REPORT OF THE
DEPARTMENT OF INFORMATION TECHNOLOGY

ANALYSIS OF FEASIBILITY OF AND COST ASSOCIATED WITH REQUIRING PUBLIC BODIES TO COMPILE INDICES OF CERTAIN COMPUTER DATABASES SJR 68

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

SENATE DOCUMENT NO. 10

COMMONWEALTH OF VIRGINIA
RICHMOND
1997

Table of Contents

Executive Summary

Prepared in response to Senate Joint Resolution 68, this report presents a study of the feasibility and associated costs of creating an annual index of state government databases, within certain parameters, as directed by Section 2.1-342 of the Code of Virginia. This section of the Code, modified by Senate Bill 326 (1996 Session), expands upon the current Virginia Freedom of Information Act to incorporate a requirement to index certain computer databases.

The focus of this study is computer resident database files which are also part of the official record. Although the Department of Information Technology (DIT) strongly supports making official information available to the public, this study does not extend itself into the general discussion of Virginia's Freedom of Information Act or Privacy Protection Act. Nor does it extend itself into discussion of any issues raised by passage of SB 326.

Implementation of an index of computer resident database files begs consideration of numerous factors, from the potential for data mining to the cost implications for agencies and, subsequently, the Commonwealth as a whole. This study explores these issues and makes specific recommendations identifying the material which should be indexed and addressing the implications data mining may hold for the Commonwealth.

Developing cost estimates, on the other hand, is more difficult because of the variables involved. Resource allocation depends on factors such as the number of databases to be considered, the complexity of each database and its technological structure. Specific algorithms incorporating these variables must be developed to gain a cost estimate of any accuracy. Therefore, the resource allocation issue is addressed here only in general terms.

Introduction

Purpose

The purpose of this paper is to report on a study of the feasibility of creating a state government database index under Virginia's Freedom of Information Act (FOIA), and to identify issues related to creating that index.

Scope

The Department of Information Technology (DIT), in cooperation with the State Librarian and the State Archivist, was directed by Senate Joint Resolution 68 to study specifically the feasibility of, and costs associated with, creating and maintaining an index of computer databases created before, on or after July 1, 1997 (see language below). Although some language in Section 2.1-342 of the Code of Virginia, which mandates the creation of this index, may raise questions about the process, this study focuses on the specific issues outlined in SJR 68.

It is important to note that the official records to be indexed have always been available under, and within the guidelines of, the FOIA. By providing for a mechanism that lists information which is stored in an electronic database rather than on paper, Va. Code § 2.1-342 simply makes access to this existing information easier.

Implementation of the index involves numerous factors, from the potential for data mining to the cost implications for the Commonwealth. This study addresses that range of issues, touches on similar efforts undertaken by other organizations, outlines recommendations and offers direction for pursuit of an implementation strategy.

Applicable Legislation

FOIA is an integral element of the state government process. Under FOIA, information about government policies and agency processes must be readily available to the public. SB 326, enacted as Chapter 469 of the 1996 Acts of Assembly, amends the Virginia FOIA to require that computer databases of public bodies of state government be indexed, effective July 1, 1997, and includes a specific charge to DIT to develop guidelines for compliance with this requirement. The applicable section reads:

> *Beginning July 1, 1997, every public body of state government shall compile, and annually update, an index of computer databases which contains at a minimum those databases created by them on or after July 1, 1997. "Computer database" means a structured collection of data or documents residing in a computer. Such index shall be an official record and shall include, at a minimum, the following information with respect to each database listed therein:*

a list of data fields, a description of the format or record layout, the date last updated, a list of any data fields to which public access is restricted, a description of each format in which the database can be copied or reproduced using the public body's computer facilities, and a schedule of fees for the production of copies in each available form. The form, context, language, and guidelines for the indices and the databases to be indexed shall be developed by the Director of the Department of Information Technology in consultation with the State Librarian and the State Archivist. The public body shall not be required to disclose its software security, including passwords.

SJR 68 was also passed during the 1996 General Assembly Session, directing DIT to study the feasibility and costs of creating the index, described in somewhat different language. The applicable section reads:

RESOLVED by the Senate, the House of Delegates concurring, That the Director of the Department of Information Technology, in cooperation with the State Librarian and the State Archivist, be requested to study the feasibility of and costs associated with requiring public bodies to compile, and annually update, an index of computer databases maintained or created by them before, on, or after July 1, 1997. "Computer database" means a structured collection of data or documents residing in a database management program or spreadsheet software. Such indices shall include, at a minimum, the following information with respect to each database listed therein: a list of data fields, a description of the format or record layout, information as to the frequency with which the database is updated, a list of any data fields to which public access is restricted, a description of each form in which the database can be copied or reproduced using the public body's computer facilities, and a schedule of fees for the production of copies in each available form.

Background

The Virginia Freedom of Information Act

The Freedom of Information Act requires that "all official records shall be open to inspection and copying by any citizens of the Commonwealth." The requirement applies to all "official records" of public bodies except for official records exempted under the 66 specific categories provided for in FOIA and several other categories provided in other state or federal laws.

Privacy Concerns

The Privacy Protection Act, which was established as law in 1976 in Virginia, is intended primarily to protect individual privacy and ensure that safeguards are in place and adhered to. The pri-

vacy principles dictate that information should not be collected unless there is a clear reason for keeping such information. Also, the ultimate protection is that individuals can have access to information about themselves in order to verify the information's existence as well as its accuracy. In the debate leading to its passage, the General Assembly found:

1. *That an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;*
2. *That the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;*
3. *That an individual's opportunities to secure employment, insurance, credit and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and*
4. *That in order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.*

This was the foundation for the argument that privacy protections were essential for Virginia. The law is designed to protect individuals, providing them with a vehicle to protect their own personal interest against corrupt or inaccurate information. These protections apply to information contained on information systems as well as those in traditional paper formats. With the creation of an index of databases that in many cases contain information about individuals, there is an intuitive fear that privacy rights may be sacrificed or made more vulnerable.

Library of Virginia Inventory System

Official records are required under FOIA to be made available to the public. One of the major state government processes currently in place to provide access to official records is managed through the Library of Virginia. The Library maintains a list of publications produced by Virginia agencies. The collection is published each year and identifies the agency and its publications by title. A similar approach might be used for reporting databases. Instead of addressing paper publications alone, the library might expand the requirement to include the databases which agencies maintain.

Other States and the Federal Government

The interest in creating database indexes in Virginia is not without parallel. Other systems are in place with similar objectives. Among these are:

◆ North Carolina: North Carolina's law was established in 1995. In calling for "the index," the bill prescribes the existence of one set of database documentation standards applying equally to

all state agencies, county and municipal governments, regional authorities, and other custodians of these records. And as agencies collect the specific information required by the bill, they will be collecting basic data needed for both records retention/disposition scheduling and locator-service indexing.

• Florida: The Florida state government also established an index requirement in 1995. As noted by the Florida governor and his cabinet, the rapidly evolving development of information technology, most notably the recent proliferation of resources on and access to the Internet, has opened up unprecedented opportunities for citizen access to electronic government information.

• Federal Government: As part of the federal role in the National Information Infrastructure, the Government Information Locator Service (GILS) identifies and describes information resources throughout the federal government, and provides assistance in obtaining the information. GILS supplements other government and commercial information dissemination mechanisms, and uses international standards for information search and retrieval so that information can be retrieved in a variety of ways. Congress and the Office of Management and Budget directed all federal U.S. agencies to create, and to make available to the public, GILS records on their information holdings. These mandates also directed that agency efforts were to be based on internationally accepted standards for information search and retrieval. GILS efforts are also being implemented in some instances at the state level, by other nations and by international organizations.

Discussion of Fundamental Issues

What is SB 326 and What Information is Affected?

Senate Bill 326 amends Section 2.1-342 of the Code of Virginia to expand the existing Virginia Freedom of Information Act to include the requirement to index certain computer databases.

What are the Specific Requirements?

Essentially, Va. Code § 2.1-342 states that starting July 1, 1997 each public body of Virginia state government will create an index of databases that are "created" on or after July 1, 1997. The index, to be updated annually and maintained as an official record, is to include several specific items of information to aid in identifying the content of the database:

1. list of data fields,
2. description of the format or record layout,
3. date last updated,
4. list of any data fields to which public access is restricted,

5. description of each format in which the database can be copied or reproduced using the public body's computer facilities, and

6. schedule of fees for the production of copies in each available form.

Much of the information called for in the above six categories is highly technical and would be difficult for the general public to understand. It may be more appropriate to change this requirement to reflect a brief narrative description of the database and its contents as opposed to the current level of detail. Item two, "description of the format or record layout," also poses a potential security risk: Making public a detailed description of a database structure exposes that database to hackers in much the same way that publicizing a blueprint makes a bank vault vulnerable to a thief. It would be useful for the guidelines to take that into account. Security risks in general are discussed further below in "What Security Risks Does Indexing Pose to Agencies?"

Further, when applying the above requirements to the complex variety of databases in state government, it becomes clear that, for effective and consistent indexing, several terms must be clarified. Many of these would probably be most effectively addressed in developing procedures for the index. Areas which beg definition include:

◆ The meaning of "created on or after July 1, 1997." The information in most databases changes constantly. Is a database considered "new" only if it never existed before July 1, 1997? What if a certain percentage of the data it contains is new since that date? What if the software used to organize the data is changed or updated?

Va. Code § 2.1-342 is silent on any requirement to index existing databases, but one might argue that at some point a significantly modified or redesigned database might be construed as having been "recreated."

◆ What is a database? Va. Code § 2.1-342 defines "computer database" as "a structured collection of data or documents residing in a computer;" this broad definition could be construed as almost any collection of data, from clip art collections to desk organizers, with potentially burdensome implications for complying bodies. A narrower definition would be helpful, and in fact, one already exists in the Code. According to Va. Code § 42.1-77, "'Database' means a set of data, consisting of one file or a group of integrated files, maintained as an information system managed by a database management system." This definition might be useful in a practical interpretation of indexing requirements.

What are the Implications for Data Mining?

"Data mining" refers to the concept of integrating two or more unrelated data sets through a relatively sophisticated process to discover correlations between those data sets that represents new information. The basic methods used to pursue these types of correlations range from simple queries to join data sets, to the use of neural network and fuzzy logic concepts. Over the past few years the availability of tools and processes which make this activity attractive have increased substantially.

This issue is addressed here to draw attention to the potential risks which may exist when two or more data sets acquired from the Commonwealth through FOIA are combined in a data mining process. The result may be new data that the government did not originally intend to create or make available, or claims of unquestionable reliability for the data created because of the unimpeachable source (i.e., the Commonwealth).

It is not the process itself which poses the risk. It is the intended use of the resulting product that should be examined. The Code requires that only data necessary to support a specific function be collected as it is relative to that function. Further, the PPA states that personal information can be released only if it is required or permitted by law to be released or necessary to accomplish a proper purpose of the agency, (Va. Code § 2.1-380). The code defines personal information as:

> *...all information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.*

Within this context, data collected to support an approved activity within the Department of Motor Vehicles could easily have fields which are similar, if not identical, to fields collected to support a Department of Health activity. The two activities may have no relationship at all. But once databases are identified through indices, an organization or individual could apply data mining processes to create a new correlation which supports an activity that has nothing to do with the

original intent of either department or the approved activities for which the data was collected. Three hypothetical examples:

Name of Virginians who graduated from certain colleges + occupations and salary information from PMIS could yield a result indicating that Virginians who attend certain schools receive lower-paying state jobs.

Records of traffic safety course attendee addresses + drug and alcohol program attendee addresses could yield information on Virginians charged with DUI.

Data from waste management about landfill locations + data from the health department on addresses of people with certain diseases could yield a correlation of risk to people living near landfills.

Data mining that targets areas such as spending practices, voting patterns and financial standing opens a new and growing threat to citizen privacy. Of course, the data has always existed as records on paper or film, but the cost of manipulating it manually was generally prohibitive. Now, large sets of easily manipulated electronic data yield fast analytical results with a relatively minor investment in computer hardware and software.

The intent of this discussion is not to dissuade the reader from supporting enhancements to the FOIA, but to outline this new and substantial risk.

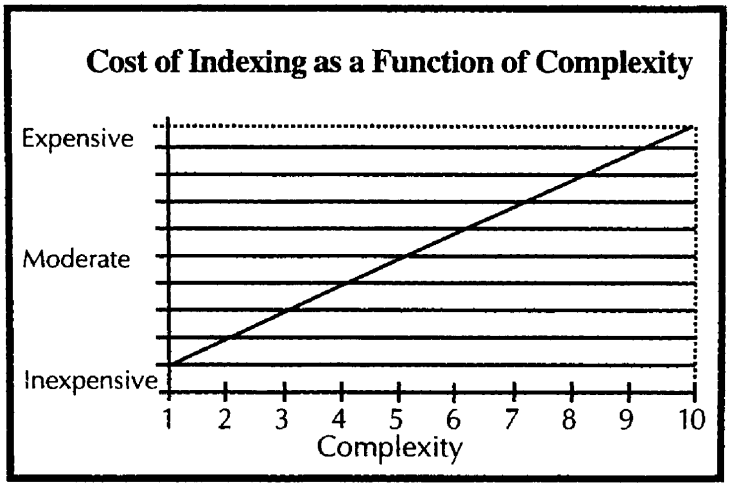
What are the Implications for Privacy Protection?

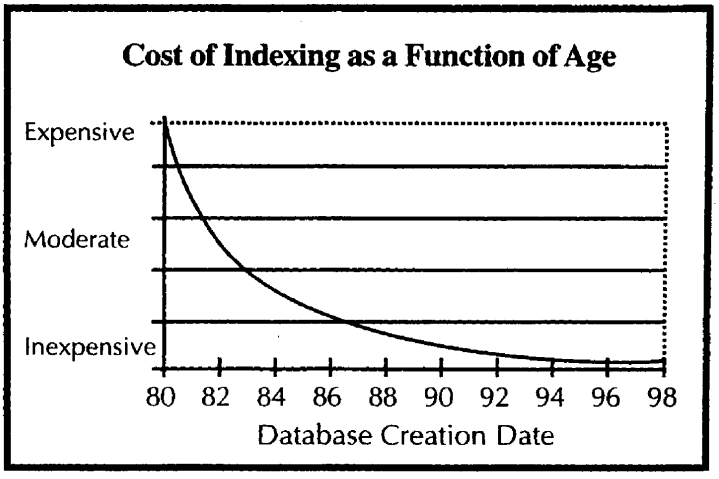
Privacy protection concerns have been raised in connection with Va. Code § 2.1-342. However, with the exception of the data mining issue outlined above, the bill appears to pose no increased risk to citizen privacy, since information contained in databases, like all state records, will be released according to existing FOIA and PPA guidelines.

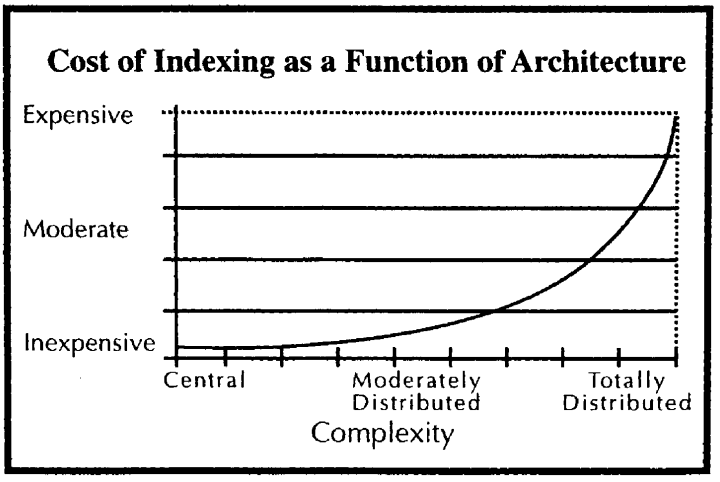
What are the Resource Implications of Indexing?

Resource allocation depends in part on whether or not indexing is restricted to databases created on or after July 1, 1997, on the definition of a "new" database (see discussion on page 7), and on several other factors. The resources required to implement indexing are strongly affected by the effective date of the effort. If databases created prior to July 1, 1997 are to be indexed, the number of databases and, therefore, the implementation cost, will be significantly higher.

Examples of Index Cost Drivers







Regardless of the effective date, developing models to estimate necessary resources is difficult because of the variables involved. Estimates depend on factors such as the number of databases an agency maintains; the complexity of each database; the technology used to maintain it; and

the rate at which information contained in each database is refreshed. To accurately arrive at detailed cost estimates, agencies must define the multiple variables and create an algorithm based on a simultaneous linear equation problem. The three models in Appendix A will serve as a rough estimator for agencies interested in broaching the actual cost of resource allocation.

What Security Risks Does Indexing Pose to Agencies?

Releasing indexed descriptions of underlying electronic file structures or granting, perhaps eventually, on-line access to databases raises the issue of security risks. The risks range from revealing file structures, which can then be exploited, to allowing data mining, which can lead to misuse of acquired information. There is merit in such concerns. Although computer hackers have always been a threat to the integrity of electronic information, an index describing how a database is housed and structured makes illegal entry even easier. However, these concerns can be addressed.

There is, in the computing industry, a generally accepted knowledge of the vulnerabilities of various file systems and their access procedures. The reality of these risks can be illustrated through a brief discussion of several of the vulnerabilities known to exist under UNIX system environments, one of the most widely used for database creation and storage.

Recently, Bob Gallen and Lee Sutterfield discussed the most common vulnerabilities of UNIX systems in the article "Network Security Points of Failure" (UNIX Review, November 1996). A few examples of vulnerabilities that are the "targets of choice for most intrusion attacks:"

TELNET: While TELNET itself is not considered vulnerable to attack, its control or access mechanisms are. Lax configuration implementation by the system administrator makes the use of "sniffers" by hackers very effective in catching user passwords and log-on identifications to gain access to otherwise inaccessible files.

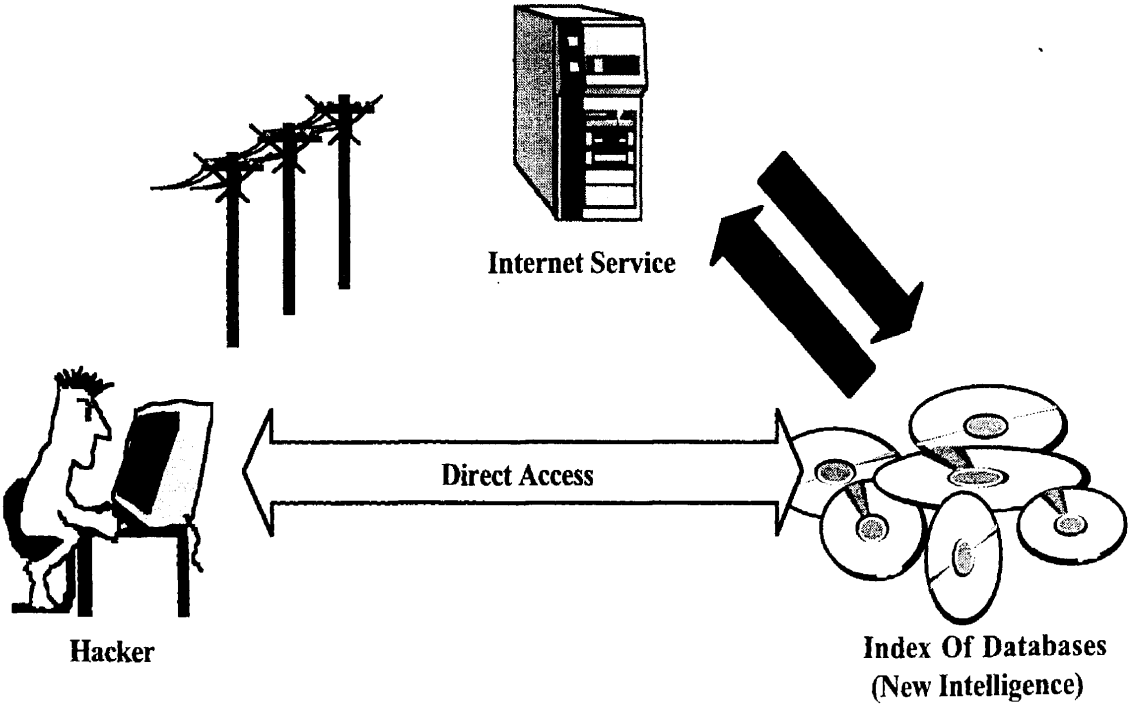
File Transfer Protocol: Again the risk is derived from less-than-stringent configuration by a system administrator, which leads to remote access on files residing on file servers which in turn escalates to further accesses to ever deeper privileges in a UNIX system.

