to the ISC for review and approval.

Frequency

OIR, as staff to the ISC, continually reviews the policies as technology changes, when appropriate any change would be presented to the ISC for review and approval. In addition, OIR instituted a cycle of periodic review of all policies in 2004. The next scheduled review is December of 2014.

Technology Purchasing Recommendations

In accordance with TCA 4-3-5504, the Office for Information Resources submitted to the ISC a recommendation for “OIR Research and State Standard Setting Proprietary Purchasing” (Attachment B). This recommendation was approved by the ISC at the January 25, 2001 meeting and continues to be used.

The ISC also made recommendation regarding purchasing laws and the “Limit of Liability” change made in the early 2000 timeframe. This change was brought about by the number of vendors not willing to respond to technology RFP’s and ITB’s due to the State’s existing unlimited liability clause.

Under the direction of the ISC, OIR works closely with the Central Procurement Office to develop policies and processes that result in improved technology outcomes. Meetings with the vendor community have been held during FY 2014 to discuss innovative approaches to procurement.

Other Recommendations

Other information technology related recommendations made by the ISC include:

- Security legislation to protect State Network. TCA Section 10-7-504 (January 2001)
- Changes to Department of Personnel Rating for technical positions. TCA Section 8-30-333 (SB 1326 and HB635) (January 2001)

- Access to State’s Digital Information. TCA Section 10-7-506 (September 1999)
 - Adoption of the Acceptable Use Policy Network Access Rights and Obligations (September 2003, revised September 2004 and February 2008)
 - Assessments and recommendations concerning the information technology divisions of each executive branch department as part of Next Generation IT.
9. Describe the council’s process for reviewing the overall effectiveness and efficiency with which the state’s information systems network is managed as required at Section 4-3-5502(2). Who performs the reviews? How often are reviews performed? What types of issues are covered in the reviews? How many such reviews were conducted during fiscal year 2013 and to date in 2014? Are written reports prepared and transmitted to the appropriate agency head, the Governor, and the Speakers of the Senate and House of Representatives?

The ISC reviews the overall effectiveness and efficiency with which the State’s information systems network is managed. Such reviews are conducted where appropriate on a department by department basis for the purpose of identifying weaknesses in the current system as well as opportunities for improvements in each department’s information systems. Such reviews include, but are not be limited to:

- The adequacy of systems development planning and implementation;
- Opportunities for increased efficiency through either a reduction of the long run current operating costs for various programs of state government and/or the opportunity to provide increased services through more effective use of management information systems; and
- The most appropriate and cost effective hardware and software.

The ISC uses several techniques in reviewing the overall effectiveness and efficiency in managing information systems. Some of the ways are:

- An outside consultant may be used to evaluate the direction the state is taking in deploying technology. Examples include various studies conducted by Gartner Group, Inc. (a national research firm in technology) over the years. These include:
 - a. Assessment of the Department of Human Services’ technology assets and recommendations of a strategic roadmap for that Department (FY 2014)
 - b. Evaluation of the Department of Children’s Services TFACTS System (FY 2013)
- The ISC may request any agency to appear before it to review any new application, to define the services to be provided, the cost effectiveness of the application, cost savings attributable to the application, and describe how service is being improved by the application.
- The ISC reviews status reports for major system developments at each meeting.
- The ISC has instituted a statewide information systems planning process where the agencies develop an information systems plan that is submitted by July 1 of each year. This year the Office for Information Resources, Business Solutions Delivery

and Finance and Administration's Division of Budget reviewed approximately 50 plans for departments and agencies from all three branches of government. The review focuses on the applications and the technology infrastructure required to support the agency's business strategy as well as the maximization of data sharing among state and local governments. One major objective is to eliminate the duplication of systems in different departments.

Also, major projects are evaluated by analyzing all cost components in development, implementation, operation as well as existing cost savings and improved services to be delivered. After the review, each agency head receives a disposition of their plan with appropriate recommendations from the review committee. From this process the department may submit a request for funding of any projects they have defined in their plan.

The Office for Information Resources uses the information systems plans and industry trends to anticipate new technologies that may be needed, along with the infrastructure required to support the implementation of future technologies and applications. Risk evaluations are also performed to ensure that the state's existing information infrastructure is not adversely affected in a manner harmful to the job performance of program personnel and the delivery of services to the citizens.

From these agency plans, a Consolidated Information Systems Plan is prepared and distributed to each member of the ISC, commissioners and agency heads. OIR plans to present copies directly to the governor and speakers of the house of representatives and senate beginning with the next publication of the Consolidated Information Systems Plan. The plan is also made available via the Internet:
http://oir.intranet.tn.gov/sites/oir.intranet.tn.gov/files/planning/statewide-plan-2014/2013-14_Statewide_Plan.pdf

10. When establishing the policy under which the state procures telecommunications, computer, or computer-related equipment or services, how does the council ensure that it has selected the purchasing method that will produce the lowest and best overall costs to the state? Describe the factors the council considers, the sources of information it uses, etc.

The Information Systems Council is responsible for establishing the policy under which the State procures telecommunications, computer or computer-related equipment or services. The Council, in establishing procurement policy, also has the ability to authorize research and development, including the procurement of equipment, for the purpose of improving the State's information system. Such procurements are administered by either the Department of General Services and/or the Department of Finance and Administration under existing laws, rules and regulations governing procurements.

The Council uses different techniques and frequency in reviewing the overall effectiveness and efficiencies of the management of the status information.

- On occasions where appropriate, the Council through OIR has used consulting services to provide review and direction in implementing technology. For example, Salvaggio, Teal and Associates, Inc. provided review and direction as the State designed and implemented its Enterprise Resource Planning system (Project Edison). The Department of Human Services is completing an engagement with Gartner to develop a strategic roadmap for its information systems portfolio. Similar engagements have been secured through competitive procurements for various departments over the years.
- At each ISC meeting, OIR provides a status review of each major system under development. In addition, agencies that have completed major projects are asked to present to the Council a review of the projects, how it is meeting stated objectives and benefits being received.
- The Council through OIR has used consultants to compare the cost effectiveness of services being provided to other governmental and private entities. A benchmark evaluation was completed in 2006, when the State's information technology organizations and functions were benchmarked by the Hackett Group. A review of OIR's major rates was completed in FY 2014 by the Gartner Group.

One of the major factors the ISC considers in the IT acquisition is "Total Cost of Ownership." This cost considers not only the purchase price but the cost of training, support, maintenance, and other variable factors that occur over the life of the technology. In approving the "OIR Research and State Standard Setting Proprietary Purchasing" procedure (Attachment B), a major factor considered is how effective the technology will integrate into the state's standard architecture.

The State of Tennessee uses the research services (selected through the competitive procurement process) of a national research group (Gartner Group, Inc). The company specializes in information technology and the evaluation of products and services. This firm focuses on the viability of products and the life cycle cost, as well as, the shortcomings of products being offered by vendors. Additionally, the projected long-term financial stability of a vendor is provided.

Risk evaluations are also performed to ensure that the state's existing information infrastructure is not adversely affected in a manner harmful to the job performance of program personnel and the delivery of services to the citizens.

11. Section 4-3-5508, *Tennessee Code Annotated*, refers to functions for the council that are spelled out in Sections 47-10-117 through 47-10-120, *Tennessee Code Annotated*, referred to as the Uniform Electronic Transactions Act, which was enacted in 2001. Please describe those functions and what policies the council has implemented to address these functions. How have the policies been communicated to other state departments and agencies that must comply with the policies?

OIR adopted Entrust as the public key infrastructure standard in 1999 and serves as the foundation for digital signature capability. With the passage of the new ISC functions enacted in 2001, OIR dealt with requests for the use of digital and electronic signatures on a

case by case basis. As the number of requests for the usage of electronic signatures increased, it became necessary to develop a formal policy. The ISC adopted Policy 14, Electronic and Digital Signatures, to delegate the review and approval of requests to OIR. Requests to use electronic and digital signatures are made in agencies' Information Systems Plans and are reviewed through the standard planning process. This was communicated to State departments and agencies in regularly scheduled Information Technology Management Association (formerly Information System Management) group meetings. In addition, the Information Systems Planning Guidelines includes information about this review. The costs, benefits and business needs are discussed as appropriate with agency management in the yearly Information Systems Plan review meetings.

12. Has the council set goals and measured its performance compared to those goals? What performance indicators or goals does management use to measure the effectiveness and efficiency of the council? How well has the council performed based on those performance indicators?

The Council has not set goals.

13. What reports does the council prepare on its operations, activities, and accomplishments, and who receives these reports?

The Council has not prepared any reports on its operations and accomplishments. However, the consolidated Information System Plan is published annually and is an important deliverable in meeting the requirements of ISC Policy 7.00: Information Systems Planning. This document provides an Executive Overview for Information Systems; information on the Office for Information Resources; an overview of each department; and a summary of Information Technology Management issues.

http://oir.intranet.tn.gov/sites/oir.intranet.tn.gov/files/planning/statewide-plan-2014/2013-14_Statewide_Plan.pdf

14. Can the council promulgate rules? If not, is rule-making authority needed? If rules have been promulgated, please cite the reference.

The ISC statute does not contain authority to promulgate rules. Since the Council's work pertains to the internal operations of state government, rulemaking authority does not seem to be needed. However since OIR serves as staff to the ISC, and is a division of the Department of Finance and Administration, OIR anticipates that any need for rule-making could be satisfied under the rule-making authority of the Department of Finance and Administration.

15. Describe any items related to the council that require legislative attention and your proposed legislative changes.

There are no proposed legislative changes at this time.

16. Should the council be continued? To what extent and in what ways would the absence of the council affect the public health, safety, or welfare?

Tennessee taxpayers demand increased services in a more timely and cost-effective way and information technology is a major mechanism utilized to meet that demand. Information technology today is absolutely critical to all State business functions. At the same time, the information technology infrastructure is much more complex than it was a decade ago. The risks associated with a breach of confidentiality of data, unavailability of essential information systems, and the need to ensure data integrity drive the State to ensure proper oversight of its information technology resources. Therefore, it is absolutely critical to maintain a guiding Council with the authority to establish and maintain all technical (and product) standards, standard information technology practices, and security standards for the State. Without this, the State would inevitably experience exponentially escalating costs, security risks, and unplanned, interruption of business services.