Simple Mail Transfer Protocol: This protocol is very popular because it is associated with the "Send Mail Program." The send mail program has a history of vulnerabilities and subsequent attempts to plug the holes. The program fixes to plug holes commonly referred to as patches typically follow a discovered vulnerability which has been exploited by someone for other than official use. A common practice is to enclose an executable program script in the

mail portion and then cause the mail server to execute the script. A favorite script technique is to make the server return to the mail originator a copy of the system password file.

Even systems thought to be much more secure in their architectures and environments, such as IBM's MVS system, are still vulnerable to misuse, not so much from a hacker element as from lax administration and handling of user passwords and identifications or practices such as leaving terminals turned on, actively logged in, and unattended. An MVS system can be hacked by an outside presence just as handily as a UNIX system if the hacker discovers or is passed the information required to access application files.

Potential Computer Hacking Scenario



In short, indexing presents the same threat – although, perhaps, from a different direction – that most on-line database managers already face daily. These security risks are not insurmountable. Most can be overcome by a disciplined approach to system security that becomes a natural habit for conducting daily business. Admittedly, it requires effort to reach that point, but security concerns can be addressed by insisting that electronic security measures be firmly integrated into the implementation instructions for an indexing system.

Conclusion and Recommendations

A "feasible" task is defined as one which is possible, suitable and logical. Without consideration of resources, it is certainly possible to index all state databases. However, whether it is suitable and logical to do so –particularly in terms of what it will cost and what resources must be allocated – depends largely on how certain key terms are defined, and how the procedures for developing and implementing the index are written. In order for indexing to be feasible, these terms must be consistently and precisely defined, through procedural guidelines or by other means. Further, there are related issues to be addressed, specifically that of data mining.

To this end, DIT recommends that the General Assembly consider:

• That the definition of database found in Va. Code § 42.1-77 be used when discussing indexing. This section defines database as "...a set of data, consisting of one file or a group of integrated files, maintained as an information system managed by a database management system." This description clarifies the legislation's intent by providing a practical and practicable "universe" of items to draw from.

• That the guidelines for implementation of the index appropriately construe the term "created," as this definition will have significant impact on which records are affected. DIT recommends basing this definition on the Council on Information Management's (CIM) models for information systems development projects. CIM Guidelines 91-3, 91-4 and 91-5 include a specific decision point before design proceeds which would be an appropriate point for determining the "creation" of a new database.

• That the guidelines resulting from Va. Code § 2.1-342, amended, incorporate a requirement for a "plain English" description of the database and its contents and delete the requirements relating to data fields and record formats and layouts. Doing so would provide the general public with more useful information with the least possible risk of security.

• That regarding the effective date of this legislation, the General Assembly not direct agencies to index existing databases, as cost would be prohibitive. DIT recommends that only databases created on or after July 1, 1997 be affected.

Appendix A

Cost Models

APPENDIX A
Cost Models

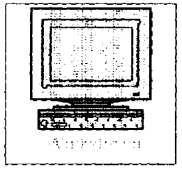
This Appendix contains three models offered as examples of how an agency may approach the task of determining a reasonable estimate of the cost to index databases as envisioned under the amended Freedom of Information Act. The objective in using these models is primarily to establish a baseline common to all agencies and thereby present a resulting estimate that will have meaning to all who review the results.

The models provided speak to three fundamental environments which all assume electronic or computer based databases. The first portrays the most simplistic environment where the databases are resident on a single workstation which is not networked within the agency and dependent on shared resources. The second model looks at locally networked environments where resources are shared. In this case, qualifying data bases will reside not only on individual workstations, but also in a shared environment on agency servers. The third environment looks at the case of agency databases residing on centralized computing resources either at the State level as with the Department of Information Technology but also on other contractually acquired computing service centers which require cost recovery or fees for service.

There appears to be general agreement in discussions with parties contacted that this effort will require a large degree of dedicated effort. A consensus of the level of that effort and therefore the identification of a specific grade level to be assigned is not possible to specify at this point. Accordingly, for the purpose of this effort, two assumptions are proposed. One is that for a continuing effort of administration and maintenance of an Index, an agency will have to assign sufficient personnel resources. The level of the resource will have to be determined by each individual agency. The second assumption is predicated on the concept that in preparing new databases, the design effort will require the construction of links to the new database to those fields, table rows or columns that are either eligible or exempt for disclosure under FOIA. Experience shows that in new system development efforts, the costs range from a low of $30.00 per hour to a high of $125.00 per hour by consulting firms in private enterprise. Taking a midrange of these costs, an arbitrary cost of $70.00 per hour is assigned.

The cost elements and construction of the model algorithms are expected to be subject to modification. Only experience over time will attest to the true costs to be expected from implementation of the requirement to Index the databases.

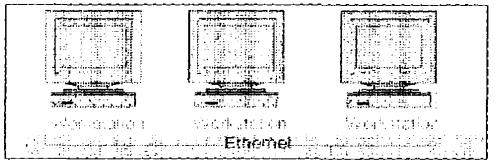
Cost Estimation Models for Implementation of an Index of Databases



Data Bases on Single Workstation

Cost Elements:	
Hours of effort*	(a)
Cost per hour**	(b)
Cost to administer and maintain	(c)

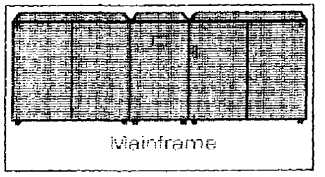
Algorithm:
(a* b) + c = estimated cost



Data Bases on Local Area Networks

Cost Elements:	
Hours of effort*	(a)
Cost per hour	(b)
Cost of additional software license	((s)
Cost of additional hardware	(h)
Cost to administer and maintain	(c)

Algorithm:
(a * b)+ (s + h + c) = estimated cost



Data Bases on Central Computer Systems with Cost Recovery or Fee for Service

Cost Elements:	
Hours of effort*	(a)
Cost per hour	(b)
Cost to compile	(c1)
Cost to test	(c2)
Cost to store	(c3)
Cost to execute	(c4)
Cost to administer	(c5)
Order of magnitude of effort compared to other configurations	(m)

Algorithm:
(a * b) + (c1 + c2 + c3 + c4 + c5)(m) = estimated cost

Notes:
* Effort is considered to include:
1. Building a table/inventory of databases
2. Review of each and building a table of data fields for each database
3. Identify each field as exempt or eligible under FOIA
4. Build an Index Data Base

** Cost per hour is based on:
1. The level of the resource will have to be determined by each individual agency.
2. An average of $70.00 per hour for a Systems Development effort to develop the index table for new databases created on or after July 1, 1997

Appendix B

Chapter 469, An Act to amend and reenact § 2.1-342 of the Code of Virginia, relating to the Virginia Freedom of Information Act; index of certain computer databases required.

CHAPTER 469

An Act to amend and reenact § 2.1-342 of the Code of Virginia, relating to the Virginia Freedom of Information Act; index of certain computer databases required.

[S 326]

Approved April 1, 1996

Be it enacted by the General Assembly of Virginia:

1. That § 2.1-342 of the Code of Virginia is amended and reenacted as follows:

§ 2.1-342. Official records to be open to inspection; procedure for requesting records and responding to request; charges; exceptions to application of chapter.

A. Except as otherwise specifically provided by law, all official records shall be open to inspection and copying by any citizens of the Commonwealth during the regular office hours of the custodian of such records. Access to such records shall not be denied to citizens of the Commonwealth, representatives of newspapers and magazines with circulation in the Commonwealth, and representatives of radio and television stations broadcasting in or into the Commonwealth. The custodian of such records shall take all necessary precautions for their preservation and safekeeping. Any public body covered under the provisions of this chapter shall make an initial response to citizens requesting records open to inspection within five work days after the receipt of the request by the public body which is the custodian of the requested records. Such citizen request shall designate the requested records with reasonable specificity. A specific reference to this chapter by the requesting citizen in his request shall not be necessary to invoke the provisions of this chapter and the time limits for response by the public body. The response by the public body within such five work days shall be one of the following responses:

1. The requested records shall be provided to the requesting citizen.

2. If the public body determines that an exemption applies to all of the requested records, it may refuse to release such records and provide to the requesting citizen a written explanation as to why the records are not available with the explanation making specific reference to the applicable Code sections which make the requested records exempt.

3. If the public body determines that an exemption applies to a portion of the requested records, it may delete or excise that portion of the records to which an exemption applies, but shall disclose the remainder of the requested records and provide to the requesting citizen a written explanation as to why these portions of the record are not available to the requesting citizen with the explanation making specific reference to the applicable Code sections which make that portion of the requested records exempt. Any reasonably segregatable portion of an official record shall be provided to any person requesting the record after the deletion of the exempt portion.

4. If the public body determines that it is practically impossible to provide the requested records or to determine whether they are available within the five-work-day period, the public body shall so inform the requesting citizen and shall have an additional seven work days in which to provide one of the three preceding responses.

Nothing in this section shall prohibit any public body from petitioning the appropriate court for additional time to respond to a request for records when the request is for an extraordinary volume of records and a response by the public body within the time required by this chapter will prevent the public body from meeting its operational responsibilities. Before proceeding with this petition, however, the public body shall make reasonable efforts to reach an agreement with the requester concerning the production of the records requested.

The public body may make reasonable charges for the copying, search time and computer time expended in the supplying of such records. The public body may also make a reasonable charge for preparing documents produced from a geographic information system at the request of anyone other than the owner of the land that

is the subject of the request. However, such charges shall not exceed the actual cost to the public body in supplying such records or documents, except that the public body may charge, on a pro rata per acre basis, for the cost of creating topographical maps developed by the public body, for such maps or portions thereof, which encompass a contiguous area greater than fifty acres. Such charges for the supplying of requested records shall be estimated in advance at the request of the citizen. The public body may require the advance payment of charges which are subject to advance determination.

In any case where a public body determines in advance that search and copying charges for producing the requested documents are likely to exceed $200, the public body may, before continuing to process the request, require the citizen requesting the information to agree to payment of an amount not to exceed the advance determination by five percent. The period within which the public body must respond under this section shall be tolled for the amount of time that elapses between notice of the advance determination and the response of the citizen requesting the information.

Official records maintained by a public body on a computer or other electronic data processing system which are available to the public under the provisions of this chapter shall be made reasonably accessible to the public at reasonable cost. *Beginning July 1, 1997, every public body of state government shall compile, and annually update, an index of computer databases which contains at a minimum those databases created by them on or after July 1, 1997. "Computer database" means a structured collection of data or documents residing in a computer. Such index shall be an official record and shall include, at a minimum, the following information with respect to each database listed therein: a list of data fields, a description of the format or record layout, the date last updated, a list of any data fields to which public access is restricted, a description of each format in which the database can be copied or reproduced using the public body's computer facilities, and a schedule of fees for the production of copies in each available form. The form, context, language, and guidelines for the indices and the databases to be indexed shall be developed by the Director of the Department of Information Technology in consultation with the State Librarian and the State Archivist. The public body shall not be required to disclose its software security, including passwords.*

Public bodies shall not be required to create or prepare a particular requested record if it does not already exist. Public bodies may, but shall not be required to, abstract or summarize information from official records or convert an official record available in one form into another form at the request of the citizen. The public body shall make reasonable efforts to reach an agreement with the requester concerning the production of the records requested.

Failure to make any response to a request for records shall be a violation of this chapter and deemed a denial of the request.

B. The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

1. Memoranda, correspondence, evidence and complaints related to criminal investigations; adult arrestee photographs when necessary to avoid jeopardizing an investigation in felony cases until such time as the release of such photograph will no longer jeopardize the investigation; reports submitted to the state and local police, to investigators authorized pursuant to § 53.1-16 and to the campus police departments of public institutions of higher education as established by Chapter 17 (§ 23-232 et seq.) of Title 23 in confidence; portions of records of local government crime commissions that would identify individuals providing information about crimes or criminal activities under a promise of anonymity; records of local police departments relating to neighborhood watch programs that include the names, addresses, and operating schedules of individual participants in the program that are provided to such departments under a promise of confidentiality; and all records of persons imprisoned in penal institutions in the Commonwealth provided such records relate to the imprisonment. Information in the custody of law-enforcement officials relative to the identity of any individual other than a juvenile who is arrested and charged, and the status of the charge or arrest, shall not be excluded from the provisions of this chapter.

Criminal incident information relating to felony offenses shall not be excluded from the provisions of this chapter; however, where the release of criminal incident information is likely to jeopardize an ongoing criminal

investigation or the safety of an individual, cause a suspect to flee or evade detection, or result in the destruction of evidence, such information may be withheld until the above-referenced damage is no longer likely to occur from release of the information.

2. (Effective until July 1, 1996) Confidential records of all investigations of applications for licenses and permits, and all licensees and permittees made by or submitted to the Alcoholic Beverage Control Board, the State Lottery Department or the Virginia Racing Commission.

2. (Effective July 1, 1996) Confidential records of all investigations of applications for licenses and permits, and all licensees and permittees made by or submitted to the Alcoholic Beverage Control Board, the State Lottery Department, the Virginia Racing Commission, or the Charitable Gaming Commission.

3. State income, business, and estate tax returns, personal property tax returns, scholastic records and personnel records containing information concerning identifiable individuals, except that such access shall not be denied to the person who is the subject thereof, and medical and mental records, except that such records can be personally reviewed by the subject person or a physician of the subject person's choice; however, the subject person's mental records may not be personally reviewed by such person when the subject person's treating physician has made a part of such person's records a written statement that in his opinion a review of such records by the subject person would be injurious to the subject person's physical or mental health or well-being.

Where the person who is the subject of medical records is confined in a state or local correctional facility, the administrator or chief medical officer of such facility may assert such confined person's right of access to the medical records if the administrator or chief medical officer has reasonable cause to believe that such confined person has an infectious disease or other medical condition from which other persons so confined need to be protected. Medical records shall be reviewed only and shall not be copied by such administrator or chief medical officer. The information in the medical records of a person so confined shall continue to be confidential and shall not be disclosed to any person except the subject by the administrator or chief medical officer of the facility or except as provided by law.

For the purposes of this chapter such statistical summaries of incidents and statistical data concerning patient abuse as may be compiled by the Commissioner of the Department of Mental Health, Mental Retardation and Substance Abuse Services shall be open to inspection and releasable as provided in subsection A of this section. No such summaries or data shall include any patient-identifying information. Where the person who is the subject of scholastic or medical and mental records is under the age of eighteen, his right of access may be asserted only by his guardian or his parent, including a noncustodial parent, unless such parent's parental rights have been terminated or a court of competent jurisdiction has restricted or denied such access. In instances where the person who is the subject thereof is an emancipated minor or a student in a state-supported institution of higher education, such right of access may be asserted by the subject person.

4. Memoranda, working papers and correspondence (i) held by or requested from members of the General Assembly or the Division of Legislative Services or (ii) held or requested by the office of the Governor or Lieutenant Governor, Attorney General or the mayor or other chief executive officer of any political subdivision of the Commonwealth or the president or other chief executive officer of any state-supported institution of higher education. This exclusion shall not apply to memoranda, studies or other papers held or requested by the mayor or other chief executive officer of any political subdivision which are specifically concerned with the evaluation of performance of the duties and functions of any locally elected official and were prepared after June 30, 1992 nor shall this exclusion apply to agenda packets prepared and distributed to public bodies for use at a meeting.

Except as provided in § 30-28.18, memoranda, working papers and correspondence of a member of the General Assembly held by the Division of Legislative Services shall not be released by the Division without the prior consent of the member.

5. Written opinions of the city, county and town attorneys of the cities, counties and towns in the Commonwealth and any other writing protected by the attorney-client privilege.

6. Memoranda, working papers and records compiled specifically for use in litigation or as a part of an active administrative investigation concerning a matter which is properly the subject of an executive or closed meeting under § 2.1-344 and material furnished in confidence with respect thereto.

7. Confidential letters and statements of recommendation placed in the records of educational agencies or institutions respecting (i) admission to any educational agency or institution, (ii) an application for employment, or (iii) receipt of an honor or honorary recognition.

8. Library records which can be used to identify both (i) any library patron who has borrowed material from a library and (ii) the material such patron borrowed.

9. Any test or examination used, administered or prepared by any public body for purposes of evaluation of (i) any student or any student's performance, (ii) any employee or employment seeker's qualifications or aptitude for employment, retention, or promotion, or (iii) qualifications for any license or certificate issued by any public body.

As used in this subdivision 9, "test or examination" shall include (i) any scoring key for any such test or examination, and (ii) any other document which would jeopardize the security of such test or examination. Nothing contained in this subdivision 9 shall prohibit the release of test scores or results as provided by law, or limit access to individual records as is provided by law. However, the subject of such employment tests shall be entitled to review and inspect all documents relative to his performance on such employment tests.

When, in the reasonable opinion of such public body, any such test or examination no longer has any potential for future use, and the security of future tests or examinations will not be jeopardized, such test or examination shall be made available to the public. However, minimum competency tests administered to public school children shall be made available to the public contemporaneously with statewide release of the scores of those taking such tests, but in no event shall such tests be made available to the public later than six months after the administration of such tests.

10. Applications for admission to examinations or for licensure and scoring records maintained by the Department of Health Professions or any board in that department on individual licensees or applicants. However, such material may be made available during normal working hours for copying, at the requester's expense, by the individual who is the subject thereof, in the offices of the Department of Health Professions or in the offices of any health regulatory board, whichever may possess the material.

11. Records of active investigations being conducted by the Department of Health Professions or by any health regulatory board in the Commonwealth.

12. Memoranda, legal opinions, working papers and records recorded in or compiled exclusively for executive or closed meetings lawfully held pursuant to § 2.1-344.

13. Reports, documentary evidence and other information as specified in §§ 2.1-373.2 and 63.1-55.4.

14. Proprietary information gathered by or for the Virginia Port Authority as provided in § 62.1-132.4 or § 62.1-134.1.

15. Contract cost estimates prepared for the confidential use of the Department of Transportation in awarding contracts for construction or the purchase of goods or services and records, documents and automated systems prepared for the Department's Bid Analysis and Monitoring Program.

16. Vendor proprietary information software which may be in the official records of a public body. For the purpose of this section, "vendor proprietary software" means computer programs acquired from a vendor for purposes of processing data for agencies or political subdivisions of the Commonwealth.

17. Data, records or information of a proprietary nature produced or collected by or for faculty or staff of state

institutions of higher learning, other than the institutions' financial or administrative records, in the conduct of or as a result of study or research on medical, scientific, technical or scholarly issues, whether sponsored by the institution alone or in conjunction with a governmental body or a private concern, where such data, records or information has not been publicly released, published, copyrighted or patented.

18. Financial statements not publicly available filed with applications for industrial development financings.

19. Lists of registered owners of bonds issued by a political subdivision of the Commonwealth, whether the lists are maintained by the political subdivision itself or by a single fiduciary designated by the political subdivision.

20. Confidential proprietary records, voluntarily provided by private business pursuant to a promise of confidentiality from the Department of Economic Development, the Virginia Economic Development Partnership, or local or regional industrial or economic development authorities or organizations, used by the Department, the Partnership, or such entities for business, trade and tourism development; and memoranda, working papers or other records related to businesses that are considering locating or expanding in Virginia, prepared by the Partnership, where competition or bargaining is involved and where, if such records are made public, the financial interest of the governmental unit would be adversely affected.

21. Information which was filed as confidential under the Toxic Substances Information Act (§ 32.1-239 et seq.), as such Act existed prior to July 1, 1992.

22. Documents as specified in § 58.1-3.

23. Confidential records, including victim identity, provided to or obtained by staff in a rape crisis center or a program for battered spouses.

24. Computer software developed by or for a state agency, state-supported institution of higher education or political subdivision of the Commonwealth.

25. Investigator notes, and other correspondence and information, furnished in confidence with respect to an active investigation of individual employment discrimination complaints made to the Department of Personnel and Training; however, nothing in this section shall prohibit the disclosure of information taken from inactive reports in a form which does not reveal the identity of charging parties, persons supplying the information or other individuals involved in the investigation.

26. Fisheries data which would permit identification of any person or vessel, except when required by court order as specified in § 28.2-204.

27. Records of active investigations being conducted by the Department of Medical Assistance Services pursuant to Chapter 10 (§ 32.1-323 et seq.) of Title 32.1.

28. Documents and writings furnished by a member of the General Assembly to a meeting of a standing committee, special committee or subcommittee of his house established solely for the purpose of reviewing members' annual disclosure statements and supporting materials filed under § 2.1-639.40 or of formulating advisory opinions to members on standards of conduct, or both.

29. Customer account information of a public utility affiliated with a political subdivision of the Commonwealth, including the customer's name and service address, but excluding the amount of utility service provided and the amount of money paid for such utility service.

30. Investigative notes and other correspondence and information furnished in confidence with respect to an investigation or conciliation process involving an alleged unlawful discriminatory practice under the Virginia Human Rights Act (§ 2.1-714 et seq.); however, nothing in this section shall prohibit the distribution of information taken from inactive reports in a form which does not reveal the identity of the parties involved or other persons supplying information.

31. Investigative notes; proprietary information not published, copyrighted or patented; information obtained from employee personnel records; personally identifiable information regarding residents, clients or other recipients of services; and other correspondence and information furnished in confidence to the Department of Social Services in connection with an active investigation of an applicant or licensee pursuant to Chapters 9 (§ 63.1-172 et seq.) and 10 (§ 63.1-195 et seq.) of Title 63.1; however, nothing in this section shall prohibit disclosure of information from the records of completed investigations in a form that does not reveal the identity of complainants, persons supplying information, or other individuals involved in the investigation.

32. Reports, manuals, specifications, documents, minutes or recordings of staff meetings or other information or materials of the Virginia Board of Corrections, the Virginia Department of Corrections or any institution thereof to the extent, as determined by the Director of the Department of Corrections or his designee or of the Virginia Board of Youth and Family Services, the Virginia Department of Youth and Family Services or any facility thereof to the extent as determined by the Director of the Department of Youth and Family Services, or his designee, that disclosure or public dissemination of such materials would jeopardize the security of any correctional or juvenile facility or institution, as follows:

(i) Security manuals, including emergency plans that are a part thereof;

(ii) Engineering and architectural drawings of correctional and juvenile facilities, and operational specifications of security systems utilized by the Departments, provided the general descriptions of such security systems, cost and quality shall be made available to the public;

(iii) Training manuals designed for correctional and juvenile facilities to the extent that they address procedures for institutional security, emergency plans and security equipment;

(iv) Internal security audits of correctional and juvenile facilities, but only to the extent that they specifically disclose matters described in (i), (ii), or (iii) above or other specific operational details the disclosure of which would jeopardize the security of a correctional or juvenile facility or institution;

(v) Minutes or recordings of divisional, regional and institutional staff meetings or portions thereof to the extent that such minutes deal with security issues listed in (i), (ii), (iii), and (iv) of this subdivision;

(vi) Investigative case files by investigators authorized pursuant to § 53.1-16; however, nothing in this section shall prohibit the disclosure of information taken from inactive reports in a form which does not reveal the identity of complainants or charging parties, persons supplying information, confidential sources, or other individuals involved in the investigation, or other specific operational details the disclosure of which would jeopardize the security of a correctional or juvenile facility or institution; nothing herein shall permit the disclosure of materials otherwise exempt as set forth in subdivision 1 of subsection B of this section;

(vii) Logs or other documents containing information on movement of inmates, juvenile clients or employees; and

(viii) Documents disclosing contacts between inmates, juvenile clients and law-enforcement personnel.

Notwithstanding the provisions of this subdivision, reports and information regarding the general operations of the Departments, including notice that an escape has occurred, shall be open to inspection and copying as provided in this section.

33. Personal information, as defined in § 2.1-379, (i) filed with the Virginia Housing Development Authority concerning individuals who have applied for or received loans or other housing assistance or who have applied for occupancy of or have occupied housing financed, owned or otherwise assisted by the Virginia Housing Development Authority, (ii) concerning persons participating in or persons on the waiting list for federally funded rent-assistance programs, or (iii) filed with any local redevelopment and housing authority created pursuant to § 36-4 concerning persons participating in or persons on the waiting list for housing assistance programs funded by local governments or by any such authority. However, access to one's own information

shall not be denied.

34. Documents regarding the siting of hazardous waste facilities, except as provided in § 10.1-1441, if disclosure of them would have a detrimental effect upon the negotiating position of a governing body or on the establishment of the terms, conditions and provisions of the siting agreement.

35. Appraisals and cost estimates of real property subject to a proposed purchase, sale or lease, prior to the completion of such purchase, sale or lease.

36. Records containing information on the site specific location of rare, threatened, endangered or otherwise imperiled plant and animal species, natural communities, caves, and significant historic and archaeological sites if, in the opinion of the public body which has the responsibility for such information, disclosure of the information would jeopardize the continued existence or the integrity of the resource. This exemption shall not apply to requests from the owner of the land upon which the resource is located.

37. Official records, memoranda, working papers, graphics, video or audio tapes, production models, data and information of a proprietary nature produced by or for or collected by or for the State Lottery Department relating to matters of a specific lottery game design, development, production, operation, ticket price, prize structure, manner of selecting the winning ticket, manner of payment of prizes to holders of winning tickets, frequency of drawings or selections of winning tickets, odds of winning, advertising, or marketing, where such official records have not been publicly released, published, copyrighted or patented. Whether released, published or copyrighted, all game-related information shall be subject to public disclosure under this chapter upon the first day of sales for the specific lottery game to which it pertains.

38. Official records of studies and investigations by the State Lottery Department of (i) lottery agents, (ii) lottery vendors, (iii) lottery crimes under §§ 58.1-4014 through 58.1-4018, (iv) defects in the law or regulations which cause abuses in the administration and operation of the lottery and any evasions of such provisions, or (v) use of the lottery as a subterfuge for organized crime and illegal gambling where such official records have not been publicly released, published or copyrighted. All studies and investigations referred to under subdivisions (iii), (iv) and (v) shall be subject to public disclosure under this chapter upon completion of the study or investigation.

39. Those portions of engineering and construction drawings and plans submitted for the sole purpose of complying with the building code in obtaining a building permit which would identify specific trade secrets or other information the disclosure of which would be harmful to the competitive position of the owner or lessee; however, such information shall be exempt only until the building is completed. Information relating to the safety or environmental soundness of any building shall not be exempt from disclosure.

40. [Repealed.]

41. Records concerning reserves established in specific claims administered by the Department of General Services through its Division of Risk Management as provided in Article 5.1 (§ 2.1-526.1 et seq.) of Chapter 32 of this title, or by any county, city, or town.

42. Information and records collected for the designation and verification of trauma centers and other specialty care centers within the Statewide Emergency Medical Care System pursuant to § 32.1-112.

43. Reports and court documents required to be kept confidential pursuant to § 37.1-67.3.

44. [Repealed.]

45. Investigative notes; correspondence and information furnished in confidence with respect to an investigation; and official records otherwise exempted by this chapter or any Virginia statute, provided to or produced by or for the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission; or investigative notes, correspondence, documentation and information furnished and provided to or produced by or for the Department of the State Internal Auditor with respect to an investigation initiated through the State

Employee Fraud, Waste and Abuse Hotline. Nothing in this chapter shall prohibit disclosure of information from the records of completed investigations in a form that does not reveal the identity of complainants, persons supplying information or other individuals involved in the investigation; however, disclosure, unless such disclosure is prohibited by this section, of information from the records of completed investigations shall include, but is not limited to, the agency involved, the identity of the person who is the subject of the complaint, the nature of the complaint, and the actions taken to resolve the complaint. In the event an investigation does not lead to corrective action, the identity of the person who is the subject of the complaint may be released only with the consent of the subject person.

46. Data formerly required to be submitted to the Commissioner of Health relating to the establishment of new or expansion of existing clinical health services, acquisition of major medical equipment, or certain projects requiring capital expenditures pursuant to former § 32.1-102.3:4.

47. Documentation or other information which describes the design, function, operation or access control features of any security system, whether manual or automated, which is used to control access to or use of any automated data processing or telecommunications system.

48. Confidential financial statements, balance sheets, trade secrets, and revenue and cost projections provided to the Department of Rail and Public Transportation, provided such information is exempt under the federal Freedom of Information Act or the federal Interstate Commerce Act or other laws administered by the Interstate Commerce Commission or the Federal Rail Administration with respect to data provided in confidence to the Interstate Commerce Commission and the Federal Railroad Administration.

49. In the case of corporations organized by the Virginia Retirement System, RF&P Corporation and its wholly owned subsidiaries, (i) proprietary information provided by, and financial information concerning, coventurers, partners, lessors, lessees, or investors, and (ii) records concerning the condition, acquisition, disposition, use, leasing, development, coventuring, or management of real estate the disclosure of which would have a substantial adverse impact on the value of such real estate or result in a competitive disadvantage to the corporation or subsidiary.

50. Confidential proprietary records related to inventory and sales, voluntarily provided by private energy suppliers to the Department of Mines, Minerals and Energy, used by that Department for energy contingency planning purposes or for developing consolidated statistical information on energy supplies.

51. Confidential proprietary information furnished to the Board of Medical Assistance Services or the Medicaid Prior Authorization Advisory Committee pursuant to Article 4 (§ 32.1-331.12 et seq.) of Chapter 10 of Title 32.1.

52. Patient level data collected by the Virginia Health Services Cost Review Council and not yet processed, verified, and released, pursuant to § 9-166.7, to the Council by the nonprofit organization with which the Executive Director has contracted pursuant to § 9-166.4.

53. Proprietary, commercial or financial information, balance sheets, trade secrets, and revenue and cost projections provided by a private transportation business to the Virginia Department of Transportation and the Department of Rail and Public Transportation for the purpose of conducting transportation studies needed to obtain grants or other financial assistance under the Intermodal Surface Transportation Efficiency Act of 1991 (P.L. 102-240) for transportation projects, provided such information is exempt under the federal Freedom of Information Act or the federal Interstate Commerce Act or other laws administered by the Interstate Commerce Commission or the Federal Rail Administration with respect to data provided in confidence to the Interstate Commerce Commission and the Federal Railroad Administration. However, the exemption provided by this subdivision shall not apply to any wholly owned subsidiary of a public body.

54. Names and addresses of subscribers to Virginia Wildlife magazine, published by the Department of Game and Inland Fisheries, provided the individual subscriber has requested in writing that the Department not release such information.

55. Reports, documents, memoranda or other information or materials which describe any aspect of security used by the Virginia Museum of Fine Arts to the extent that disclosure or public dissemination of such materials would jeopardize the security of the Museum or any warehouse controlled by the Museum, as follows:

a. Operational, procedural or tactical planning documents, including any training manuals to the extent they discuss security measures;

b. Surveillance techniques;

c. Installation, operation, or utilization of any alarm technology;

d. Engineering and architectural drawings of the Museum or any warehouse;

e. Transportation of the Museum's collections, including routes and schedules; or

f. Operation of the Museum or any warehouse used by the Museum involving the:

(1) Number of employees, including security guards, present at any time; or

(2) Busiest hours, with the maximum number of visitors in the Museum.

56. Reports, documents, memoranda or other information or materials which describe any aspect of security used by the Virginia Department of Alcoholic Beverage Control to the extent that disclosure or public dissemination of such materials would jeopardize the security of any government store as defined in Title 4.1, or warehouse controlled by the Department of Alcoholic Beverage Control, as follows:

(i) Operational, procedural or tactical planning documents, including any training manuals to the extent they discuss security measures;

(ii) Surveillance techniques;

(iii) The installation, operation, or utilization of any alarm technology;

(iv) Engineering and architectural drawings of such government stores or warehouses;

(v) The transportation of merchandise, including routes and schedules; and

(vi) The operation of any government store or the central warehouse used by the Department of Alcoholic Beverage Control involving the:

a. Number of employees present during each shift;

b. Busiest hours, with the maximum number of customers in such government store; and

c. Banking system used, including time and place of deposits.

57. Information required to be provided pursuant to § 54.1-2506.1.

58. Confidential information designated as provided in subsection D of § 11-52 as trade secrets or proprietary information by any person who has submitted to a public body an application for prequalification to bid on public construction projects in accordance with subsection B of § 11-46.

59. All information and records acquired during a review of any child death by the State Child Fatality Review Team established pursuant to § 32.1-283.1.

60. Investigative notes, correspondence, documentation and information provided to or produced by or for the committee or the auditor with respect to an investigation or audit conducted pursuant to § 15.1-765.2. Nothing in this section shall prohibit disclosure of information from the records of completed investigations or audits in a form that does not reveal the identity of complainants or persons supplying information.

61. Financial, medical, rehabilitative and other personal information concerning applicants for or recipients of loan funds submitted to or maintained by the Assistive Technology Loan Fund Authority under Chapter 11 (§ 51.5-53 et seq.) of Title 51.5.

C. Neither any provision of this chapter nor any provision of Chapter 26 (§ 2.1-377 et seq.) of this title shall be construed as denying public access to contracts between a public official and a public body, other than contracts settling public employee employment disputes held confidential as personnel records under subdivision 3 of subsection B of this section, or to records of the position, job classification, official salary or rate of pay of, and to records of the allowances or reimbursements for expenses paid to, any public officer, official or employee at any level of state, local or regional government in the Commonwealth or to the compensation or benefits paid by any corporation organized by the Virginia Retirement System, RF&P Corporation and its wholly owned subsidiaries, to their officers or employees. The provisions of this subsection, however, shall not apply to records of the official salaries or rates of pay of public employees whose annual rate of pay is $10,000 or less.

Go to (General Assembly Home)

Appendix C

Senate Joint Resolution No. 68, Requesting the Director of the Department of Information Technology, in cooperation with the State Librarian and the State Archivist, to study the feasibility of and costs associated with requiring public bodies to compile indices of certain computer databases.

SENATE JOINT RESOLUTION NO. 68

Requesting the Director of the Department of Information Technology, in cooperation with the State Librarian and the State Archivist, to study the feasibility of and costs associated with requiring public bodies to compile indices of certain computer databases.

Agreed to by the Senate, February 13, 1996
Agreed to by the House of Delegates, February 26, 1996

WHEREAS, the General Assembly enacted the Virginia Freedom of Information Act in 1968 to ensure the people of this Commonwealth ready access to the official records of public bodies of the Commonwealth; and

WHEREAS, the Virginia Freedom of Information Act is designed to prevent the affairs of government from being conducted in an atmosphere of secrecy; and

WHEREAS, the public is to be the beneficiary of any action taken at any level of government; and

WHEREAS, the Virginia Freedom of Information Act is to be liberally construed so as to promote an increased awareness by all persons of governmental activities and to afford every opportunity to citizens to witness the operations of government; and

WHEREAS, any exemption or exception from the Virginia Freedom of Information Act is to be narrowly construed in order that no thing which should be public may be hidden from any person; and

WHEREAS, an increasing number of official records of the public bodies of the Commonwealth are created and maintained within computer databases; and

WHEREAS, in keeping with the policy behind the Virginia Freedom of Information Act, the public has a right to know about the existence of such computer databases and the official records that may be contained therein; now, therefore, be it

RESOLVED by the Senate, the House of Delegates concurring, That the Director of the Department of Information Technology, in cooperation with the State Librarian and the State Archivist, be requested to study the feasibility of and costs associated with requiring public bodies to compile, and annually update, an index of computer databases maintained or created by them before, on, or after July 1, 1997. "Computer database" means a structured collection of data or documents residing in a database management program or spreadsheet software. Such indices shall include, at a minimum, the following information with respect to each database listed therein: a list of data fields, a description of the format or record layout, information as to the frequency with which the database is updated, a list of any data fields to which public access is restricted, a description of each form in which the database can be copied or reproduced using the public body's computer facilities, and a schedule of fees for the production of copies in each available form.

The Department of Information Technology shall provide staff support for the study. Technical assistance shall be provided by The Library of Virginia. Upon request, all agencies of the Commonwealth shall provide assistance to the study. The study shall seek the participation and input of local government representatives. The study shall be completed in time to submit a report of findings and recommendations to the Governor and the 1997 Session of the General Assembly as provided in the procedures of the Division of Legislative Automated Systems for the processing of legislative documents.

Appendix D

Current Statutes Governing Information Policy in Virginia, Senate Document No. 40

REPORT OF THE
COUNCIL ON INFORMATION MANAGEMENT ON

CURRENT STATUTES GOVERNING INFORMATION POLICY IN VIRGINIA

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

SENATE DOCUMENT NO. 40

COMMONWEALTH OF VIRGINIA
RICHMOND
1995

COMMONWEALTH of VIRGINIA

COUNCIL ON INFORMATION MANAGEMENT

HUDNALL B. CROASDALE
DIRECTOR

WASHINGTON BUILDING, SUITE 901
1100 BANK STREET
RICHMOND, VIRGINIA 23219
(804) 225-3622

V/TDD: (804) 225-3624
FACSIMILE: (804) 371-7932

January 31, 1995

TO: The Honorable George Allen, Governor of Virginia
Members of the General Assembly

On behalf of the Council on Information Management, I am pleased to provide you with the report called for by Senate Joint Resolution 238 adopted by the General Assembly in January 1993. In carrying out its responsibilities, the Council has received the assistance of the Institute of Bill of Rights Law at The College of William and Mary, as well as policy experts representing the Virginia Citizens Consumer Council, the Virginia Press Association, the National Archives, agencies of state and local government, the Woodrow Wilson International Center for Scholars and the law firm of Fenwick and West.

This report has two distinct purposes. As directed by the General Assembly, the report provides an assessment of the impact of technology on the collection, maintenance, preservation, use and dissemination of information. Further, it examines whether, in an electronic environment, current state law ensures public access to government information, protects the rights of the individual to control information about himself, promotes the accuracy and integrity of public records and protects the taxpayer's investment in collecting, developing, storing and maintaining public records.

In submitting this report for publication, the Council believes it is important to emphasize that, with the advent of advanced information technologies, the process for managing and providing access to public records has become more complex. While the study reveals that current laws, for the most part, are adequate to address these issues, resolving the question of access versus privacy involves a unique set of challenges for the Commonwealth.

Respectfully submitted,

Hud Croasdale

TABLE OF CONTENTS

INTRODUCTION

Information policy clearly constitutes an emerging challenge for public officials in Virginia in the 1990s. Although state and local governments have always recognized their role in managing and providing access to public records, the advent and increasing use of computers and other advanced information technologies have increased the complexity of this task and have revealed ways in which the Commonwealth's information policies can sometimes conflict.