The unique composition of the ISC includes representation from the Legislative, Judicial, and Executive branches of state government, in addition to a Constitutional officer and private business leaders. This representation fosters the development of technology and security standards that transcend the separate branches of government whenever feasible. The varied experience and expertise of Council members ensures that technology will be utilized in a cost-effective and citizen-beneficial way.

What negative effects would result if the Council were not in existence?

If this Council were not in existence, Tennessee would lose its unique ability to be guided by senior management from all three branches of State government as well as the private sector. As a result, cost efficiencies and information technology effectiveness realized over the past 25-30 years would be in jeopardy.

17. Please list all council programs or activities that receive federal financial assistance and, therefore are required to comply with Title VI of the Civil Rights Act of 1964. Include the amount of federal funding received by program/activity.

Not Applicable

- 18. *If the council does receive federal assistance, please answer questions 19 through 26. If the council does not receive federal assistance, proceed directly to question 25.***

19. Does your council prepare a Title VI plan? If yes, please provide a copy of the most recent plan.

20. Does your council have a Title VI coordinator? If yes, please provide the Title VI coordinator's name and phone number and a brief description of his/her duties. If not, provide the name and phone number of the person responsible for dealing with Title VI issues.

21. To which state or federal agency (if any) does your council report concerning Title VI? Please describe the information your council submits to the state or federal government and/or provide a copy of the most recent report submitted.
22. Describe your council's actions to ensure that council staff and clients/program participants understand the requirements of Title VI.
23. Describe your council's actions to ensure it is meeting Title VI requirements. Specifically, describe any council monitoring or tracking activities related to Title VI, and how frequently these activities occur.
24. Please describe the council's procedures for handling Title VI complaints. Has your council received any Title VI-related complaints during the past two years? If yes, please describe each complaint, how each complaint was investigated, and how each complaint was resolved (or, if not yet resolved, the complaint's current status).

25. Please provide a breakdown of current council staff by title, ethnicity, and gender.

Name	Title	Race	Gender	Over 60
Larry Martin, Chair	Commissioner, Dept. Of Finance and Administration	White	Male	Yes
Bob Oglesby	Commissioner, Dept. of General Services	White	Male	No
Justin Wilson	Comptroller of the Treasury	White	Male	Yes
Thelma Harper	State Senator	Black	Female	Yes
Brian Kelsey	State Senator	Caucasian	Male	No
Ken Yager	State Senator	Caucasian	Male	No
Mike Harrison	State Representative	Caucasian	Male	No
Ryan Haynes	State Representative	Caucasian	Male	No
Steve McDaniel	State Representative	Caucasian	Male	Yes
Ann Lynn Walker	Assistant Director, Administrative Office of the Courts	Caucasian	Female	No
Vinay Dattu	Information Technology Director, General Assembly	Other	Male	No
Donald Enfinger	Bank of New York	White	Male	Unknown

Non-Voting Members

Name	Position	Race	Gender	Over 60
Ken Bernhardt	Chair, Information Technology Management Association	White	Male	No
Martha Wettemann	TSEA Representative	White	Female	?

26. Please list all council contracts, detailing each contractor, the services provided, the amount of the contract, and the ethnicity of the contractor/business owner.

The Council does not have any contracts.

ISC – Information Resources Policies

Table of Contents

POLICY 1.00: DATA SECURITY	2
POLICY 2.00: RESERVED FOR FUTURE USE	4
POLICY 3.00: RESERVED FOR FUTURE USE	5
POLICY 4.00: RESERVED FOR FUTURE USE	6
POLICY 5.00: INFORMATION SYSTEMS MANAGEMENT & SYSTEM DEVELOPMENT LIFE CYCLE	7
POLICY 6.00: ARCHITECTURE	9
POLICY 7.00: INFORMATION SYSTEMS PLANNING	10
POLICY 8.00: RESERVED FOR FUTURE USE	12
POLICY 9.00: DISASTER RECOVERY	13
POLICY 10.00: DATA RESOURCE MANAGEMENT	15
POLICY 11.00: RESERVED FOR FUTURE USE	17
POLICY 12.00: OPEN ACCESS TO ELECTRONIC INFORMATION	18
POLICY 13.00: NETWORK INFRASTRUCTURE SUPPORT AND MAINTENANCE	21
POLICY 14.00: ELECTRONIC AND DIGITAL SIGNATURES	24

ISC – Information Resources Policies

Policy 1.00: Data Security

All information technology resources must be appropriately and adequately protected against unauthorized access, modification, destruction or disclosure.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that all information technology resources are protected in accordance with the statutes of the State of Tennessee.
2. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.
3. Define the responsibilities of information systems management and users in the protection of information technology resources.
4. Provide access to authorized users.

SCOPE:

All information technology resources and associated components, such as Internet-facing applications, networks, telecommunications, hardware, software, data, related documentation, and reports.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Provide the technology infrastructure, including but not limited to networks and Data Center hosting facilities, required to provide secure, Internet-facing applications.
2. Develop the standards, procedures, and guidelines necessary to assure security of the State's information technology resources.
3. Provide technical consulting support to agencies in fulfilling their information technology resources security goals.
4. Provide technical support, training and recommendations for the agencies' use of the State's standard systems security software.
5. Provide ongoing technical reviews of security aids, tools, techniques and other methods to meet security requirements: develop and recommend, in conjunction with agencies, to the Information Systems Council new or revised policies necessary to assure security of the State's information technology resources.
6. Provide for an administrative review of security standards, procedures, and guidelines in light of technical, environmental, procedural or statutory changes which may occur.

ISC – Information Resources Policies

6. Protect information technology resources under OIR's control in accordance with statewide policies, standards, and procedures.
7. Assign an individual the responsibility and authority for administrative oversight of security for the State's information technology resources.

Agency Management, Information Systems Group

1. Collaborate with F&A/OIR to ensure that all Internet-facing applications are hosted in a State-managed Data Center.
2. Assign an individual the responsibility and authority for administrative oversight of security for information technology resources under the agency's control.
3. Establish agency policies, standards, procedures, and guidelines for securing the agency's information technology resources consistent with published statewide directives.
4. Protect information technology resources under agency control in accordance with applicable statutes and with policies, standards, procedures, and guidelines established at both the statewide and agency levels.
5. Educate agency users on security policies, standards, procedures and guidelines related to information technology resources.
6. Provide for an agency administrative review of security standards, procedures and guidelines in light of technical, environmental, procedural, or statutory changes which may occur.

Individual Users

1. Adhere to statewide and agency policies, standards, procedures and guidelines pertaining to information technology resources security.

ISC – Information Resources Policies

Policy 2.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 3.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 4.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 5.00: Information Systems Management & System Development Life Cycle

Information systems projects will follow a standard project management methodology and business information systems will be developed using an industry standard methodology.).

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Provide a defined project management methodology, which will provide guidance and consistency in the execution of all projects.
2. Provide a common process for status reporting and facilitate quality and funding reviews.
3. Provide a development life cycle methodology, which will define a detailed framework for ensuring the requirements are identified and the solutions are developed and deployed using a standardized process.
4. Deliver quality systems on time and within budget in a consistent and maintainable manner that conforms to the State's software and hardware architectural and security infrastructure standards.

SCOPE:

The policy applies to all (a) statewide and departmental, (b) mainframe and distributed, and (c) in-house developed and procured information system projects and application systems development.

IMPLEMENTATION:

Department of Finance & Administration, Business Solutions Delivery (BSD)

1. Develop and maintain an Information Technology Methodology (ITM) based on industry best practices that are adapted to the state's needs for a standard project management and other key project disciplines guide.
2. Develop a System Development Life Cycle (SDLC) methodology that incorporates design and development standards, procedures, guidelines, and best practices in support of the State's architectural standards.
3. Provide the availability of training classes in the use of the methodologies and development processes.

ISC – Information Resources Policies

4. Provide consulting support in the use of the methodologies and development processes.
5. Provide access to the ITM and SDLC documentation on the State's Intranet with access from the OIR Intranet.
6. Provide a base of skilled project managers in support of agencies' business solutions needs.
7. Incorporate the methodologies and development techniques in all business solutions projects.

Agency Management

1. Train appropriate agency personnel in the use of the methodologies and techniques.
2. Incorporate the methodologies and development techniques in all application development projects.

ISC – Information Resources Policies

Policy 6.00: Architecture

Standards and guidelines will be established to support a common Information Technology infrastructure that enables the effective use of information technology in the State.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

Office for Information Resources, *Tennessee Information Resources Architecture*.

OBJECTIVES:

1. Ensure a compatible statewide network of information technology hardware, software, and communications resources.
2. Enable the interchange of data.
3. Allow for the cost effective use of information technology systems while maintaining maximum compatibility statewide.
4. Provide standard prerequisite functional requirements for hardware and software procurements.
5. Ensure agency technical direction is in alignment with overall State technology policy.

SCOPE:

The policy applies to all information technology resources.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Establish a process for the review of agency requests for exceptions to the Tennessee Information Resources Architecture.
2. Maintain the *Tennessee Information Resources Architecture*.
3. Establish procedures to support the use of the architecture at the state, departmental, and desktop levels.
4. Establish procedures to ensure that the architecture evolves as technology progresses.

Agency Management

1. Technology direction and objectives must be in alignment with overall State objectives and comply with the Tennessee Information Resources Architecture.
2. Participate in the architectural review process and provide input to the review of components of the architecture.

ISC – Information Resources Policies

Policy 7.00: Information Systems Planning

An Information Systems Plan will be prepared annually by each agency. All agency requests for information technology resources and services will be reviewed. Major technology requests may be presented to the Information Systems Council. The Office for Information Resources will administer the planning and review process and prepare a Statewide plan.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

State of Tennessee Information Systems Planning Guidelines

State of Tennessee Cost Benefit Analysis Methodology

OBJECTIVES:

1. Develop and document the agency's information technology needs, costs and anticipated benefits and savings to the State.
2. Provide a mechanism for identifying future technology needs, and information resource management issues within the State.
3. Identify and prioritize the information technology projects within the agency as a prelude to the budgetary process.
4. Provide for the formal review of information technology requests. Reviews will consider business alignment, feasibility, service level, cost effectiveness and adherence to the State's information technology policies and architectural standards.
5. Identify statewide information technology requirements.
6. Provide information to facilitate the management of information resources within the State.