Over the past few years, a number of issues have been raised concerning access to government information, preservation of electronic records, privacy and intellectual property which may call into question the efficacy of Virginia information laws in the electronic age. Because new technology is putting considerable pressure on the laws that were passed to regulate government information policy when government information was recorded primarily on paper, there may be a need to amend those laws in order to make certain that the policies represented in those laws are not lost as that information becomes electronic.

Senate Joint Resolution 238 was adopted by the General Assembly in January 1993. This resolution called for a study to determine whether current law ensures public access to government information, protects the rights of the individual to control information about himself, promotes the accuracy and integrity of public records and protects the taxpayer's investment in collecting, developing, storing and maintaining public records.

To ensure a thorough discussion of the issues, the Council on Information Management ("Council") formed a committee of policy experts. Serving on the committee were:

Robert D. Harris, Chair, Council on Information Management
Rodney A. Smolla, The Institute of Bill of Rights Law
John Westrick, Office of the Attorney General
Charles C. Livingston, Department of Information Technology
Marie B. Allen, National Archives
Jean Ann Fox, Virginia Citizens Consumer Council

The committee was assisted by a member from each of the Council's advisory committees, representing the technology community in state and local governments:

Dr. Franklin E. Robeson, The College of William and Mary, Education Advisory Committee
Jacqueline M. Ennis, Department of MHMR/SAS, Agency Advisory Committee
H. Bishop Dansby, GIS Law, Advisory Committee on Mapping, Surveying, and Land Information Systems
Robert Yorks, Local Government Advisory Committee

A second group of individuals was formed to provide specific policy assistance in the areas of copyright, privacy, access and public records:

J. T. Westermeier, Fenwick & West
David H. Flaherty, Woodrow Wilson Int'l. Center for Scholars
Edward Jones, *The Free Lance-Star* (Fredericksburg, Virginia)
A. W. Quillian, Department of Motor Vehicles
Louis Manarin, Library of Virginia

The committee held a series of meetings at which individuals and representatives of organizations who had expressed interest in this topic attended and were given an opportunity to express their concerns and recommendations.

The Council has concluded that the tension between the Commonwealth's current policies cannot be completely eliminated but rather calls for a balancing of objectives. The Council believes that many of these tensions can be addressed administratively or with relatively minor statutory changes. The Council recommends that compliance with minimum requirements as well as full attainment of the Commonwealth's policies regarding access, privacy, and records preservation can best be addressed in a programmatic fashion through ongoing development of guidance that relates compliance with these laws to the evolving technology and overall management of information technology planning and acquisition. Protecting the taxpayer's investment in collecting and maintaining government databases and protecting the citizen's ability to control information about himself cannot be fully accomplished within the current statutory framework and will present significant policy issues that the General Assembly may wish to address.

OPPORTUNITIES AND CONCERNS IN THE ELECTRONIC RECORDS ERA

Preserving and Protecting Government Records

The electronic records era presents opportunities for more effective archiving and retrieval of government records. Imaging and other digital technologies represent new preservation techniques that can be used in place of, or in conjunction with, analog processes such as photocopy or microfilm, thereby providing an alternative of comparable quality and lower cost.

Converting electronic records from operational media into durable form for permanent storage presents a challenge because most electronically-stored information is very short-lived, and the media used in operations typically are nondurable. Tapes, diskettes and hard drive space can become unreliable relatively quickly or may need to be reused in ordinary course, and computer memory is subject to loss whenever computers are turned off. This is especially a concern with respect to government actions and transactions occurring entirely in electronic form and which no longer generate a traditional paper record. Archiving of electronic records also requires selection of appropriate "snapshots" of data, as the electronic environment often consists of evolving sets of data rather than series of separate documents.

An additional challenge for electronic preservation arises from the fact that many information management systems employ custom-designed data structures or require customized or proprietary software to retrieve or display data. As information management systems are replaced by more efficient systems (and older software ceases to be supported, understood or even licensed), it can become difficult to maintain the access to non-current records which the agency chooses not to translate for continued use.

An important issue created by the electronic environment is the question of how much information to capture. The electronic environment offers the potential to capture far more information as public records than was previously the case. Without judging the desirability of doing so, vast amounts of information from informal messages, phone conversations, preliminary drafts of documents, workplace surveillance devices and other electronic sources, as a technical matter, can be captured and preserved. Whether this is advisable from the viewpoint of cost, efficiency, privacy and other factors is another matter.

Ensuring Access To Current Government Information

Some of the same factors discussed above with regard to the archiving of electronic records apply also to citizen access to current government information. The increased quantity of preservable data enhances the completeness of the information which may be obtained by citizens, and the electronic format can facilitate research and retrieval

of information previously obtainable, if at all, only by manual search. The electronic format, however, also presents potential barriers to access if unique data structures are used or if customized or proprietary software is needed to locate or retrieve data.

An issue which is intensified by the electronic environment is the question of how much time and money a public body ought to spend to assist citizens who wish to access government information in forms or ways that would require special efforts by the public body. The "snapshot" issue also presents difficulties, because a search of an electronic database ordinarily cannot be performed instantly upon receipt of a request but ought to be available in some form that does not unduly burden the ongoing operations of public bodies.

Enhancing the Efficiency Of Government

Great opportunities to improve the efficiency of government have been and continue to be available through e-mail, voice mail, electronic bulletin boards, word processing, information management systems, automation of agency functions, electronic monitoring of the work place and other technologies. However, the efficiency gains offered by these technologies may be limited to the extent a public body's use of the technologies triggers time-consuming and expensive requirements to retain and index electronic files, translate data or provide for continuing use of older software to manage non-current records, or document every deletion or non-retention of electronic data.

A further loss of efficiency may be created to the extent voice mail, e-mail or other technologies are avoided by employees in favor of more costly meetings or telephone calls that do not generate a permanent record of their every communication.

The electronic records era has also raised a further issue of efficiency in managing available staff resources and agency budgets. Responding to a Freedom Of Information Act (FOIA) request for electronic records, together with all related Privacy Protection Act measures, can involve a significant diversion of staff resources from the agency's primary mission. This diversion can take the form of programming assistance, report generation, or review of records to determine whether they are disclosable or to segregate disclosable from exempt portions. As information, particularly in electronic form, attains commercial value outside traditional FOIA purposes, the quantity and frequency of such requests, as well as the volume of material sought in any particular request, is likely to increase and make the cost issue more acute.

Protecting the Taxpayer's Investment in Databases and Systems

Development of computer systems and associated databases can represent an enormous investment of taxpayer funds and can result in databases and systems that resemble valuable information products much more than they resemble records of public transactions. In such cases, an issue of proper stewardship of publicly-held

assets and of minimizing future tax burdens is created when information marketers seek to obtain, at no or little cost under FOIA, the fruits of the public investment. In some cases, a system may be economically feasible only if the cost of its creation can be shared with private entities that will also benefit from the technology. However, a public body's ability to partner in this fashion is undercut to the extent the public body can be required to provide the fruits of the effort to anyone for free, whether or not they contributed to the development effort.

In some cases, the public body's mission may require wide disbursement of the information in question. In such cases, making the information freely available does not present the same conflict between the taxpayer's interest and the interest of users of that information. Similarly, if the taxpayers' representatives have concluded that free disbursement of valuable information products is in the best interest of the public due to economic development or other considerations, this would reflect a public policy determination not to protect the government's proprietary interest in such products.

Protecting the Individual's Ability to Control Personal Information

The concerns that originally prompted the passage of the Virginia Privacy Protection Act seem even greater today as electronic record-keeping continues to expand. Many citizens fear that far too much information about identifiable individuals is collected, retained and disseminated by government, and that too few controls are exercised to prevent unauthorized uses or to correct errors. All this is causing citizens to lose a measure of privacy from "practical obscurity" -- the difficulty, in the absence of computer matching, of gathering and linking the many bits of personal information that citizens are constantly required or encouraged to provide as a condition of receiving various benefits or services in the public and private sectors. This collection, retention and dissemination of personal information endangers the individual's opportunities to secure employment, insurance, credit and due process and other legal protections. Particular concern exists with respect to the continued use of social security numbers as identifiers, as this information more than any other is believed to facilitate private, unauthorized access and use of credit and other records.

While the increased usage of electronic records heightens citizen interest in assuring full compliance with the Privacy Protection Act, this alone is not viewed as sufficient. The Privacy Protection Act does not prevent dissemination of information, but instead merely requires that certain measures be taken in connection with that dissemination, such as retaining a list of recipients so that, for example, they can be notified of any corrections, and so that the data subject, if he undertakes the effort, can find out who has received information about him and what decisions about him were affected by that information. What these citizens really seek, however, is protection against dissemination of personal information by government.

REVIEW OF CURRENT LAWS

The four statutes identified in Senate Joint Resolution 238, the Virginia Public Records Act,[1] the Virginia Freedom Of Information Act,[2] the Privacy Protection Act of 1976,[3] and the Intellectual Property Act,[4] interact to form most of the Commonwealth's current information policy. Following is a review of these laws and areas in which they could be improved to meet needs arising in the electronic records era.

Freedom Of Information Act

The Freedom of Information Act is intended, among other goals, to ensure that the people of the Commonwealth have ready access to records in the custody of public officials.[5] The FOIA directs that all official records shall be open to inspection and copying within five work days after the request, except as may be otherwise specifically provided by law. The FOIA itself currently lists 58 exemptions from mandatory disclosure, most of which are designed specifically to exempt particular records of particular agencies. The FOIA provides for quick judicial enforcement in the event of alleged violations.

The FOIA has a conceptual problem at its core: the concept of an "official record" is no longer entirely valid as a clearly-defined unit of information in the electronic environment. The concept of the "official record" is rooted in the paper era, when paper documents could be viewed as the building blocks of government information. An official record typically was a visually-perceivable paper document, and many of the balances struck by the FOIA between the goals of access versus administrative

---

1 Code of Virginia, §§ 42.1-76 through 42.1-91.

2 Code of Virginia, §§ 2.1-340 through 2.1-346.1.

3 Code of Virginia, §§ 2.1-377 through 2.1-386.

4 Code of Virginia, § 2.1-20.1:1.

5 Code of Virginia, § 2.1-340.1.

efficiency and cost, were structured around that concept.[6] As other, non-paper media evolved, the definition of "official record" has been adapted to the new media.[7] Now, with electronic record-keeping, the concept of an identifiable "record" consisting of a reasonably specific discussion or report on some government action is significantly at odds with reality. Eventually a statutory change may be necessary.

For the present, however, the Council believes the current definition is workable. The definition of "official record" contemplates some physical embodiment of the information.[8] In the case of electronic records, this may be a tape, diskette or optical disk.[9] It would appear that the minimum requirements of current law are simply to make the record reasonably accessible at reasonable cost. Ordinarily this can be a tape onto which the data in question have been dumped, preferably in a standard format such as ASCII files (if the programming effort is not unreasonable). Where feasible, the agency is authorized, but not required, to prepare summaries or reports by extracting specific information from tapes, disks or other records that is more directly responsive to the requester's research topic.[10] Programming or report generation tasks appear mandated only in connection with segregating exempt from non-exempt portions of a record where such segregation is reasonable. The five work-day turn-around time provides some guidance as to the level of effort that is reasonable for segregating specific entries from a database.[11] This does not preclude public bodies from undertaking greater efforts voluntarily within a larger time agreeable to both the public body and the requester. The Council believes that public bodies generally are

---

[6] A request must reasonably identify the record sought and must be made to the custodian of the record. The request must identify an existing record; the public body is not required to create new ones. Code of Virginia, § 2.1-342(A). These limitations envision compliance as simply a matter of retrieving an identified document from the agency's files. With the assumption that significant government actions tend to generate records, the limitation to existing records minimizes compliance costs while providing information that is most likely to shed light on government operations.

[7] See, Code of Virginia, § 2.1-341.

[8] Official records are defined as "all written or printed books, papers, letters, documents, maps and tapes, photographs, films, sound recordings, reports or other material, regardless of physical form or characteristics, prepared, owned, or in the possession of a public body or any employee or officer of a public body in the transaction of public business." Code of Virginia, § 2.1-341.

[9] In Associated Tax Service, Inc. v. Fitzpatrick, 372 S.E.2d 625, 626 and 629 (1988), the Virginia Supreme Court stated that a "computer disk file" is an official record, but the precise description of what constituted a record was not at issue in the case.

[10] See Code of Virginia, § 2.1-342(A).

[11] See Code of Virginia, § 2.1-342(A).

cooperative, provided that excessive diversion of staff resources can be avoided.

The FOIA does not directly indicate what factors should be considered in determining whether electronic records are reasonably accessible, or what level of effort can reasonably be expected of the agency to enhance accessibility. While guidance in this area would be helpful, the wide variety of existing electronic information systems both within state government and as between state and local government, as well as the likelihood that technology will continue to evolve rapidly, weigh against efforts to standardize the specifics of access through legislation. This is not to say that access is as complete as all would desire. Rather, the Council's conclusion is that the statute imposes certain minimum standards, but that higher ideals of access, as a practical matter, can best be pursued only through strategic planning of information technology resources, especially at the information systems procurement or implementation stage. The Council recommends that information technology management guidelines issued under § 2.1-563.31(B)(5) should include guidance for the attainment of FOIA and other information policy requirements and goals in a manner which reasonably takes into account cost and efficiency trade-offs. This effort would be enhanced by more specific authorization, but current statutory language is probably adequate.

Privacy Protection Act of 1976

The Privacy Protection Act establishes certain principles of information practice and makes them applicable to governmental agencies that maintain manual or automated record keeping systems containing information that describes, locates or indexes anything about an individual.[12] Among other requirements, the Privacy Protection Act requires that agencies collect, maintain, use and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated or necessary to accomplish a proper purpose of the agency; maintain information in the system with accuracy, completeness, timeliness and pertinence as necessary to assure fairness in determinations relating to a data subject; make no dissemination to another system without specifying requirements for security and usage, including limitation on access thereto, and receiving reasonable assurances that those requirements and limitations will be observed; maintain a list of all persons and organizations having regular access; and maintain a complete and accurate record including the identity and purpose of any access to personal information in the system.[13]

The Privacy Protection Act also grants certain rights to individuals, including the right to be told, when the information is collected, whether one may refuse to provide the information and what the consequences will be; the right to be notified of the possible

---

[12] See Code of Virginia, §§ 2.1-378(B) and 2.1-379.

[13] Code of Virginia, § 2.1-380.

dissemination of the information to another agency or nongovernmental organization; the right to inspect the data and the list of all those who have accessed it, the right to challenge, correct, or explain information; the right to have the agency investigate and record the current status of that personal information and promptly purge or correct incomplete, inaccurate, non-pertinent, untimely or unnecessary information; the right to file a statement of up to 200 words and have a copy thereof sent to any previous recipient; and the right to have past recipients of purged or corrected data notified of such action.[14] Injunctive relief and attorneys' fees are available to remedy violations of the Act.[15]

There are two aspects to the privacy concerns expressed to the Council during its study. The first is directly addressed to the Privacy Protection Act: the feeling that its provisions provide significant protection but that there is no auditing effort to assure compliance by state agencies. The Act's requirements do seem to provide a vehicle for addressing many privacy concerns. However, the Act is very complicated, and attainment of its objectives in a cost-efficient manner presents many challenges. The Council recommends that agency compliance with the Act be audited. In addition, uniform guidance should be provided to assist agency compliance and to enhance the public's ability to comprehend the measures that are available to protect their privacy. Like access, privacy protection can be enhanced significantly if provision for compliance is made at the information systems procurement or implementation stage.

The other major privacy concern expressed to the Council during its study cannot be completely addressed within the current statute: while significant restraints may be imposed upon collecting only that data which is expressly or implicitly authorized by law, and disseminating it only with adequate assurances regarding its use, many citizens are most interested in preventing dissemination, particularly in electronic form, of personal information. The current Act prohibits dissemination except when dissemination is "permitted or required by law" or necessary to accomplish a proper purpose of the agency.[16] Since the current FOIA at least permits disclosure of virtually all public records (even those which are exempt from mandatory disclosure),[17] the Privacy Protection Act's ostensible limitation on dissemination of such information is illusory.[18]

---

[14] Code of Virginia, § 2.1-382(A).

[15] Code of Virginia, § 2.1-386.

[16] Code of Virginia, § 2.1-380(1).

[17] See Code of Virginia, § 2.1-342(A) and (B).

[18] This is in contrast to federal law, which generally prohibits dissemination of personal information records if disclosure of the record would constitute a clearly unwarranted invasion of personal privacy. See 5 U.S.C. §§ 552(b)(6) and 552a(b)(2). Although the Virginia FOIA and Privacy Protection Acts are patterned after the federal statutes, the key difference is that the federal privacy protection act permits dissemination if disclosure is "required under [the FOIA]" (see 5

While dissemination is difficult to prevent under current law, it appears that the Privacy Protection Act permits the use of contracts in connection with dissemination to other systems to address some of the above privacy concerns.[19] However, if the General Assembly wants to protect against dissemination of personal information, the Council would recommend considering amendments to Virginia's FOIA and Privacy Protection Act along the lines of the federal counterparts of these statutes.

Virginia Public Records Act

The Virginia Public Records Act provides for the management and preservation of public records throughout the Commonwealth and is intended to promote uniformity in the procedures used to manage and preserve public records.[20] In addition to serving as the custodian of all records transferred to the state archives, the State Library Board is authorized to issue regulations to "facilitate" the creation, management, preservation and destruction of records by agencies.[21] The Act prohibits agencies from destroying or discarding records without a retention and disposition schedule approved by the State Librarian.[22] A recent amendment appears to grant agencies somewhat greater autonomy in scheduling the retention and destruction of electronic records.[23]

Record management rules, particularly in the electronic environment, can present significant trade-offs between cost, access, privacy protection, preservation of records and public access. Currently, the statutes provide oversight authority in this area to the Council, the State Library Board and the various agency heads.[24] While the

---

U.S.C. § 552a(b)(2)) whereas the Virginia Privacy Protection Act permits dissemination if dissemination is "permitted or required by law" (see § 2.1-380(1) of the Code). Thus, a record which is exempt from mandatory disclosure under the FOIA would not meet the above federal requirement for permissible dissemination but would meet the Virginia privacy protection standard. In addition, the federal FOIA contains a general exemption from mandatory disclosure for any record if the disclosure of the record would constitute a clearly unwarranted invasion of privacy (see 5 U.S.C. § 552(b)(6)), whereas the Virginia FOIA has no such general exemption from mandatory disclosure.

19 See Code of Virginia, § 2.1-380(5).

20 Code of Virginia, § 42.1-76.

21 Code of Virginia, § 42.1-82(1).

22 Code of Virginia, § 42.1-86.1.

23 Code of Virginia, § 42.1-87.

24 See, e.g., Code of Virginia, §§ 2.1-563.31(B)(5), 42.1-82, 42.1-85, 42.1-86.1 and 42.1-87.

statutory lines of responsibility are not as clear as they could be, the Council feels that a cooperative approach will be successful. The major goal to be accomplished should be the proper balancing of cost, access, privacy, preservation and other objectives at the earliest possible stage in the information management process -- ideally at the systems procurement or implementation stage.

It is unclear whether the Act permits the State Library Board sufficient flexibility to take advantage of evolving technology. Many provisions seem to mandate particular technologies, particularly microfilm.[25] Given the dynamic nature of innovation in electronic information storage, it would be preferable to avoid writing any particular technology into a statute.