SCOPE:

This policy applies to all state agencies.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Establish guidelines and procedures by which the plan will be developed.
2. Establish procedures for the review of agency requests for information technology resources and services. The review will consider business alignment, feasibility, cost effectiveness and adherence to the information systems policies and standards.
3. Responsible for the consolidation of the agency plans into a statewide plan.

ISC – Information Resources Policies

4. Responsible for the identification of statewide information technology requirements for budgetary planning.
5. Responsible for providing training and guidance to agencies to support the development of their plan.

Agency Management

1. Responsible for developing the agency Information Systems Plan following the guidelines provided.
2. Responsible for updating the plan as needed throughout the year.
3. Establish procedures for the review of agency requests for information technology resources and services by agency management.

ISC – Information Resources Policies

Policy 8.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 9.00: Disaster Recovery

Disaster recovery planning and the capability for implementing a recovery are required encompassing all critical data processing applications and their peripheral support activities.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that all critical information systems can be recovered in the event of a disaster which disrupts any of the data processing facilities of the State.
2. Provide the capability to continue processing critical information systems, both centralized and departmental, in the event of a disaster.
3. Define the responsibilities of OIR and agency information system management in the development of a disaster recovery plan for critical information systems.

SCOPE:

The policy will apply to all Agency-level and Statewide systems.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Develop and recommend to agencies, the standards, procedures and guidelines necessary to assure recovery capabilities for the State's information systems.
2. Define the procedure for declaring a disaster.
3. Define criteria for an application to be defined as critical.
4. Provide an ongoing technical review of disaster recovery aids, tools, techniques and other methods to meet ongoing disaster recovery requirements.
5. Provide for an administrative review of disaster recovery considerations in light of technical, environmental, procedural or statutory changes which may occur.
6. Provide management and technical consulting support to agencies in fulfilling their disaster recovery roles.
7. Utilize disaster recovery software and create the centralized disaster recovery plan.
8. Provide centralized disaster recovery coordinator and alternate.

Agency Management

1. Responsible for establishing policies and procedures for the development of the agency's disaster recovery plan.

ISC – Information Resources Policies

2. Provide an agency disaster recovery coordinator who will be responsible for ensuring that the agency's portion of the centralized plan and that the agency's individual plan allow the agency to recover their critical information systems.
3. Responsible for establishing recovery procedures for the peripheral activities required to continue the agency's critical production tasks.

ISC – Information Resources Policies

Policy 10.00: Data Resource Management

Data is a valuable resource and shall be managed and optimized to benefit the State as a whole.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Plan and promote the effective and efficient sharing and usage of data to support State Government.
2. Ensure personnel have access to the data they need to perform their job functions.
3. Promote the understanding and accessibility of the State data resources.
4. Facilitate ad hoc access and reporting of data maintained in relational databases.
5. Ensure data resources will be shared among systems (applications, users, agencies).
6. Ensure data redundancy is minimized and managed.
7. Ensure data will be precisely and consistently defined (i.e. that standards exist and are enforced).
8. Manage the data life cycle independent of the application system life cycle.

SCOPE:

This policy applies to all data utilized at the State.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Implement the facilities, standards, and procedures necessary to document and maintain information about data in a State repository.
2. Develop and implement standards, procedures, and guidelines for the use of database management facilities.
3. Ensure the physical security and protection of data on systems managed by the Office for Information Resources.
4. Implement and maintain the physical storage definitions, standards, and procedures so that the operational efficiency, integrity, and security of databases are maintained; and that development productivity is maximized in accessing the data.
5. Provide ongoing performance monitoring and tuning of State and departmental level relational databases.

ISC – Information Resources Policies

6. Provide design review and approval for logical and physical data models delivered in accordance with the appropriate methodology and State standards, procedures, and guidelines.
7. Provide data access support and guidance.
8. Provide tools and techniques necessary to support ad hoc reporting.
9. Ensure the consistency and quality of the State data resources by coordinating the ongoing maintenance of standards, guidelines, and procedures; ensuring that published standards and procedures are followed.
10. Provide training for the use of techniques and facilities related to data analysis and the utilization of State database facilities.

Agency Management

1. Construct agency data models. Provide data analysis deliverables in accordance with the appropriate methodology and State standards, procedures, and guidelines.
2. Provide complete and accurate business descriptions of data elements to maintain the central repository.
3. Ensure the integrity of data maintained in automated files or databases and of reports produced from the data.
4. Ensure the physical security and protection of data on systems managed by the Agency.
5. Develop internal procedures which comply with State data-related standards and guidelines.
6. Assign responsibility for controlling access to agency data resources.

ISC – Information Resources Policies

Policy 11.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 12.00: Open Access to Electronic Information

The State of Tennessee will aggressively and cost-effectively use information technology, as well as emerging technologies, in order to provide efficient, effective, equal, and universal citizen access to public information as defined by law.