The current definition of "public record" is not adequate. The definition of this term currently is so broad that it includes any form of data representation, no matter how transitory.[26] When this is combined with the Act's prohibition against destruction of public records (except in accordance with required retention and disposition schedules),[27] it becomes literally illegal to turn off a computer, which can result in the loss of information in computer memory. More readily apparent examples of necessary loss of such "records" include editing with a word processor, automatic or manual deletion of e-mail messages after they are sent or after one's electronic mailbox is full, periodic purging of voice mail messages after a period of time, re-use of dictation tapes, and other administratively necessary actions. While the Act apparently authorizes agencies to schedule disposition and theoretically could schedule for immediate destruction, this apparently must be in accordance with procedures that document the destruction[28] -- an approach which appears inconsistent with streamlining government.

The Council recommends that the definition of "public record" be amended to strike a balance between data for which full-blown record preservation and destruction documentation measures are appropriate and data that are too transitory to be viewed appropriately as rising to the level of a public record. One suggestion would be to define public records to exclude a recording which, at the time of its creation, is intended only to substitute for a face-to-face conversation, telephone call or other non-written communication or if it is intended by its creator to serve only as a personal

---

[25] See, e.g., Code of Virginia, §§ 42.1-83 and 42.1-84. Greater flexibility seems permitted for certain purposes. See e.g., Code of Virginia, § 42.1-86.

[26] "The general types of records may be, but are not limited to ... any representation held in computer memory." Code of Virginia, § 42.1-77.

[27] Code of Virginia, §§ 42.1-86.1 and 42.1-87.

[28] See Code of Virginia, § 42.1-87, Section 5 of A Manual for Public Records Management in the Commonwealth of Virginia (1992); and The Library of Virginia Guidelines for Managing Electronic Records, at p. 11 (requiring preparation and approval of a Certificate of Records Disposal (form RM-3) before any electronic record can be destroyed).

note or draft to assist the creator in preparing his own later oral or written presentation. Similarly, with respect to dynamic databases, agencies could be required to schedule reasonably periodic snapshots of such databases, and "official record" could be defined to include the snapshots but exclude the evolving, underlying database.

Finally, the Council recommends that the definition of "public record" and "official record" should be synonymous and uniform for both the Public Records Act and the FOIA.

Intellectual Property Act

The FOIA anticipated one instance in which there is a competing policy goal of recovering from the user not just search and copy costs, but also a portion of the cost of developing a record that is in the nature of an information product.[29]

In addition, it has long been recognized that the Commonwealth can exercise its rights under the federal Copyright Act[30] to control commercialization of works of authorship in which it owns the copyright.[31] Exercise of such rights under the copyright law is not in conflict with FOIA, because citizens retain the initial right to inspect and make their own copy of such government works of authorship (unless an exception to FOIA applies). The government's rights as a copyright owner may be exercised to control the commercial requester's subsequent duplication, adaptation and distribution of works of authorship, and if desired, to obtain royalties. The government's control over subsequent duplication and distribution is appropriately limited, however, by provisions of the Copyright Act which would permit the fair use of copyrighted works without the copyright owner's permission for purposes such as criticism, comment or news reporting regarding government operations.[32]

The Intellectual Property Act provides that patents, copyrights or materials which were potentially patentable or copyrightable developed by a state employee during working hours or within the scope of his employment or when using state-owned or state-controlled facilities shall be the property of the Commonwealth. It authorizes the

---

[29] Public bodies are authorized to "charge, on a pro rata per acre basis, for the cost of creating topographical maps developed by the public body, for such maps or portions thereof, which encompass a contiguous area greater than fifty acres." Code of Virginia, § 2.1-342(A).

[30] See 17 U.S.C. § 106.

[31] See, e.g., 1981-1982 Att'y Gen. Ann. Rep. 443, 444.

[32] See 17 U.S.C. § 107.

Governor to set policies as he deems necessary to implement this provision.[33]

Under this authority, Executive Memorandum 2-86 was issued, and subsequent governors have retained it in effect. The executive memorandum, which has come to be known as the state's "intellectual property policy," ("IPP") governs disposition of intellectual property by state executive branch agencies. Separate statutes authorize intellectual property policies for state-supported institutions of higher education.[34]

The Intellectual Property Act and the IPP issued under it, however, are not currently adequate to fully protect the taxpayer's investment in the gathering and storing of government information. The current tools are limited to the protection which is available under the copyright and patent laws. At the time of the Act's passage, the prevailing view was that copyright law provided significant protection for databases, and the IPP stated that it applied to databases. Subsequently, case law under the Copyright Act has undercut that view.[35] While other legal theories may be available to supplement copyright, it is speculative whether these will prove adequate.

In view of the uncertain protection available under copyright law and other legal theories, the chief means employed by the private sector to assure that the creator of a database is able to recover a fair return is through contract. Contract formation, however, requires the recipient's agreement and receipt of consideration. In the private sector, the recipient's agreement and the consideration derive from the fact that the holder of the data is within his rights to refuse to disclose the data to the requester. This option currently is not available to public bodies in receipt of a FOIA request for nonexempt official records. Accordingly, one questions whether a recipient will agree to a contract, and if he did, one would question whether consideration for the resulting promise would exist.

At least two approaches could be considered to fully protect the taxpayer's investment in government information by enabling the public body to require a licensing agreement comparable to the agreements typically used in the private sector. These approaches are designed to provide this flexibility while not undercutting the policy of ensuring that citizens are able to witness the operations of government.

One approach would be to work within the current FOIA provision relating to

---

[33] Code of Virginia, § 2.1-20.1:1.

[34] Code of Virginia, §§ 23-4.3, 23-4.4 and 23-9.10:4.

[35] See, e.g., Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340, 111 S. Ct. 1282 (1991) and Kern River Gas Transmission Co. v. Coastal Corporation, 899 F.2d 1458 (5th Cir.), cert. den., 498 U.S. 952, 111 S. Ct. 374 (1990), which call into question the effectiveness of copyright protection for databases.

permissible charges for topographical maps.[36] One could expand the exception for topographic maps to include any record which is in the nature of an information product, i.e., one which has uses other than as a window into the operations of government and which is in fact the subject of bona fide marketing efforts by the agency. Any usefulness of such information products as a window into the operations of government could be preserved by mandating at-cost electronic access and duplication for any requester who is willing to sign a form representing that the requester does not intend any commercial use of the information and agrees not to use it or permit others to use it commercially. If the requester is unwilling to sign such a form, the agency could be authorized to charge a price designed to recover development costs (as is the case with topographical maps) or could be authorized to charge a fair market price. In either case, the public body would need authority to require the recipient to sign an agreement not to duplicate and distribute the document without further permission.

Another approach would be to require at-cost disclosure of all public records, but provide that an agency need not provide electronic copies of records if the requested copies can be provided in printed form. As with the above approach, provision of electronic copies could nonetheless be mandated if the requester is willing to sign a form representing that the requester does not intend any commercial use of the electronic copy and agrees not to use it or permit others to use it commercially. As a practical matter, the open government goals of the FOIA can be obtained if the electronic records are readily available for inspection, and if copying is unconditionally available in some form and conditionally available in electronic form. The interest in having the information in electronic form is precisely because private parties wish not only to have access to the information, but also to appropriate for themselves the value of taxpayer-funded typing and entry of the data into electronic form. This second approach would provide a basic window into government operations while preserving a domain within which the public body would be able to charge for the added value.

---

[36] Code of Virginia, § 2.1-342(A).

CONCLUSIONS

The Council finds that current laws for the most part are adequate to address the challenges which the electronic environment presents to the Commonwealth's access, preservation and privacy policies. As the policies of the Commonwealth are in competition with one another, the issue becomes more a programmatic one -- how best to plan and coordinate the way information is collected and managed in order to maximize attainment of all the Commonwealth's goals. Due to the extraordinary pace of technical change, it is unwise to specify rigid technical standards in the law in a way that reduces flexibility to devise and adapt to current technology and available solutions. Therefore, in FOIA, the current reliance on rules based on a "reasonableness" concept is preferable at this point to any specifically-mandated requirement. While flexibility is desirable, chaos is not. The problems are difficult and dynamic enough that uniform guidance to assist agencies' compliance efforts is advisable. The Council recommends that its authority under § 2.1-563.31(B)(5) to direct the promulgation of policies, standards and guidelines for managing information technology resources in the Commonwealth be used to provide this assistance. Specific statutory direction may facilitate this function but is not essential.

Recommendations for change to current statutes include: (1) providing a uniform definition for "official records" and "public records" in FOIA and the Public Records Act; (2) revising the definition of public records (and official records) to exclude transitory recordings and include periodic snapshots of dynamic databases; and (3) expand existing auditing processes to include auditing for compliance with the Privacy Protection Act. Further consideration and study should be given to the issue of data dissemination and whether the Commonwealth wants to enable its citizens to prevent government disclosure of information that unduly invades personal privacy. Finally, further consideration should be given to amending FOIA to carve out an area within which public bodies may protect the taxpayer's investment in geographic information systems or other databases by conditioning disclosure upon the payment of fees and agreement to a licensing contract.

Appendix

SENATE JOINT RESOLUTION 238

Requesting the Council on Information Management, in conjunction with The Institute of Bill of Rights Law, to study issues regarding public access to government information.

Agreed to by the Senate, February 9, 1993
Agreed to by the House of Delegates, February 17, 1993

WHEREAS, the Virginia Freedom of Information Act, the Virginia Privacy Protection Act of 1976, the Virginia Public Records Act and the Intellectual Property Act regulate the collection, maintenance, preservation, use, and dissemination of information by state and local government agencies in the Commonwealth; and

WHEREAS, the flow of information from citizens to government and back to citizens is essential in a democratic society, providing citizens with knowledge of their public institutions, society and economy; and

WHEREAS, the privacy of an individual is directly affected by the collection, maintenance, use, preservation and dissemination of personal information by government; and

WHEREAS, information is a vital component of all government programs and decisions; and

WHEREAS, advancements in information technology have enhanced the value and potential uses of public information; and

WHEREAS, the increasing value of government information, developed at public expense is a key factor in Virginia's economic, technological and cultural development; and

WHEREAS, the increased demand for, and provision of, public information may lead to a significant economic and human resources burden on government agencies; and

WHEREAS, the increased demand for and provision of public information may entail an exposure to legal liability for government agencies; and

WHEREAS, the collection, maintenance, preservation, use and dissemination of information in electronic environments have unrealized potential for management, services and accountability but may require modification of traditional policies and procedures; now, therefore, be it

RESOLVED by the Senate, the House of Delegates concurring, That the Council on Information Management, in conjunction with The Institute of Bill of Rights Law be requested to study whether current state law ensures public access to government information, protects the rights of the individual to control information about himself, promotes the accuracy and integrity of public records and protects the taxpayer's investment in collecting, developing, storing and maintaining public records.

The Council is requested to consult with the Virginia State Library and Archives, Department of Information Technology, Virginia Municipal League, Virginia Press Association, Virginia Association of Counties and agencies of state and local government in conducting its study.

The Council shall complete its work in time to submit its findings and recommendations to the 1994 Session of the General Assembly as provided in the procedures of the Division of Legislative Automated Systems for the processing of legislative documents.

Appendix E

CERT Coordination Center 1995 Annual Report

CERT℠
Coordination Center

CERT Coordination Center
1995 Annual Report (Summary)

1. Introduction

The CERT Coordination Center was formed by the Advanced Research Projects Agency (ARPA) in November 1988 in response to the needs exhibited during an Internet security incident. Our charter is to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. Our specific mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

2. Activities and Services

Incident Response

From January through December 1995, the CERT Coordination Center received 32,084 email messages and 3,428 hotline calls. We handled 2,412 computer security incidents during this period. More than 12,000 sites were affected by these incidents, which involved 732 break-ins and nearly that many probes and pranks. Among the most serious intruder activities for 1995 are the following.

- IP spoofing. There was a surge in IP spoofing this year. The year began with an advisory about IP spoofing, and attacks continued throughout the year. In a matter of weeks during the summer, we received more than 170 reports of IP spoofing attacks or probes, many resulting in successful break-ins. We found that several sites believed incorrectly that they were blocking such packets, and other sites had planned to block them but hadn't yet done so.

- Network File Service (NFS) attacks. This year there was a large increase in the number of attacks relating to weaknesses in NFS. Many of the attacks were successful; moreover, programs to automate these attacks have become widespread in the intruder community. A successful attack usually results in the intruders gaining root access.

- Network scanning. Intruders have been scanning a large range of network addresses using Internet Security Scanner (ISS). This tool interrogates all computers within a specific address range, determining the security posture of each with respect to several common system vulnerabilities.

Intruders have used the information gathered from these scans to compromise sites, and we are aware of many systems that have suffered a root compromise as a result of information intruders obtained from ISS scans.

• Packet sniffers. This year we continued to receive new incident reports about sniffers on compromised hosts. These sniffers, used to collect account names and passwords, frequently have been installed using a kit. In some cases, the packet sniffer was found to have been running for months. Occasionally, sites had been explicitly warned of the possibility of compromise, but the activity continued because the site did not address the problem in the comprehensive manner we suggest in our security documents.

• Sendmail attacks. Intruders have been using a variety of techniques to exploit sendmail, with most of the attacks aimed at getting root privileges on the victim machine. This year, we released four CERT advisories and one vendor-initiated bulletin relating to problems with sendmail. In many cases, intruder attacks were successful because sites had not installed upgrades and patches nor taken other precautions such as running the sendmail restricted shell program (smrsh).

The year ended with a series of attacks on Internet sites that resulted in our issuing an alert to network service providers and the network community in general warning them of the intruder activities listed below (list taken from advisory CA-95:18).

• Using automated tools to scan sites for NFS and NIS vulnerabilities
• Exploiting the rpc.ypupdated vulnerability to gain root access
• Exploiting the loadmodule vulnerability to gain root access
• Installing Trojan horse programs and packet sniffers
• Launching IP spoofing attacks

Work continues in 1996 on incidents involving all the types of activity noted in this annual report.

Advisories

Eighteen advisories were published in 1995. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. Advisories are sent to the cert-advisory mailing list, posted to the USENET newsgroup comp.security.announce, and made available for anonymous FTP from ftp://info.cert.org/pub/cert_advisories/.

We use README files associated with each advisory to keep information current without changing the original content of an advisory. The files are available from our FTP archive site, and we urge advisory readers to check README files periodically for updated information.

A complete listing of the advisories issued during 1995 can be found in Appendix A.

Vendor Bulletins

In December 1994, we began publishing CERT vendor-initiated bulletins. These bulletins contain verbatim text from vendors describing security problems and their solutions. Our goal is to help the vendors' security information get wide distribution quickly. The bulletins are distributed through the same channels as advisories.

Ten bulletins were published in 1995. A complete listing can be found in Appendix B.

CERT Summaries

This year we began publishing the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. The first CERT Summary was issued on July 26; others followed on September 26 and November 28. The primary purpose of the summary is to call attention to the types of attack currently being reported to the CERT incident handling staff. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Starting with the September publication, each summary also contains a list of new and updated files available for anonymous FTP.

Training Courses

CERT staff continued to present "Internet Security for System and Network Administrators" and "Internet Security for Managers." Both courses help organizations assess and improve their level of computer and information security.

This year, "Internet Security for System and Network Administrators" was approved by the SEI Education and Training Review Board as an SEI course. The course will be presented at the SEI four times during 1996: February 15, April 11, July 11, and December 11.

3. Research and Development

Information Security Risk Evaluations

During the year, we completed two field tests of an information security risk evaluation (ISRE) method being developed by the CERT staff. Both tests were conducted at financial service organizations. The ISRE includes a security taxonomy, a set of interviews, and a technology review.

The information security risk evaluation is one component of an overall information security improvement program under development. With the risk evaluation as a starting point, this program will provide practical guidance in addressing the issues and shortcomings that are identified as risk areas. The objective is to start a site on an improvement path in a way that ensures a high probability of success.

4. Advocacy and Community Support

The CERT Coordination Center staff members were invited to give presentations at several conferences, workshops, and meetings during 1995. This has been found to be an excellent tool to educate attendees in the area of network information system security and incident response. Below are some examples of the CERT staff's participation in external events.

- Avoiding the Crisis in Healthcare Information Security, a conference sponsored by MIS Training and INFO Security. A CERT staff member presented "Securing your Interface to the Internet."
- FBI Academy. A CERT staff member spoke on Internet security issues and the use of the Internet.
- Institute of Internal Auditors (IAA). At the IAA Advanced Technology Conference held September

16-20, 1995, a staff member gave a talk on "Defensive Strategies on the Information Highway."
• Internet Symposium on Network and Distributed System Security. A CERT staff member served as the general chair of the three-day symposium.
• NISSC (National Information Systems Security Conference - formerly National Computer Security Conference). A CERT member presented "Internet Sniffer Attacks," which won outstanding paper for the conference.
• Public meeting on National Information Infrastructure (NII) Security Issues. A CERT team member testified at a public meeting held at the Department of Commerce in March. Topics included the risks to information, educating and setting expectations of users, and how the government can support availability and reliability in the NII.
• SEC EDGAR Technology Conference. A staff member participated in a panel entitled "Technical Options for Achieving Fundamental Objectives."
• Uniforum UNIX show. A CERT staff member presented an all-day tutorial, "Internet Security for UNIX System and Network Administrators," to 82 people. He also presented "Managing the Risk" to more than 50 people during a regular session of the conference.
• The USENIX Association presented team member Jim Ellis with the USENIX Lifetime Achievement Award. This award recognizes and celebrates singular contributions to the UNIX community in both intellectual achievement and service that are not recognized in any other forum. For 1995, Ellis and two others received the award for their work in creating USENET.

Internet Engineering Task Force

The CERT Coordination Center is actively involved in the security-related work of the Internet Engineering Task Force (IETF). CERT staff member Barbara Fraser is a member of the Security Directorate, a standards body, and is chair of two workings groups. The working groups are producing two site security handbooks - one for system and network administrators, and one for users - and are developing guidelines for security incident response teams and technology vendors.The CERT Coordination Center provides archive space for the work of these groups (ftp://info.cert.org/pub/ietf/).

Forum of Incident Response and Security Teams

The CERT Coordination Center co-sponsored the FIRST Incident Response Workshop, which was held in Karlsruhe, Germany, September 18-22, 1995. There were 129 attendees, representing more than 30 response teams from around the world. This annual workshop provides a forum for teams to exchange information and discuss ways to coordinate response activities. Topics this year included how to form an incident response team, communication among teams, recent developments in network liability, and techniques for tracking incidents.

Appendix A: CERT Advisories Published in 1995

The following advisories were published in 1995. We will continue to add updated information to CA-95:xx.README files as necessary.

CA-95:01.IP.spoofing.attacks.and.hijacked.terminal.connections
This advisory describes attacks in which intruders create packets with spoofed IP addresses and exploit applications that use authentication based on IP. The advisory also discusses a tool intruders use to take control of open terminal or login sessions.

CA-95:02.binmail.vulnerabilities

This advisory supersedes CA-91:01a and CA-91:13. It addresses vulnerabilities in some versions of /bin/mail based on BSD 4.3 UNIX. It includes a list of vendor patches and source code for mail.local.c, an alternative to /bin/mail. Updated information will be placed in the CA-95:02.README file.

CA-95:03.telnet.encryption.vulnerability
Description and patch information for a security problem in the Berkeley Telnet clients that support encryption and Kerberos V4 authentication. **This information is superseded by CA-95:03a.

CA-95:03a.telnet.encryption.vulnerability
Description and patch information for a security problem in the Berkeley Telnet clients that support encryption and Kerberos V4 authentication. It provides additional information. **This information supersedes CA-95:03.

CA-95:04.NCSA.http.daemon.for.unix.vulnerability
This advisory provides a patch for a vulnerability in the NCSA HTTP daemon version 1.3 for UNIX.