REFERENCE:

Tennessee Code Annotated, Sections 10-7-301, 10-7-503, and 10-7-504 -- as amended.

Federal laws, such as the Freedom of Information Act, the Privacy Act, and the Americans with Disabilities Act, which govern the use, disclosure, and accessibility of data collected by government programs which are partially or completely federally funded.

OBJECTIVES:

1. Promote interaction among citizens, governments, businesses and organizations, as well as efficient dissemination of mission-related public information, through the use of information technology.
2. Provide broad, equitable, and affordable access to electronically-stored, non-restricted public records seeking to ensure that all citizens have access to such records. This includes citizens with disabilities, citizens with limited financial resources, and citizens from rural areas.
3. Assure protection of the individual citizen's privacy rights by safeguarding electronically-stored, legally-defined private and confidential information.
4. Maximize the convenience and cost-effectiveness of electronic access to public information through intergovernmental coordination and organization of information.
5. Based upon statutory authorization, establish uniform methods for calculating charges for the creation and provision of online electronic access to public records, as well as for the copying of electronic files containing public records.
6. Provide a coherent and collaborative framework for government agencies to address these objectives.

SCOPE:

All electronically-stored, non-restricted public records housed within the state's information technology environment.

ISC – Information Resources Policies

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Incorporate in the Information Systems Planning process (see Policy No. 7.00) a component which addresses the electronic dissemination and access of public information to Tennessee citizens.
2. Develop a comprehensive and structured identification or classification system (TILS - Tennessee Information Locator System) which provides an effective means for organizing and locating information resources made available for electronic access; thus, in composite form, establishing a state inventory for managing the state's information holdings.
3. Ensure that agency information holdings are identified and described in the state's information inventory, and that information is effectively disseminated.
4. Require that appropriate security controls are in place to protect critical systems and to prohibit access to restricted information by remote electronic means.
5. Guided by statute(s), establish pricing guidelines for creating and providing online electronic access to public records, as well as for copying electronic files containing public records.
6. Provide the infrastructure for remote access to public records via the most widely dispersed and generally available technologies.
7. Promote collaboration among government agencies to provide citizens with access to "related" public records. Through the "bundling" of these records, OIR will seek to avoid duplication of information, to make access to information more convenient for citizens, and to share the cost of technology.

Agency Management, Information Systems Group

1. Provide access to electronically-stored, non-restricted government information. While online public access may not be feasible for existing information systems, agencies must plan for such capacity in the design of future systems and information dissemination strategies.
2. Confer with the appropriate agency officials to identify the types of electronic public records and public record information under their custody which are exempt from inspection, examination, and copying under Tennessee's Open Records Law or other legislation.
3. Assess and define electronic dissemination and access needs, together with the information systems required to respond to those needs, for any new systems at an early stage of the project planning process.
4. Be knowledgeable of all electronic public access activities that involve the agency's data.
5. Provide adequate staff training in the requirements of Tennessee's Open Records Laws and the responsibilities set forth in this policy, with particular attention to staff's responsibility for maintaining the confidentiality of exempt information or records.
6. Ensure that all electronic data subject to restricted access (in accordance with Tennessee's Open Records laws and other applicable statutes or regulations which authorize such restriction) are properly identified and managed.

ISC – Information Resources Policies

7. Assure that all data provided for electronic dissemination and access to the public are kept up-to-date and accurate.
8. Provide timely updates to the state's inventory of information resources. The provisioning of public records via information technology must be compliant with the Tennessee Information Locator System (TILS) Guidelines to ensure the widest possible access to these records.
9. Minimize repetition and duplication of electronically disseminated information by utilizing the state's information inventory.
10. Adhere to established guidelines and statutes concerning the calculation of charges for the creation and provision of online electronic access to public records, as well as for the copying of electronic files.
11. Publicize that public information can be accessed via technology.

ISC – Information Resources Policies

Policy 13.00: Network Infrastructure Support and Maintenance

The Office for Information Resources will manage and secure the State's network infrastructure to ensure the reliability, integrity, availability, and confidentiality of the operations of government and those it serves.

REFERENCE:

Tennessee Code Annotated § 4-3-5501, effective May 10, 1994 [Acts 1994, ch. 992, § 2; 1995, ch. 305, § 66]

Tennessee Code Annotated § 4-3-5502, effective May 10, 1994 [Acts 1994, ch. 992, § 3.]

Tennessee Code Annotated § 4-3-5503, effective May 10, 1994 [Acts 1994, ch. 992, § 4.]