CA-95:05.sendmail.vulnerabilities
This advisory supersedes all previous advisories relating to sendmail. Three vulnerabilities are addressed; vendor vulnerability and patch information is included, along with a sendmail wrapper.

CA-95:06.satan
An overview of the Security Administrator Tool for Analyzing Networks (SATAN) based on the CERT staff's review of beta version 0.51. Includes a list of vulnerabilities probed and advice on securing systems.

CA-95:07.vulnerability.in.satan
This advisory describes precautions to take against a vulnerability in SATAN 1.0. **Superseded by CA-95:07a.

CA-95:07a.REVISED.satan.vul
This revised advisory supersedes CA-95:07. The revision provides new information about the problem described in CA-95:07, and includes precautions to take when running SATAN. A tutorial by the SATAN authors, "SATAN Password Disclosure," is appended to the advisory.

CA-95:08.sendmail.v.5.vulnerability
This advisory describes a vulnerability in sendmail v.5, which is still in use and which includes IDA sendmail. Many vendors have previously fixed the problem; others recently developed patches.

CA-95:09.Solaris.ps.vul
This advisory describes a vulnerability in Solaris that can be exploited if the permissions on the /tmp and /var/tmp directories are set incorrectly.

CA-95:10.ghostscript
This advisory describes a vulnerability involving the -dSAFER option in ghostscript versions 2.6 through 3.22 beta. The advisory includes instructions for fixing the problem and pointers to version 3.33 of ghostscript.

CA-95:11.sun.sendmail-oR.vul
This advisory describes a vulnerability in the sendmail -oR option in SunOS 4.1.X. At the time of the advisory, the vulnerability was being actively exploited.

CA-95:12.sun.loadmodule.vul
The advisory describes a problem with the loadmodule(8) program in Sun OS 4.1.X and provides patch information.

CA-95:13.syslog.vul
This advisory describes a general problem with syslog, lists vendor information about patches, and provides a workaround for solving the syslog problem in sendmail in particular.

CA-95:14.Telnetd_Environment_Vulnerability
This advisory describes a vulnerability with some telnet daemons and includes patch information from vendors, along with a workaround.

CA-95:15.SGI.lp.vul
This advisory points out accounts that are distributed without passwords and urges SGI customers to create passwords for those accounts.

CA-95:16.wu-ftpd.vul
This advisory describes a vulnerability in the wu-fptd SITE EXEC command and provides solutions for both Linux users and others.

CA-95:17.rpc.ypupdated.vul
This advisory describes a vulnerability in the rpc.ypupdated program, for which an exploitation program has been posted to several newsgroups. The advisory includes vendor information and a workaround.

CA-95:18.widespread.attacks
This advisory warns readers of attacks on hundreds of Internet sites in which intruders exploit known vulnerabilities, all of which have been addressed in previous CERT advisories. These advisories are listed.

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1995

The following vendor-initiated bulletins were published in 1995.

VB-95:01.hp
This bulletin addresses problems with Remote Watch in fileset WATCH-RUN for releases of HP-UX, in particular HP 9000 series 300/400s 10.2(1) through 10.2(5); 10.0(1) through 10.0(9); and all previous versions.

VB-95:02.sgi
Vulnerability and patch information for the IRIX 5.2, 6.0, 6.0.1 Desktop Permissions Tool.

VB-95:03.hp
Sendmail vulnerability and patch information for HP 9000 series 300/400s and 700/800s 8.x and 9.x.

VB-95:04.venema
Vulnerability and patch information for S/Key software enhancements for FreeBSD 1.1.5.1 and 2.0 and for logdaemon versions prior to 4.9.

VB-95:05.osf

Description of a security hole in all releases of OSF/DCE prior to version 1.1, and information about the fix.

VB-95:06.cisco
Problem description, upgrade information, and workaround for a vulnerability in Cisco's IOS software versions 10.3(1) through 10.3(2); 10.2(1) through 10.2(5); 10.0(1) through 10.0(9); and all previous versions.

VB-95:07.abell
Description of a directory and file vulnerability in lsof 3.18 through 3.43, along with instructions on getting later versions.

VB-95:08.X_Authentication_Vul
Vulnerability and patch information for an X authentication vulnerability.

VB-95:09.hp
Vulnerability and patch information for a vulnerability in ftp in releases 9.X and 10.X of HP-UX (platforms: HP 9000 series 300/400s and 700/800s).

VB-95:10.elm
Vulnerability and patch information for a vulnerability in elm 2.4 PL 24.

VB-95:10a.elm
This updated version of VB-95:10 lists additional FTP sites.

● Return to the CERT/CC home page

Appendix F

State Board of Elections Invoice, Guidelines and Contract for person requesting voter data

Commonwealth of Virginia
STATE BOARD OF ELECTIONS
200 N. 9Th Street, Room 101
Richmond, Virginia 23219-3497

(804) 786-6551
Toll-free within Virginia (800) 552-9745
Voice or TDD on either number

INVOICE

Mr. John R. Snoddy III, Chairman
Political Party
Buckingham County Democratic Committee
PO Box 325
Dillwyn, VA 23936

Account Number	10253
Invoice Date	10/23/1996

REF #	DESCRIPTION OF ITEMS TO BE PURCHASED	QTY	UNIT PRICE	AMOUNT
14536	Registered Voters List Computer Printout Buchingham County - 029 Locality/Pct/Registrant Address Sequence	1	56	$56
	Make checks payable to: State Board of Elections	TOTAL AMOUNT OF INVOICE		$56
	Sign and return Original and Yellow copies with payment.			

READ THE FOLLOWING CAREFULLY BEFORE SIGNING:

I have reviewed this invoice carefully. The items listed are those I wish to purchase and are indicated as being produced in the sequence I desire. Further, as required by law, I hereby subscribe to the following statement. I understand that the lists requested are the property of the State Board of Elections of the Commonwealth of Virginia, and I hereby state or agree, subject to felony penalties for making false statements pursuant to § 24.2-1016, that (i) I am a person authorized by § 24.2-405 or § 24.2-406 of the Code of Virginia to receive a copy of the [items] described; (ii) the [data] will be used only for the purposes prescribed and for no other use; and (iii) I will not permit the use or copying of the [data] by persons not authorized by the Code of Virginia to obtain them. (NOTE: Any violation of these restrictions is a punishable offense; Falsely subscribing to this statement is a Class 5 felony under Virginia law. The punishment is a maximum fine of $2,500 and /or confinement for up to ten years. Also, you lose your right to vote.)

_____
signature of purchaser

_____
date

SBE-170 REV 7/18/94

INVOICE WILL BE CANCELLED IF NOT SIGNED AND RETURNED WITHIN 30 DAYS

EXCERPTS FROM THE CODE OF VIRGINIA

§ 24.2-405. Persons who may obtain lists of registered voters.--- The State Board of Elections shall furnish, at a reasonable price, lists of registered voters for their districts to (i) courts of the Commonwealth and the United States for jury selection purposes, (ii) candidates for election or political party nomination to further their candidacy, (iii) political party committees or officials thereof for political purposes only, (iv) incumbent officeholders to report to their constituents, and (v) nonprofit organizations which promote voter participation and registration for that purpose only. The lists shall be furnished to no one else and used for no other purpose...

§ 24.2-406. Persons who may obtain lists of persons voting at primaries and elections.--- The State Board of Elections shall furnish to candidates, elected officials, or political party chairmen and to no one else, on request and at a reasonable price , lists for their districts of persons who voted at any primary or general election held in the two preceding years. Such lists shall be used only for campaign and political purposes and for reporting to constituents...

§ 24.2-407. Statement for persons receiving lists of persons registered or voting; penalties.--- Any person receiving lists pursuant to § 24.2-405 or § 24.2-406 shall sign the following statement:

"I understand that the lists requested are the property of the State Board of Elections of the Commonwealth of Virginia, and I hereby state or agree, subject to felony penalties for making false statements pursuant to § 24.2-1016, that (i) I am a person authorized by § 24.2-405 or § 24.2-406 of the Code of Virginia to receive a copy of the lists described; (ii) the lists will be used only for the purposes prescribed and for no other use; and (iii) I will not permit the use or copying of the lists by persons not authorized by the Code of Virginia to obtain them."...

§ 24.2-1016. False Statements; penalties.--- Any willfully false material statement or entry made by any person in any statement, form, or report required by this title shall constitute the crime of election fraud and be punishable as a Class 5 felony....

NOTE: The punishment for a Class 5 felony is a maximum fine of $2,500 and/or confinement for up to ten years. Upon conviction, you lose your right to vote.

REV 6/15/95

CONTRACTOR STATEMENT[1]

I, the undersigned authorized representative of the data processing, mailing list, campaign management, consulting, or other firm indicated below, understand that the Registered Voter Lists or Lists of Those Who Voted that have been entrusted to me are the property of the State Board of Elections of the Commonwealth of Virginia; and I hereby affirm that I and my organization will ensure that the lists are used only by and for the persons and purposes prescribed in §§ 24.2-405 and 24.2-406 of the Code of Virginia as set forth below; and I will not permit the use or copying of such lists by anyone else or for any other purpose, and then only with the permission of the legally qualified original purchaser.

§ 24.2-405. Persons who may obtain lists of registered voters. – The State Board of Elections shall furnish, at a reasonable price, lists of registered voters for their districts to (i) courts of the Commonwealth and the United States for jury selection purposes, (ii) candidates for election or political party nomination to further their candidacy, (iii) political party committees or officials thereof for political purposes only, (iv) incumbent officeholders to report to their constituents, and (v) nonprofit organizations which promote voter participation and registration for that purpose only. **The lists shall be furnished to no one else and used for no other purpose...** (Emphasis added)

§ 24.2-406. Persons who may obtain lists of persons voting at primaries and elections. -- The State Board of Elections shall furnish to candidates, elected officials, or political party chairmen **and to no one else**, on request and at a reasonable price lists for their districts of persons who voted at any primary or general election held in the two preceding years. **Such lists shall be used only for campaign and political purposes and for reporting to constituents...** (Emphasis added)

PENALTY FOR FALSE STATEMENTS:
Falsely subscribing to any untrue statement required by Title 24.2 of the Code of Virginia is a Class 5 felony under Virginia law. The punishment is a maximum fine of $2,500 and /or confinement for up to ten years. Upon conviction, you lose your right to vote.

_____
signature of authorized contractor representative

_____
name of contracting firm

_____
date

ACKNOWLEDGED BY:

_____
signature of legally qualified purchaser

_____
date

[1]For the protection of any qualified purchaser of a registered voters list or list of those who voted who contracts with any data processing, mailing list, campaign management consulting, or other firm for work with such lists, a representative of the firm must be required to sign the above statement. The original should be forwarded to the State Board of Elections; a copy should be maintained in the purchaser's files.

REV 6/15/95

Appendix G

Written comments and suggestions relating to the feasibility study.

State agencies and Institutions:

- Department of Housing and Community Development
- University of Virginia (Polley Ann McClure, Erv Blythe)
- University of Virginia (Chip German)
- George Mason University

Local Government:

- County of Henrico
- County of Hanover
- City of Norfolk

Organizations:

- Virginia Municipal League
- Virginia Press Association

COMMONWEALTH of VIRGINIA

George Allen
Governor

DEPARTMENT OF
HOUSING AND COMMUNITY DEVELOPMENT

Robert T. Skunda
Secretary of
Commerce and Trade

Warren C. Smith
Director

November 13, 1996

Mr. Charles C. Livingstone
Director
Department of Information Technology
110 South Seventh Street
Richmond, Virginia 23219

RE: SJR 68 "Feasibility Study of Indexing State Databases"

Dear Mr. Livingstone:

The Department of Information Technology's (DIT) draft report on the feasibility and cost for complying with the provisions of SB 326 contains both reassuring and troubling material. The following items are relatively reassuring:

- The report asserts the amendments contained in SB 326 focus on official records that happen to be computer resident and not vice versa. If this view is correct and acceptable to all interested parties, the bill's potential burdens would be greatly diminished.

- The report notes uncertainties about the effect of the bill on existing databases, recommending that only databases created after July 1, 1997 be affected. Greater clarification on this point is required, if for no other purpose than to assure that all of the interested parties have the same understanding of which databases are to be included.

- The report recommends employing a narrow definition of the term "created" to assure that only appropriate computerized databases are subject to indexing. Again, as in the previous paragraph, greater clarification on this point could prevent subsequent misunderstandings.

- The report points out the potential for the indexes to be used to facilitate "data mining", a process of integrating unrelated data sets that could be used for legitimate, questionable, or illegitimate purposes. This caution is timely and appropriate. DIT's suggestion that statutory or administrative rules be used to assure the proper use of materials obtained through the Freedom of Information Act (FOIA) is a reasonable response.

Several other items appear to be unresolved or require additional consideration:

- Although § 2.1-342 does, indeed, address official records, the new language included in HB 326 appears to command the indexing of *every* database, with the index itself becoming an official record. The implication seems to be that any "structured collection of data or documents residing in a computer" might be an official record and that the only way to assure the public's access to these potential official records is to index all of them.

- The equation of official records with public records is troubling. As Senate Document No. 40 pointed out in 1995, the definition of "official record" employed by the FOIA and the definition of "public record" used in the Virginia Public Records Act (VPRA) are not congruent. While this seemed a minor concern in 1995, the breadth of the language used in the VPRA could be construed to make virtually every written (or electronically developed and stored) item a public record.

- That DIT could not develop more detailed estimates of the cost of compliance is not surprising, given the uncertainties surrounding some of the key definitions and program parameters associated with the application of SB 326. The generic algorithms included in the report accurately capture the factors influencing agencies' cost estimates, but the fiscal impact on most agencies will remain uncertain.

- Because the bill simply amended the FOIA, it did not set clear responsibility for developing the rules of the road on how to comply with the act's provisions. In the case of North Carolina, the state's records management agency provided explicit guidance and assistance to affected state agencies. As it stands, agencies will have to decide for themselves how to comply with the indexing provisions of the FOIA as well as the relevant provisions of the VPRA and the Privacy Protection Act (PPA).

DIT's assessment of the impact of SB 326 has been useful in pointing out areas requiring further clarification before agencies embark on the potentially costly activities needed to assure compliance with the new provisions of the FOIA. The goal of assuring public access at a reasonable cost is important. Properly applied, the provisions of SB 326 may advance that public purpose. Much remains to be done to assure that the public is properly served not only by providing access to appropriate information, but also by not expending public resources in ways that neither the authors of the legislation nor the advocates of openness in government in general would require.

Sincerely,

William J. Ernst, III
Policy Analyst

UNIVERSITY OF VIRGINIA

108 Cresap Road • Charlottesville, VA 22903-1710 • Tel. (804) 982-2249 • FAX (804) 924-3579 • Internet: oit@virginia.edu

OFFICE OF INFORMATION TECHNOLOGIES

November 27, 1996

Mr. Charles C. Livingston
Director
Department of Information Technology
110 South Seventh Street
Richmond, VA 23219

Dear Chuck:

Our staffs have communicated our views about SB 326 to appropriate people in your department, but we want to also express our concerns directly to you.

The DIT Feasibility Study of Indexing State Databases identifies many of the issues related to the requirement for public agencies to index all databases. Among the issues discussed is the matter of scope, i.e.: precisely which databases are covered. Our special concern is related to this ambiguity in that if the scope includes significant portions of our electronic data, the cost will be huge. For UVa and Va Tech alone, the initial cost to index all data currently maintained in central mainframe files would significantly exceed $20 million, with ongoing annual costs in excess of $5 million/year. Clearly the value of access to this information in electronic form would have to be very high in light of costs of this magnitude.

Beyond cost issues, we have concerns about the usefulness of such a heterogeneous assemblage of data. We question whether citizens will be able to make sense of comparative information across agencies which will almost certainly differ in data definitions. This relates to the cost issue in that a huge cost could be incurred with little or no benefit to the public.

We believe there are other more effective and efficient ways to respond to the public access issue. We would be glad to explore with you, at a time and place of your convenience, some of these alternatives.

If you would like to discuss these matters in person, we're prepared to meet with you at a mutually convenient time.

Sincerely,

Polley Ann McClure
Vice President and CIO
University of Virginia

Erv Blythe
Vice President for Information Services
Virginia Polytechnic Institute and
State University

To: Art Phaup@IRM@DIT,Stephanie Saccone@HRD@DIT,Bill Endicott@DIR@DIT,Alvin Hunter@TCB@DIT
Cc:
Bcc:
From: Tom Kusiak@TMD@DIT
Subject: FYI: URGENT stance on data indexing
Date: Monday, November 18, 1996 09:05:28 EST
Attach:
Certify: N
Forwarded by: Tom Kusiak@TMD@DIT

Comments :
here is Uva's assessment of sjr 68.

tom
----------[Original Message]----------
To : <tkusiak.dit@state.va.us>
Cc :
From : Chip German <Chip@virginia.edu>
Date : Friday, November 15, 1996 at 5:08:39 pm EST

Tom:

Could you pass this along to the proper folks? It represents the University of Virginia's comments on the feasibility study draft. We appreciate very much the opportunity to make comments.

The University's biggest concern is that the study makes no serious attempt to establish the costs of implementing the legislation statewide. The absence of such information will lead the General Assembly to believe that this activity can easily be absorbed by the institutions and agencies, and nothing could be further from the truth. There is specific information about our estimate of costs to comply at U.Va. in later paragraphs.

The definition of data affected is very broad in the bill's language. It appears to encompass everything from large production databases to spreadsheets on an individual worker's desktop -- as the study notes, anything that could be construed as an official record. As the study draft notes, the data affected by the bill is limited to newly created databases (including systems undergoing major application upgrades or other such changes). This means that U.Va.'s set of major databases will not be affected at first, but over the next few years -- especially if we start a cycle of implementing new systems as many institutions and

agencies are -- all will be. But changeover at the desktop takes place much more frequently. For that reason, after July 1, 1997, there still will be a large (huge may not be an overstatement) of data that -- under the current language -- that must be indexed immediately.

With the publication of a detailed index of databases including information that can only be described as technical and "architectural" in nature, we recognize a serious potential for increased security risks. The additional information about the data that would be included in the index will help enable unauthorized access to the data. If someone succeeded in breaching the entry-level security of our databases (and entry-level security is the only level that the feasibility study draft examines), the detailed information provided gives the intruder essential information on how the data could be altered or damaged as a prank, for profit, or for malice.

Finally, and perhaps most important, neither the legislation nor the feasibility study focuses in practical terms on the public interest behind this legislation. We strongly support the notion of making public information available to the public easily and in understandable form. However, so far the Commonwealth still lacks a sophisticated analysis of how to organize a system that is responsive to the public interest. As a result, under the current language, each institution and agency must invent mechanisms to comply, and in doing so will undoubtedly make it more difficult for the public to understand how to navigate through the entire array of the state's public information.

The costs of complying with this legislation are people/time costs. Some of the people/time is associated with data professionals, but inasmuch as the legislation applies to personal computers as well, much of the people/time cost is associated with individuals who do not work in data services as their primary job for the University.

We estimate that it would cost the University of Virginia approximately $1 million to initially establish the index of data elements centrally maintained in administrative systems, with their giant-sized collections of data elements. For this estimate, we used a lower personnel cost-formula than suggested by the study draft. If we use study draft's suggested rate, the estimate would increase by $200,000.

We estimate that it would cost approximately $10 million to initially establish the index of data elements stored on the desktop throughout the University. (Using the study draft's rate -- which we doubt DIT intended for this part of the process -- the estimate would increase by $1 million.)

Once the entire index is created, we estimate the ongoing annual cost of maintenance for the centrally maintained data elements at approximately $200,000. The ongoing annual cost for maintenance for the data elements stored on the desktop would be approximately $2 million. (Using the study draft's rate, the maintenance for the centrally maintained data increases by $40,000 and the maintenance for the data stored on the desktop increases by $200,000.)