OBJECTIVES:

1. Ensure continuous efforts to secure information systems authorized by the “Comprehensive National Cyber-security Initiative” of the United States and the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23).
2. Ensure connectivity for state agency systems and access to data maintained by all state departments, agencies, commissions, or boards.
3. Protect the networks serving, and the data concerning, the citizens of the State of Tennessee from unauthorized access, disruption, and/or corruption, and ensure efficiencies and network availability.
4. Ensure the security and privacy of protected health information mandated by federal law under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and ensure that the State's network infrastructure controls are compliant with the HITECH Act of 2009.
5. Ensure improved network efficiencies, availability and security.
6. Ensure enhanced security by the establishment and enforcement of standards and standard desktop configurations.
7. Implement a fully developed statewide security policy to protect the security and privacy of the State's data and the operations of government and those it serves.
8. Ensure the efficiencies offered by single State agency management of the security of network related system are maximized, under the Office for Information Resources (OIR) of the Department of Finance and Administration as it is best positioned, equipped and authorized to perform these functions.
9. Promote efficiencies to ensure the existing rate structure for Local Area Network (LAN) and Wide Area Network (WAN) nodal fees provide sufficient capacity to implement this policy.

ISC – Information Resources Policies

SCOPE:

This network infrastructure support and maintenance policy includes all information technology resources and associated network infrastructure components, including the strategies, policies, standards, procedures, and guidelines necessary to assure security of the State's information technology resources, as well as all distributive processing and network related systems; and to serve as a computer service bureau.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Responsible for and authorized to manage and secure the State's networks.
2. Ensured physical access to those areas where network infrastructure is maintained including all circuits, firewalls, intrusion detection systems, and other enterprise network defense systems required to provide connectivity and to manage and/or secure the State's networks and data.
3. Authorized to establish and enforce policy and statewide standards for security, network and internet access, servers (application servers, DNS servers, web servers, etc.) wired or wireless technology, e-mail, web sites, network monitoring, computer technology standards, firewall policy, intrusion detection, authentication, availability of resources, network maintenance, and for handling violations and security incidents for state owned or supported networks.
4. Responsible for identifying or developing guidelines covering cyber awareness literacy, training, and education, including ethical conduct in cyberspace.
5. Responsible for providing the secure, centralized, and standardized management of Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs) including policies and connectivity to enhance the implementation and management of security and thereby reduce time lost to recover from security intrusions, viruses, and "hackers."
6. Responsible for securing the network through the effective and efficient application of resources to make satisfactory network repairs; and should detachment occur, responsible to communicate immediately with the agency to advise it of findings, cause for detachment, and commit resources to work with the agency to assist in satisfactory repair.
7. Provide assistance to and partner with agencies in the creation of guidelines, procedures, training, and tools in order for agencies to conduct self-monitoring and self-assessment.
8. Responsible for and authorized to perform audits on any device that attaches to the State of Tennessee's network or affects cyber security.
9. The State's Chief Information Officer, as a member of the State's Homeland Security Council, is authorized to act in the best interest of the State to assign network priorities in the event of either a homeland security incident, or the catastrophic loss of core network processing capability, and will ensure appropriate dialogue with the Homeland Security Council leadership.

ISC – Information Resources Policies

Agencies and Other Attached Entities

1. Each department, agency, commission, board, local governmental entity, or state supported institution that attaches to the networks managed by OIR shall adhere to all applicable security and disaster recovery policies, standards, and procedures for the State's information systems environment.
2. Information systems security coordinators shall be appointed as department, agency, commission, board, or institution representatives; and, shall be responsible for information systems security coordination.
3. Each department, agency, commission, and board that attaches to the networks managed by OIR shall adhere to standards for server configuration and shall have the configuration reviewed and approved by OIR prior to attaching the server to a network segment, and shall submit to no-notice annual OIR performed audits.
4. Each vendor, subrecipient, or contracting company and their employees doing business with the State and that attaches to OIR managed networks shall adhere to all applicable security and disaster recovery policies, standards, and procedures for the State's information systems environment and shall sign a Network Connectivity Agreement with the OIR.
5. Each department, agency, commission, and board that issues network or system user IDs to employees, contractors, vendors or subrecipients shall obtain a signed State of Tennessee Acceptable Use Policy Network Access rights and Obligations User Agreement annual acknowledgement from each employee, contractor, vendor or subrecipient as a condition of ID issuance.

Exclusions and Exemptions

1. This policy excludes Ultra High Frequency (UHF), Very High Frequency (VHF), 700 MegaHertz radio, and 800 MegaHertz radio ranges, and data wireless communication systems involving law enforcement officers and first responders; car to officer communications, with the exception of wireless Local Area Networks (LANs, 802.11x) that are included within this policy.
2. Non-executive branch agencies, including the Tennessee Bureau of Investigation, the General Assembly, the Judicial Branch, and all Constitutional Officers shall be exempted only from the governance structure defined in this ISC Policy. Exempted entities will maintain similarly stringent network operating system environments to retain full network access privileges, and their procedures, checklists, and performance reports will be reviewed upon request by the Information Systems Council or its designee. The Comptroller's Office will be the Information Systems Council's designee for the General Assembly.

ISC – Information Resources Policies

Policy 14.00: Electronic and Digital Signatures

The manner and format by which electronic and digital signatures will be used in state government will be reviewed and approved by the Office for Information Resources.

Definitions:

Electronic signature – an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Examples of an electronic signature are: a name at the end of an email, clicking a button or downloading content to indicate acceptance of a transaction or certain terms and conditions.