Obviously, there will also be an increased need to respond to questions about the data. Based on our current experiences and projections of increased activity, as well as the need to straighten out the confusion this process is likely to generate, we estimate the additional cost of personnel time associated with responding to requests at $600,000 per year. Much of the time included in this activity will be that required to work with the person inquiring to explain the context of the data and its appropriate use. This figure does not include the costs of simply providing the data itself -- recovery of those costs is already outlined in the Freedom of Information Act.

Obviously the University would not incur all of these costs in the initial year, but given our estimates of changes in administrative systems, we predict that they will become costs that we have to accommodate over the course of the next several years. And, as noted above, because the most highly changeable data is that at the desktop, the biggest costs may indeed be incurred in the earliest phase of implementation.

To summarize our comments:

1. The feasibility study should help the General Assembly understand the likely costs to the Commonwealth of implementing this legislation. Those costs are very large, and will be so even in the early phases of implementation if the current legislative language remains unchanged.

2. The feasibility study should emphasize that the current language defining data affected by the legislation is too broad and for that reason vastly increases the costs.

3. The feasibility study should emphasize that the detail-level of the information (especially technical information) required in the current legislative language for the data index is too fine, leading to vastly increased costs and significantly increased threats to the security of the systems involved.

4. The feasibility study should highlight the fact that the current language does not provide for a consistent, coordinated statewide

environment of publicly accessible information that the public will understand how to navigate. This appears counter to the intent of the legislation and is an issue worthy of deeper examination.

What recommendations do we advise DIT to include in its feasibility study?:

1. Change the language of the legislation to reduce the range of data affected and to reduce the amount of detail required for the index. This would reduce costs by significant proportions while providing great assistance to the public in understanding what information is available. Focusing on a subset of data likely to be of the greatest interest to the public will provide a more useful service faster than the current model. Reducing the detail required also will speed compliance and utility -- the federal Government Information Locator service contains examples of the level of detail that would be much less costly to maintain and much more useful to the public. Data is described at the database level, rather than the data element level. Reducing the technical detail that is present in the index would also eliminate many security concerns.

2. A delay of implementation by at least another year to allow the Council on Information Management to study the best means for providing a statewide information locator service that would be much easier to use and much more effective than the chaotic system likely to emerge from the current language. Given that the legislation as currently written will not immediately apply to the large databases that are likely to be of the greatest public interest, the Commonwealth sacrifices very little in allowing this matter to be explored at appropriate depth.

Thanks again for the opportunity to comment.

Chip

****

R. F. (Chip) German Jr.
Director, Planning and Policy Development
Office of Information Technologies
University of Virginia
108 Cresap Road
Charlottesville, Va. 22903-1710
(804) 982-2638 (voice), (804) 924-3579 (fax)
Internet: chip@virginia.edu

****

George Mason University

4400 University Drive
Fairfax, Virginia 22030-4444

December 13, 1996

Mr. Charles C. Livingston
Director
Department of Information Technology
Richmond Plaza Building
110 South 7th Street
Richmond, Virginia 23219

Dear Mr. Livingston,

Thank you for including George Mason University (GMU) in the "SJR 68 Feasibility Study" meeting held in Richmond. The following document is presented as GMU's response to the Department of Information Technology's draft copy of the "Analysis of Feasibility of and Cost Associated with Requiring Public Bodies to Compile Indices of Certain Databases (SJR 68)."

Please include the attached document as an appendix to the final draft of the study. Should you desire further information or clarification of this submission, please contact either myself or Jeanette Blanchard at (703) 993-3439.

Sincerely,

Keith B. Segerson

Keith B. Segerson
Executive Director
University Computing & Information Systems

George Mason University
(703) 993-3400
segerson@gmu.edu

attachment:

(ditindx1)

George Mason University

4400 University Drive
Fairfax, Virginia 22030-4444

December 13, 1996

Executive Summary

George Mason University (GMU) is concerned that the definition of what constitutes a database, for purposes of SJR 68, is too broad to permit effective systems analysis, design, and implementation by July 1, 1997.

The scope of the resolution is broad and unclear. Subsets of data can be construed as databases in their own right, and in a distributed data environment, control over derivative data is nearly impossible to achieve without rigorous standards and procedures that regulate the use of data derived from "official" databases.

Establishment of database indices requires agencies to engineer appropriate security and data integrity safeguards. The cost to complete a project that will achieve these safeguards is measured in personnel costs. Given the current vague definition of what constitutes a database, for the purposes of implementing SJR 68, there is no basis for designing and implementing an adequate system.

GMU concludes that it is technically feasible to establish database indices, but not operationally feasible until issues of security, data mining, and definition of scope are completed. Economic feasibility cannot be determined now, but the design of a control project of this magnitude is likely to be several man years. Economic feasibility must be weighed in the context of commitments to ongoing support and preparation for Year 2000 compliance.

GMU recommends that:

* Implementation, of SB 326, be delayed until further review and discussion be completed.

* A committee be established, composed of state agencies, local governments and special interest groups, to iron out the details of this concept to ensure that ultimate deliverables meet intended requirements.

Background and Details

Based on the information in the Department of Information Technology's Draft copy of the *"Analysis of Feasibility of and Cost Associated with Requiring Public Bodies to Compile Indices of Certain Databases (SJR 68)"* and the discussions at the *SJR 68 Feasibility Study Meeting* (12/4/96), we have determined the following to be some of the major unresolved issues facing state agencies and the Commonwealth of Virginia.

Issues:

1. Feasibility.

It is stated in the DIT draft report that "a feasible task is defined as one which is possible, suitable and logical." This is a difficult question to answer. In order to attempt to answer this question we need a clear definition of what the problem is that we are trying to resolve. Once the problem has been clearly defined, then we need a clear description of what is the expected result or outcome. If we know what the problem is (Point A) and what the desired end result is (Point B), then we can determine what is the best way to get from Point A to Point B. This will assist us in determining the feasibility of this project. Unfortunately, this issue is even more complex with the addition of a compliance date of July 1, 1997. Feasibility can not be determined without the inclusion of the compliance date.

2. Conflicting Wording.

The wording of SB 326 (Chapter 469) and SJR 68 are in direct conflict of each other.

SJR 68 states ... an index of computer databases maintained or created by them *before, on, or after* July 1, 1997.

SB 326 (Chapter 469) states "Beginning July 1 ,1997, every public body of state government shall compile, and annually update, an index of computer databases which contains at a minimum those databases created by them *on or after* July 1, 1997."

Which data range is correct? Are we to include databases prior to July 1, 1997?

3. Definition of Terms.

There are no clear definition of terms in this legislation.

What is a "database"? Is it all records housed on a computer (from Mainframes to standalone Personal Computers)? Are spreadsheets, word processor documents, organizers, e-mail, voice mail, among other types of files considered databases? Is the results of a query from a database or from multiple relational databases considered a database?

What does "certain databases" mean? Are some databases excluded? Who determines which databases are included or excluded?

What does "created" mean? Does it mean that it never existed before? Is a modified or redesigned database considered created?

What is the distinction between "Official Records" and "Public Records"? Are all files on a state owned computer considered official records?

4. Security Risks.

What are the possible security risks to the data and to the individual computers? If we give data in electronic form, how do we ensure data integrity?

5. Data Mining.

What are the implications for data mining. Can we deter data mining?

6. Cost Analysis.

There is no clear way to determine the cost of this legislation based on the above unanswered questions.

7. Implications/Liabilities related to Privacy Protection, Confidentiality and other agency specific laws.

What are the implications for privacy protection, confidentiality and other agency specific laws (such as, laws related to student information). Would legal review be required to determine what database field information can be released and what field information would be in violation of various laws?

Conclusion:

It is probably not feasible to establish full compliancy by July 1, 1997. The realistic date for compliancy will depend upon the size of the agency, the definition of a "database", the definition of "created" and whether or not databases, established prior to July 1, 1997, are intended to be included. There will be less that 6 months to implement and comply with something that is not clearly defined.

GMU is concerned over the potential cost (manpower & resources) potentially required to fulfill this database indexing deliverable, as currently outlined. Given the weakness and fluidness of definition, costs could be very high, relative to each agency - large or small.

Finally, the most important issue is whether or not this initiative, however defined, will really provide benefit to the Citizens of the Commonwealth of Virginia. Until further review and discussion is completed, this determination can not be finalized. It is critical to fully define the requirement prior to mandating action by all state agencies.

Recommendation:

1. Delay implementation of SB 326 (Chapter 469) until a complete analysis (of the initiative, scope, definitions, costs and deliverables) can be presented to the General Assembly for review and consideration.

2. Create a committee (composed of state agencies, local governments and special interest groups) to accomplish the following:

   a. Clearly define the Problem.
      (What is the problem that this legislation is trying to solve?)
   b. Clearly define the Result.
      (What information will this index record really produce - actual data?)
   c. Clearly define terms (such as, "database" and "created" among others).
   d. Clearly define and create guidelines.
   e. Determine where the index will reside.
   f. Determine hardware and software issues for the index.
   g. Propose hardware and software for the index.
   h. Determine the security issues/risks.
   I. Develop an Impact Study to determine or estimate the cost to implement. (Possibly prototype a mid-size agency for problems, cost, manpower, and man-hours)
   j. Develop a proposed implementation schedule for state agencies.
   k. Present the findings to the General Assembly for review and action.

Respectfully Submitted,

George Mason University
University Computing and Information Systems

(ditindex)

Data Processing Department
County of Hanover
P. O. Box 470
Hanover, Virginia 23069-0470

Data Processing Telephone Numbers:
(804) 537-6015 (804) 730-6015
FAX (804) 537-5203

December 9, 1996

Mr. Chuck Livingston
Dept. of Information Technology
Commonwealth of Virginia
110 S. 7th Street St.
Richmond, VA 23219

Dear Mr. Livingston:

Thank you for the opportunity to participate in the discussion meeting and to offer comments on the SJR68 feasibility study. Attached are my comments on the draft of the study. These comments have been reviewed with other local government participants in the meeting, including Bill Cleveland of Goochland, Pam Staggs of Norfolk and Mary Jo Fields of VML. These comments will be reviewed with the LGAC on December 12, 1996.

Following are comments which are submitted to DIT, with the request that these be included in the study:

1. Based on a brief evaluation by two local governments (i.e., Hanover and Norfolk), legislation produced as a result of SJR68 would have a very significant impact on local governments, requiring hundreds of staff-hours to create the index for thousands of data elements maintained at each locality. The cost to comply would be extremely high for local governments.

2. Local governments believe the study requested by SJR68 must include a discussion and determination of the cost effect on local governments. This conclusion is based on the mandates of SJR 68 that directs the staff performing the study to:

   (a) "study the feasibility of and costs associated with requiring public bodies to compile, and annually update, an index of computer data bases"
   (b) "seek the participation and input of local government representatives"

3. If the study concludes that the base definitions of SJR68 are not clear enough to determine the cost effect on either State or local government bodies, then the study should state that these base definitions are not clear enough to determine costs and that the study should be extended until joint discussions with the proponents of the bill and representatives of State and local government can work together to determine the proper definitions and to study the cost impact of SJR68.

4. The study indicates that it would be feasible to implement the index for data bases created after July 1997. Local governments believe that costs should be evaluated, as the study mandates, before stating that the indexing of data bases created after July 1997 is feasible.

Again, I appreciate the opportunity to participate in the discussions on the feasibility study and would appreciate the inclusion of these comments in the study. Please contact me if you have any questions regarding these comments.

Sincerely yours,

Ben Blanton

Ben Blanton, Director
Data Processing Department

BB/s

cc: Bill Cleveland, Goochland & LGAC Chair
Pam Staggs, Norfolk
Tom Tokarz, Henrico County
Mary Jo Fields, VML
Clay Wirt, VML
LGAC to CIM

COMMONWEALTH OF VIRGINIA
COUNTY OF HENRICO

OFFICE OF THE COUNTY ATTORNEY

JOSEPH P. RAPISARDA, JR.
COUNTY ATTORNEY
JOHN L. KNIGHT
DEPUTY COUNTY ATTORNEY
GEORGE T. ELMORE, III
J. T. TOKARZ
RHYSA GRIFFITH SOUTH
KAREN M. ADAMS
JAMES T. MOORE, III
PHYLLIS A. ERRICO
ASSISTANT COUNTY ATTORNEYS

PARHAM AND HUNGARY SPRING ROADS
P.O. BOX 27032
RICHMOND, VIRGINIA 23273-7032
(804) 672-4342
FAX (804) 672-4140

November 14, 1996

Mr. Charles C. Livingston
Department of Information Technology
110 S. 7th Street
Richmond, Virginia 23219

Re: *Draft of Analysis of Feasibility of and Cost Associated with Requiring Public Bodies to Compile Indices of Certain Computer Databases*

Dear Chuck:

Thank you for the opportunity to comment on the draft analysis prepared by the Department of Information Technology in response to SJR 68. Because the draft analysis has not been formally released for public review, these comments should be viewed as preliminary given the complexity of the issues raised in the analysis. These comments have not been reviewed by the County's Department of Data Processing, any other local data processing department, the Virginia Municipal League, or the Local Government Attorneys' Association of Virginia, but I hope to have their input prior to the commencement of the General Assembly.

Yours truly,

J. T. Tokarz

cc: Brian D. Wantling, Henrico Department of Data Processing
Ben A. Blanton, Hanover Department of Data Processing
Pamela S. Staggs, Norfolk Department of Information Systems
Clay Wirt, Virginia Municipal League

PRELIMINARY COMMENTS ON OCTOBER 30, 1996 DRAFT
OF
ANALYSIS OF FEASIBILITY OF AND COST ASSOCIATED WITH REQUIRING PUBLIC BODIES TO COMPILE INDICES OF CERTAIN COMPUTER DATABASES

The October 30, 1996 Department of Information Technology ("Department") draft of the study required by SJR 68 ("Analysis") raises significant issues with potential impacts on local political subdivisions. Although the 1996 amendments to Va. Code § 2.1-342 concerning database indexing only apply to state government, the SJR 68 study applies to all "public bodies." Because the General Assembly may be asked to extend Chapter 469 of the 1996 Acts of Assembly to localities, these preliminary comments address those issues and impacts.

I. *The full impact of the legislation on localities requires careful study and meaningful input from the affected jurisdictions.*

SJR 68 requires the study to "seek the participation and input of local government representatives." To date, the participation and input of local government representatives has consisted of one meeting on October 30, 1996 in which the Department provided the draft Analysis to local government representatives. Unfortunately, because of the timing of this meeting and the deadline for comments, there has been insufficient time for local directors of data processing and their attorneys to review the draft Analysis.

II. *The Analysis does not address the unprecedented conversion of the Virginia Freedom of Information Act ("Act") from a tool for obtaining access to existing public records to a mechanism mandating the creation of new records.*

Page 6 of the Analysis contains a discussion of the Act which incorrectly states that the 1996 amendments were to correct an "apparent gap in citizen access" under the Act because citizens "may not know of or be aware of official records stored on computers." The discussion is incorrect because there is no "apparent gap" peculiar to computer records. Citizens may not know of or be aware of

particular official records maintained on paper and there is no way of solving this "problem" short of indexing every public record in whatever form it is maintained.

Prior to 1996, the Act clearly provided that public bodies did not have to create new records to comply with the Act. This simple rule recognized that public bodies do not have unlimited time or resources to act as *ad hoc* information generators while it preserved the public's right to access existing public records. The 1996 amendments mandating the creation of database indexes fundamentally changes this careful balance established in 1968 and may presage the imposition of new information creation burdens on state and local agencies. The logic of the 1996 amendments suggests that public bodies may eventually have to index *all* public documents, including Post-It™ notes and e-mail messages, in the interest of greater public access. The Analysis should recognize and comment upon this possibility.

III. *The Analysis does not address the inherent conflict between the* 1996 *amendments and other language in Va. Code* § 2.1-342(A).

Va. Code § 2.1-342(A) provides that public bodies "may, but shall not be required to, abstract or summarize information from official records." This language is clearly contrary to the 1996 language which requires indexes of every database maintained by a state public body.

IV. *The Analysis does not propose solutions to drafting problems in the* 1996 *amendments.*

The Analysis correctly points out on pages 11 and 12 that the 1996 legislation left important questions unanswered. If legislative amendments are necessary, the Analysis should propose specific language.

V. *The Analysis incorrectly states that "what constitutes a database as related to the wording in SB 326 is not as important as what constitutes an 'official record.'"*

For purposes of the Analysis, the definition of "database" is all-important because it is the definition which will delineate the reach of new document requirements on public bodies.

VI. *The Analysis incorrectly discounts the potential problems caused by the use of improper methods in data mining.*

In discussing the intended uses of data derived from data mining on page 12, the Analysis incorrectly states that the processes used for integrating different databases do not pose a risk. As Mark Twain said.
, there are lies, damn lies, and statistics, and there is a risk of incorrect data manipulation that should not be totally discounted as the third full paragraph on page 12 of the Analysis does. Ironically, the risk of improper data manipulation is then demonstrated in the examples listed on page 13.

This is not to say that public information should be withheld because people may reach wrong conclusions from it or even because the information may be wrong. Public bodies do not warrant the accuracy of their records and cannot prevent improper or misleading use of public information. However, there is a risk of improper processing that is not recognized to the first sentence of the third full paragraph on page 12.

VII. *The Analysis does not discuss the cost of indexing databases in personal computers or other computers in sufficient detail.*

While the Analysis contains some general information about data in different types of computing environments, the information is so general as to be of little use. The Analysis gives no indication of the cost of preparing the index for a single database, how many databases are being maintained by users, and how many users there are who have computer databases. There is simply no way for the General Assembly to use the draft Analysis to determine the cost and feasibility of its legislation in this area.

This is not intended as a criticism of the Analysis because it is difficult to envision how to compile the necessary information without surveying every employee who uses computers. Rather, it points out the lack of reliable information as the General Assembly wades into uncharted territory. For this reason, it seems prudent to see how states like North Carolina and Florida implement similar legislation before imposing a significant new burden on state public bodies.

J. T. Tokarz
Henrico County Attorney's Office

City of Norfolk
Department of Information Systems

December 13, 1996

Mr. Chuck Livingston
Department of Information Technology
Commonwealth of Virginia
110 South 7th Street
Richmond, VA 23219

Dear Mr. Livingston:

I appreciate the opportunity to take part in the SJR68 Feasibility Study discussion meeting, on December 4, 1996, and to provide comments and input into the study.

It is clear that considerable analysis was done in preparing the study, but my initial review has identified some impacts to local governments that are not addressed.

Please review and consider the following comments for inclusion in the feasibility study of indexing databases:

1. Definitions and Guidelines: In order to determine costs to local government, definitions and guidelines need to be developed. As SJR68 is written, it is not clear what automated files would need to be included.

2. Costs: If every automated file needs to be indexed then the personnel costs would be high, not only for Information Systems, but for the City Attorneys staff as well. Although the study presents a cost model, considerable analysis will be required by localities in order to use the model and determine the actual cost to them.

3. Feasibility: The study approaches feasibility from the perspective of can it possibly be done. There is another component though, can it reasonably be done. Without good cost projections, including staff requirements, feasibility cannot be determined. If enacted as written, this could become a very costly unfunded mandate, which is probably not the intention of the bill and runs counter to another State goal "no unfunded mandates."

401 Monticello Avenue / Norfolk, Virginia 23510-2408
(804) 664-4500 / Fax: (804) 664-4567

4. Freedom of Information Act (FOIA): As written, this bill would require the creation of information, which is a departure from the current implementation of FOIA. Isn't this policy change an unintentional result of this bill? Since we are talking about information that does not exist at this time, a precedent will be set to create data.

Thank you for the opportunity to comment, and raise some questions that are in my mind. Please let me know if you have any questions or need additional information.

Sincerely,

Pam Staggs

Pam Staggs
Assistant Director

December 11, 1996

Mr. Chuck Livingston
Director, Department of Information Technology
110 South 7th Street
Richmond, VA 23219

Dear Mr. Livingston:

Thank you for the opportunity to comment on the draft of the study prepared by the Department of Information Technology on the indexing of computer databases.

We appreciate the difficulties the department faced in undertaking this study. The study according to SJR 68 asks the department to study the feasibility and costs associated with requiring public bodies, including local governments, to develop indexes to computer databases. At the same time, SB 326 instructs the department to develop guidelines for the implementation of computer indexing for state agencies.

The study raises several major policy issues that deserve further attention, including the definition of a computer database, whether the indexing requirements should extend to data maintained on central computers or to every personal computer in an office, the potential hazards of data mining and potential conflict with privacy statutes.

In addition, we feel there are additional policy questions that should be addressed before making a decision to require indexing.

The required production of an index means that Virginia's Freedom of Information Act for the first time requires the production of a record. For this reason we disagree with the study's statement on page 4 that "SB 326 simply makes access to this existing information easier." A requirement to index changes the intent of the current freedom of information statute from one of ensuring access to public documents to the production of information. This policy issue is one that deserves further consideration in determining the feasibility of the production of indexes.

We also question the information on page 9 regarding the passage of similar legislation in Iowa, Texas, Missouri and California. A check with these states revealed that recent changes have been made regarding access to records maintained on a computer, but not to require the production of indexes.

The discussion of official and unofficial documents on page 10 is somewhat confusing in that it seems to indicate that the indexing requirement would not extend to all documents, but only "official" ones. Under FOIA, information is open to the public

THIRTEEN EAST FRANKLIN
P.O. BOX 12164
RICHMOND, VIRGINIA 23241
804/649-8471
FAX 804/343-3758
E-MAIL VML@VISION.COM

unless a determination is made that the information can be withheld from public release because it falls under one of the exemptions. This is broader than what seems to be covered by the discussion of "official" documents in the study.

Further, the study does not document the costs associated with indexing. It is not fiscally prudent for a government to set a course of action without having some notion of the immediate and long-term costs required by the action. It is particularly ill-advised for the state to require local governments to undertake activities whose costs are unknown. Given that the study did not include local governments until the end of the process, and that no cost estimates were prepared, we believe a reasonable conclusion the study should have drawn is that it is not feasible to require local governments to prepare these indexes at this time.

We would like to point out that Virginia's experience with indexing is very different in several respects from North Carolina's, which adopted indexing requirements as part of a larger, overall re-vamping of its open records laws. The guidelines for the implementation of the statute were developed in concert by state and local officials. The requirement to index is being phased in over a period of several years. The requirement does not apply to databases created before the enactment of the legislation. The legislation is only just taking effect in North Carolina, so there is not enough information yet available on problems with its implementation.

We feel that the General Assembly does not have enough information to proceed with the concept of requiring computer indexes, so for this reason we feel the study should recommend a postponement of the date of implementation of SB 326. We also oppose the expansion of SB 326 to include local governments, because so many major policy and fiscal issues regarding indexing remain unanswered.

Again, thank you for the opportunity to comment on this report.

Sincerely,

Mary Jo Fields

Mary Jo Fields
Director of Research

Virginia
PRESS
Association

Serving the newspapers of Virginia

November 15, 1996

Charles C. Livingston, Director
Department of Information Technology
110 South Seventh Street
Richmond, Virginia 23219

Dear Mr. Livingston:

I transmit, under cover of this letter, the Virginia Press Association's comments to the draft analysis of the Department of Information Technology concerning compliance with SB326. VPA has always placed a priority on clear understanding of the Virginia Freedom of Information Act, Its interrelationship with other laws, and its underlying policy. Because we believe a number of the statements made in the DIT draft analysis are inaccurate, we have attempted to clarify those points so that the report might be corrected accordingly.

We regret that we did not have the opportunity to comment at an earlier date. Our understanding of the process was that the Virginia Press Association would be a participant in this work. As you know, our executive manager or other VPA designees attempted on several occasions to attend announced meetings of the working group. Those meetings were either postponed or canceled, depriving VPA of an opportunity to participate. Thus, it is not clear to us what process led to the preparation of the draft report. We note that the draft has been circulated to a large number of individuals, and it would be disappointing to learn that any of those individuals had knowingly participated in the preparation of this material with an intention to exclude the VPA.

We hope that you will give careful consideration to VPA's comments. If you have any question whatsoever about VPA's position, I invite you to call me or executive manager, Ginger Stanley, and we can arrange for one or more members of our Freedom of Information committee to meet with you.

Sincerely yours,

John Edwards

P.O. Box 85613, Richmond, VA 23285-5613 • 804-550-2361 • FAX 804-550-2407

VIRGINIA PRESS ASSOCIATION COMMENTS ON THE DEPARTMENT OF INFORMATION TECHNOLOGY'S DRAFT FEASIBILITY ANALYSIS REGARDING COMPLIANCE WITH SENATE BILL 326

The Virginia Press Association offers these comments concerning a document prepared by the Department of Information Technology entitled Analysis of Feasibility of and Cost Associated With Requiring Public Bodies to Compile Indices of Certain Computer Data - bases (SJR68) (hereafter referred to as the "DIT Analysis"). The document was transmitted to the Virginia Press Association on November 7, 1996. Comments were requested no later than November 15, 1996.

EXECUTIVE SUMMARY

The General Assembly has spoken clearly in its passage of Senate Bill 326. SB326 reflects the natural evolution of freedom of information law in the Commonwealth of Virginia, which has been a leader in the field of access to electronic records for over two decades. The DIT Analysis, required by SJR68 (1996 Session), proceeds from a "can't do," rather than a "can do," mindset. VPA directs its comments to two aspects of the DIT Analysis, which are discussed in detail below:

(1) The DIT Analysis does not accurately present current Virginia law, nor does it accurately characterize SB326. As a result, the DIT Analysis suggests that there are conflicts between Virginia freedom of information law and privacy protection law which do not in fact exist. The DIT Analysis also suggests that SB326 was a new departure in the area of access to electronic information, when in fact SB326 imposed no new access requirements on any public body.

(2) The DIT Analysis fails to evaluate the practical effect of SB326 on any agency. While SB326 imposes indexing requirements on state agencies subject to the Virginia Freedom of Information Act, the DIT Analysis provides no information concerning the actual difficulty or cost of compliance in the context of a single Virginia state agency. Instead, DIT offers a series of abstract reasons why compliance with the new law will be difficult. In fact, the concerns raised by DIT are unrelated to any requirement imposed by SB326.

SPECIFIC COMMENTS CONCERNING DIT ANALYSIS

I. The DIT Analysis Presentation of Virginia Freedom of Information and Privacy Statutes is Incorrect.

The DIT Analysis misstates Virginia law and public policy on freedom of information and privacy. Because the DIT Analysis is premised on DIT's understanding of these laws, VPA offers the following considerations.

(1) The Virginia Freedom of Information Act (VFOIA) contemplates broad access to a maximum number of official records. The long-stated policy of the VFOIA is set forth in Virginia Code Section 2.1-340.1.[1] The Act is to "be liberally construed to promote an increased awareness by all persons of governmental activities and afford every opportunity to citizens to witness the operations of government. Any exception or exemption from applicability shall be narrowly construed in order that no thing which should be public may be hidden from any person." Va. Code §2.1-340.1. The exemptions in the VFOIA are not mandatory, but discretionary, presuming that public officials will not automatically apply exemptions whenever the opportunity presents itself. See Va. Code §2.1-342.B. DIT presents a "watered down" characterization of this policy. For example:

---

[1] Copies of the following Code provisions are attached as Exhibit A to this document: Va. Code §§2.1-340.1; 2.1-341; 2.1-342.

- "Under FOIA, information about government policies and agency processes that does not involve data about individuals and private organizations must be readily available to the public." DIT Analysis at 4 (emphasis added).
- "The intent of FOIA is to ensure that Virginia citizens have access to most information collected by their government (both state and local)." DIT Analysis at 6 (emphasis added).

First, VFOIA, while it provides exemptions for certain categories of information, has never prohibited access to official records solely because some records contain data about individuals or private organizations. In fact, much of the VFOIA would be eviscerated were this the case. Second, all information, not "most" information, is subject to the Act if it is in the possession of a public body not excluded by Va. Code §2.1-345.

(2) The term "official records" is clearly defined in the VFOIA:

> "Official records" means all written or printed books, papers, letters, documents, maps and tapes, photographs, films, sound recordings, reports or other material, regardless of physical form or characteristics, prepared, owned, or in the possession of a public body or any employee or officer of a public body in the transaction of public business.

Va. Code §2.1-341 (1996 Supp.). The DIT Analysis introduces the term "public records" and equates it with "official records." DIT Analysis at 9. The term "public records" is not used in the VFOIA, and its use in the DIT Analysis confuses the discussion.[2] More important is the fact that the VFOIA does not distinguish "official" from "unofficial" records as the DIT Analysis does at pages 9 and 10. The VFOIA definition of "official records" was written by the General Assembly

---

[2] "Public records" is a defined term in other sections of the Virginia Code. See, Va. Code §42.1-77. Whether the "official records" definition in the VFOIA means the same thing as the "public records" definition in the Virginia Public Records Act is an interesting academic point, but irrelevant to SB326 or to interpretation of VFOIA in general.

to include all records. Thus, the discussion at page 10 of the DIT Analysis, and the accompanying matrix, which attempt to define the potential scope of SB326, are not meaningful under VFOIA. By its plain terms, SB326 applies to all records residing in a computer database.[3]

(3) The VFOIA has expressly provided for access to computerized records for over twenty years. In 1974, House Bill 3 amended the definition of "official records" to state that all records, "regardless of physical form or characteristics," are encompassed by the Act. See 1974 Acts of Assembly, Chapter 332. In 1989, the General Assembly passed amendments recommended by Delegate Axselle's study group to clarify procedures for providing access to electronic information. See 1989 Acts of Assembly, Chapter 358.

The DIT Analysis is wrong when it states that "under SB326, the FOIA has been expanded to address access to information on state databases." DIT Analysis at 4. FOIA has required such access since at least 1974. For the same reason, the DIT Analysis is incorrect when it states that "the FOIA statutes initially established in 1968 and significantly strengthened in 1976 and 1979 envision access to information in traditional paper format." DIT Analysis at 6.

SB326 did not add to or diminish access to official records residing in an electronic database. It simply established a new requirement that certain public bodies subject to the VFOIA create an index of database materials in order to facilitate preexisting public access.

(4) The Privacy Protection Act, Va. Code §2.1-377, et seq., ("PPA") passed in 1976. See 1976 Acts of Assembly, Chapter 597. The PPA is designed to prevent the maintenance of secret government information systems, to discourage the unnecessary collection

---

[3] "Computer database" is now a defined term under Va. Code §2.1-342, as a result of the passage of Senate Bill 326. The definition of "computer database" is relevant to the scope of Senate Bill 326. This definition is discussed further in Part II below.

of personal information,[4] and to provide simple procedures for individuals to access and correct information the government holds about them. A number of significant governmental entities, including courts, professional licensing agencies, the Parole Board, the State Police, the Department of Corrections and the Virginia Economic Development Partnership, have obtained exemptions from the PPA. See Va. Code §2.1-384 (1996 Supp.).

The purpose of the PPA is to establish fair, nonintrusive information practices within the record keeping agencies of the Commonwealth. As the Supreme Court of Virginia has noted, the PPA "does not render personal information confidential," nor does it "generally prohibit dissemination of information." Hinderliter v. Humphries, 224 Va. 439 at 447, 297 S.E.2d 684 (1982). Although accuracy of information is addressed by PPA, DIT's analysis emphasizes accuracy of information as the driving force behind the Act. See DIT Analysis at 7. This overstates a secondary issue that was far overshadowed by the more fundamental concern over individual privacy. The statement at page 12 of the DIT Analysis that "the PPA restricts government from releasing 'personal information,'" is simply wrong. The PPA defines "personal information." It subjects "personal information" to rigorous record keeping requirements. It prohibits the collection of certain categories of "personal information" relating to religion and political views. The only limit on dissemination is that it must be made "to accomplish a proper purpose of the agency." See Va. Code §2.1-380.

---

[4] The PPA defines "personal information" as "all information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration whose use could not be such as to effect adversely any data subject nor does the term include real estate assessment information." Va. Code §2.1-379.2.

DIT's lack of clarity over the VFOIA and PPA has profound consequences for its analysis of Senate Bill 326.

First, it improperly suggests conflict between VFOIA and the PPA when in fact none exists. PPA imposes procedural requirements on state agencies and discourages unnecessary collection of personal information. PPA encourages data accuracy by giving data subjects access to records. Under PPA, agencies may always disseminate personal information if to do so is "necessary to accomplish a proper purpose of the agency." Va. Code §2.1-380. VFOIA compliance is certainly a proper purpose, and the VFOIA provides agencies of the Commonwealth with discretion to withhold confidential personal information where the General Assembly has deemed it appropriate. See Va. Code §2.1-342.B. (setting forth 63 categories of exempt records, including a number of categories relating directly to the protection of personal privacy). Any purported conflict between the two laws is a red herring, and SB326 does not diminish (or even address) either the protection of privacy or data accuracy.

Second, the DIT analysis suggests that SB326 plowed new ground by expanding VFOIA to permit access to electronic records. In fact, the General Assembly dealt decisively with this issue two decades ago in a remarkably prescient manner, providing Virginia with a modern regime for access to computer records. Public access to computer-based records has been granted routinely by public bodies since that time. Moreover, the principle of access to records in electronic format has been affirmed by the Supreme Court of Virginia. See Associated Tax Services, Inc. v. Fitzpatrick, 236 Va. 181, 372 S.E.2d 625 (1988) (requiring access under VFOIA to real estate assessment information on computer tapes). The only new requirement of SB326 is that state agencies create a plain language index of computer database information as a means of assisting the public to understand the scope of information under agency control.

II. The DIT Analysis Overstates Feasibility Problems and Fails to Address Implementation Costs.

The DIT analysis raises concerns in four specific areas: (1) the absence of clear definitions, (2) the possibility of "data mining," (3) resource demands created by compliance, and (4) computer system security. Each of these is addressed in turn.

(1) At page 11, the DIT Analysis states that two terms beg definition: (a) "created on or after July 1, 1997," and (b) "database."

With regard to the first definition, DIT queries whether a database may be considered "new" only if it never existed before July 1, 1997. DIT later implies an answer to its own question. At page 18 it recommends that only databases created after July 1, 1997 (the very language of the statute) be affected, suggesting that DIT has some undisclosed definition of "creation" in mind. DIT states that there is guidance in CIM Guidelines 91-3 and 91-4, but fails to attach those guidelines or discuss them in a useful way. VPA has no objection to any rational, verifiable standard for identifying when a database is "created." VPA strongly cautions against any rule or procedure that discourages compliance by encouraging strained semantic distinctions.

The definition of "computer database" is reduced to the absurd in the DIT Analysis. Presumably, creative minds can construe a computer database as "any collection of data, from clipboard collections to desk organizers," DIT Analysis at 11, but part of the charge to DIT under SJR68 is to study the feasibility of requiring public bodies to compile indices of computer databases. Presumably, a study of feasibility requires DIT, in conjunction with other state agencies, to address this very point, proposing practical limitations on the materials which should or should not be considered significant enough to be subjected to indexing requirements. It may be impracticable to index every data field in every freestanding microcomputer. However, it may

be entirely practical to provide a plain English summary of the contents of significant databases maintained on mainframes or local area networks within state agencies. To simply say that the term "computer database" is capable, under a broad and unlimited construction, of encompassing all sorts of matters, is to evade responsibility for grappling with practical application of the new law.

(2) The concern over "data mining" reflects a mindset completely at odds with Virginia's tradition of broad democratic participation in an open government, and its long-standing refusal to ferret out the motives of citizens who seek information from their government. The DIT Analysis, at page 12, states: "It is not the process itself which poses the risk. It is the **intended** use of the resulting product that should be examined." (Emphasis in original.) To VPA's knowledge, no elected official in the history of the Commonwealth of Virginia has taken the view that it is the function of the government to inquire into the intended use of public information acquired by citizens of the Commonwealth. The DIT Analysis suggests that DIT has no objection to "data mining" as long as the databases can only be "mined" by the State.

The pejorative use of the term "data mining" to describe the ability to make correlations between different sets of data merits comment. First, this ability has long been in existence. It is not affected in any way by the requirement of SB326 that indices be created. Second, the very characteristic that makes modern computers a useful tool for business, industry, academia, news organizations and the public at large is the capacity to draw inferences from data to analyze human behavior. The view that this process should be discouraged by Virginia policy makers is directly at odds with Virginia's tradition that an individual's use of information is not the government's business, and contrary to the reality of an ever expanding capacity for individuals and businesses to use information in new and creative ways.

(3) The DIT Analysis identifies three self-evident factors which will influence the cost of creating database indices: (1) the age of the database, (2) the complexity of the database , and (3) the architecture of the computer system in which the data resides. The DIT Analysis is silent on the actual costs of complying with the changes required by SB326. Determining the "feasibility of and cost associated with" complying with SB326 was the objective of SJR68. Thus, it is surprising that DIT has not attempted, in conjunction with one or more state agencies, to provide concrete information on the estimated costs of undertaking the indexing task required by the new law. The DIT Analysis assigns this task to the agencies, stating in jargon that the agencies "interested in broaching the actual cost of resource allocation" can "define the multiple variables and create an algorithm based on a simultaneous linear equation problem." DIT Analysis at 15. Whether DIT sat down with any particular agency in an attempt to create a concrete estimate of the work required to comply with the law, and the costs associated with that work, is unclear. If that work has been done, even in part, it would be extremely useful to the General Assembly and to other interested constituencies such as VPA to have the benefit of that work for comment or independent analysis.

A logical starting point might be a survey of selected agencies to determine what descriptive information presently exists. An integral task in designing and implementing computer systems is the preparation of descriptive material identifying data fields. VPA members have interacted with various public officials who operate computer systems, and surmise from those contacts that much, if not all, of the information needed to create simple indices already exists.

DIT has also failed to consider cost savings driven by indexing. Information management could be improved to some degree by better knowledge of available databases, perhaps

discouraging reinvention of the wheel by agencies. As the DIT Analysis now stands, it does not reveal a significant effort to study cost of feasibility.

(4) The discussion of security risks identifies a set of problems that do not relate to the requirements of SB326. SB326 simply requires a plain, English language description of certain categories of material maintained in computer databases by state agencies. It does not require disclosure of "descriptions of underlying electronic file structures" that would be necessary for the manipulation of computer data files. Nor does SB326 address online access to databases. Each of the risk scenarios set forth at pages 15 and 16 of the DIT Analysis assume circumstances where computer hackers have online access to electronic information or access to information describing database architecture. If these problems exist (and DIT concedes that technology can address them), SB326 has no effect on them.

CONCLUSION

The DIT Analysis does not accurately state the law in Virginia on the issues of freedom of information and privacy protection. Nor does the analysis grapple seriously with the two matters assigned to DIT by the General Assembly: the costs and feasibility of implementing SB326. Instead, the analysis sets out a number negative scenarios which do not flow from requirements imposed by SB326. The DIT Analysis seems to reflect a fundamental disagreement with the information policies embodied in Virginia law, and a desire to offer reasons for noncompliance. VPA urges DIT to develop specific proposals to move state agencies promptly in the direction commanded by the General Assembly.