Digital signature – a specific type of electronic signature that relies on the technology of cryptography to authenticate the signer's identity and ensure the integrity of the signed document. A digital signature is bound to the document being signed using a mathematical algorithm such that any modification of the document after it is signed can be detected. (Note: The term document as applied in this policy is used interchangeably with terms such as electronic document, record or transaction.)

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

Tennessee Code Annotated, Section 47-10-118, effective April 11, 2001

Uniform Electronic Transactions Act (UETA).

OBJECTIVES:

1. Ensure that digital signatures are implemented using a standard information technology architecture for interoperability of documents across government.
2. Ensure that documents and/or transactions signed using a digital signature can be reproduced over time to meet statutory requirements.
3. Facilitate online business processes that require a high degree of “trust” (identity authentication) between the parties and the “integrity” of the transaction.
4. Promote the cost effective use of electronic and digital signature technologies to provide business solutions commensurate with the value and risk to the business process.
5. Define the responsibilities of information systems management and users in the use of electronic and digital signature technologies.

ISC – Information Resources Policies

SCOPE:

This policy applies to the use of all electronic and digital signatures regardless of computing platform, type of software utilized (custom developed or commercial off the shelf product), procured, acquired or hosted by a third party.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Develop statewide standards, procedures and guidelines necessary for the implementation of electronic and digital signatures in state government.
2. Provide management and technical consulting to state agencies in planning for and utilizing electronic and digital signature technologies.
3. Provide for the ongoing technical review of electronic and digital signature technologies and legislation in order to forecast changes needed in state policy.
4. Provide for administrative review of the policies, standards, procedures and guidelines in light of technical, procedural, or statutory changes that may occur in the use of electronic and digital signatures.
5. Define the responsibilities of information systems management and users in the use of electronic and digital signature technologies.

Agency

1. Establish agency policies, standards, procedures and guidelines pertaining to the implementation of electronic and digital signatures consistent with statewide policies and standards.
2. Educate users on the policies, standards, procedures and guidelines related to the use of electronic and digital signatures.
3. Provide for agency administrative review of the policies, standards, procedures and guidelines in light of technical, procedural, or statutory changes that may occur in the use of electronic and digital signatures.

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines pertaining to the implementation of electronic and digital signatures in state government.
2. Refrain from behaviors that would expose the confidential nature of authentication and/or integrity components of electronic and digital signature technology to unnecessary or unauthorized risks.

ATTACHMENT B

OIR Research and State Standard Setting Proprietary Purchasing ISC Meeting

Recommendation: That the Information Systems Council, under its authority as set forth in TCA 4-3-5502(1)(E) and 4-3-5504, endorse the Office for Information Resources' research and development process as an acceptable basis for proprietary and sole source procurements.

Background.

The technical environment in the State of Tennessee is vital to the operation of the State and for the effective delivery of services. The rate of change in the technical arena is extremely fast and each of the changes can have a negative impact on the operation of the State technical environment. Research and development (R & D) projects in this area involve the infrastructure of the State where one of the major driving decision points is how well the potential solution works with all other software and network components.

OIR conducts extensive research on new and revised technologies to insure they will work efficiently with the entire network. The research usually leads to one of two decisions:

- the State is not prepared, or the need does not exist, to move into that technical area; or,
- the State has determined that the solution would be feasible and that the implementation of the technology is important.

These projects often lead to establishing standard products that will be used in our State infrastructure.

Project Initiation.

The decision to look at a new product is driven by different events. Each year the departments prepare a three-year information systems planning document. One of the components of this document identifies trends and new technology initiatives needed to meet the departments' business needs. The summary of these needs becomes a major source of new R&D work. Decisions are based also on movement in the market place and new product announcements.

R & D Project Methodology.

The projects are structured to define the functional needs of the technical infrastructure, the architectural requirements needed to work seamlessly in the State environment, the stability of the technology as a whole in the market place, and the level of need in the State. The team also accumulates a list of business and technical issues that must be answered before the technology can be implemented.

The project team defines the functional and architectural requirements of the State for the technology, researches the technology, reviews various research sources and technology journals to understand both the business and technology issues surrounding the specific technology, and prepares a short list of viable marketplace solutions. The solution providers identified on the short list may be requested to demonstrate their products, provide literature on their products, and answer questions the team has about their solutions. The products that appear to meet the State's functional and architectural requirements at this point are evaluated.

Evaluation Process.

The evaluation process focuses on two major areas:

1. Each product is measured against the defined, objective, business requirements.
2. Each product is measured against the established State architectural standards, for compatibility or consistency.

The R&D team produces an evaluation report that identifies the outcomes of the evaluation process. This report also includes a description of the estimated comprehensive project cost, including the initial cost and the ongoing cost of ownership.

An OIR Leadership Team reviews the recommendations to determine if the project should move forward.

Procurement Requests.

If, as a result of the evaluation process described above, more than one product meets the State's business requirements and is determined to be compatible or consistent with State established architectural standards, OIR requests that General Services issue an ITB for the needed product. If, however, as a result of the evaluation process described above, only one product meets the State's requirements, the State makes a proprietary or sole source request to General Services. If only one product meets the State's requirements and the product is available from multiple vendors, it is bid through the proprietary process; if only one source is available, OIR recommends the sole source process.

