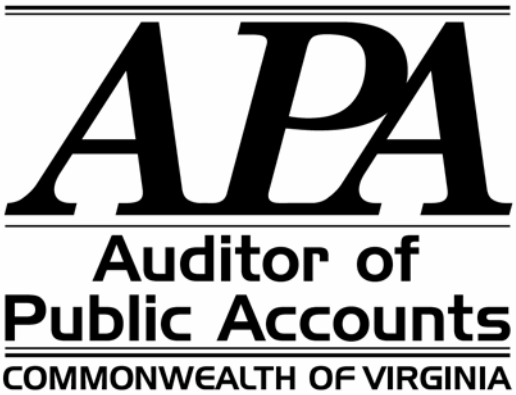
VIRGINIA DEPARTMENT OF HEALTH

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2005



AUDIT SUMMARY

Our audit of the Virginia Department of Health for the year ended June 30, 2005, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System;

- weaknesses in internal controls that require management's attention and corrective action;

- no instances of noncompliance with applicable laws and regulations; and

- the Department has taken adequate corrective action for one of two prior year audit findings.

- T A B L E O F C O N T E N T S -

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Controls for Removing Systems Access in a Timely Manner and Document Access Authorizations

The Virginia Department of Health (Health) did not remove in a timely manner or properly authorize staff access to critical systems. Health has policies and procedures addressing both deletion and authorization of access, but failed to follow them. In our testing, we found:

- seven instances where the auditor was not provided with any systems access removal or authorization documentation;
- one instance where the system access request form lacked proper authorization signatures;
- three instances where the user's actual system access deviated from the documented approved access;
- one instance where an account was created, but never used and should have been removed; and
- thirteen instances where Separating Employee Action forms were incomplete or insufficient separation documentation was provided to the auditor, of which five resulted in untimely removal of account access.

In response to last year's management recommendation, "Update Termination of Employee Access Policy," Health implemented the use of the HR-14 Separating Employee Action form in March 2005 and required supervisory personnel to use the form to notify the appropriate areas including the Office of Information Management when an employee leaves the Department.

The failure to follow agency policies and procedures can result in the inappropriate use of systems access thereby compromising system or data integrity. Noncompliance with existing policies and procedures regarding documentation of systems access requests and removals is a significant weakness in the Department's internal control structure as it does not allow for proper communications and accountability of system access.

We recommend that Health enforce its policies and procedures to ensure timely deletion of all system logon accounts upon termination and modify the HR-14 form to include all Health systems. Since the administration of some Health systems are decentralized, the policies and procedures should also provide accountability over these decentralized functions.

Obtain Assurance over Security of Information Technology Infrastructure

State policy makes the State Health Commissioner responsible for the security and safeguard of all of Health's databases, information, and information technology assets. Over the past two years, the Commonwealth has moved the information technology infrastructure supporting these databases and information to the Virginia Information Technologies Agency (VITA). As part of this transfer, Health also transferred many of the staff, who had the expertise to advise the Commissioner on these matters.

In addition to responsibilities under state policy, Health must also comply with the Health Insurance Portability and Accountability Act (HIPAA) and Homeland Security. HIPAA mandates actions and

protections that anyone obtaining and maintaining medical information must take to safeguard and secure the data. In addition, Homeland Security has additional layers of security for data protection.

We believe that Health cannot solely ensure that their data has the proper level of security to protect it from unauthorized changes, disclosure, or loss. Since VITA has assumed responsibility for the information technology infrastructure, the Commissioner must have VITA provide assurance that their infrastructure would provide the safeguards to protect the databases and information under not only state policy, but HIPAA and Homeland Security requirements.

The Commissioner needs to evaluate Health's capabilities for determining the level of assurance needed from VITA. Since Health retains ownership and maintains the application systems and databases that gather information, the Commissioner's internal staff has full responsibility for access controls to these systems. If these systems operate in a shared environment, the provider of the services would need to inform the Commissioner of the adequacy of those controls. This shared environment is the same as the mainframe data center operation that VITA and its predecessors offered. However, for the transmission of information to and from the database, the Commissioner must address whether Health has the expertise to assess this issue. Inherent within this question is whether Health has the resources to maintain the level of expertise capable of adapting to the changing infrastructure environment. There are two potential approaches to this issue. The first assumes Health has the expertise and the resources to understand the changing infrastructure and can, therefore, specifically address all security needs. The second approach only requires that Health explain, in detail, the security needs for each of its systems and databases along with the access controls it currently provides. VITA then must provide the Commissioner assurance that the infrastructure provides the level and depth of security necessary to meet state policy, HIPAA, and Homeland Security.

Under the second approach, VITA and the Commissioner clearly share responsibility for the security of information and databases. It is our opinion that while Health may currently have the resources to undertake the first approach, the long-term change at VITA dictates that the Commissioner use the second approach. Additionally, we believe that VITA should at least annually provide these assurances in writing, so the Commissioner and Health can fulfill their responsibilities under HIPAA and Homeland Security requirements.

AGENCY HIGHLIGHTS

The Virginia Department of Health (Health) seeks to achieve and maintain personal and community health by emphasizing health promotion, disease prevention, bio-terrorism preparedness, and environmental protection. Health administers the state's system of public health.

The State Board of Health, appointed by the Governor, provides planning and policy development to enable Health to implement a coordinated, prevention-oriented program that promotes and protects the health of the citizens. In addition, the Board serves as the advocate and representative of citizens in health issues.

Health operates through a central office and 35 health districts that operate 119 local health departments. Local health departments work with Health through agreements between the state and participating local governments. These agreements define the health services funded by the localities in the health districts. Programs offered include communicable disease control and prevention and health education. In addition to patient visits, local health departments are responsible for inspecting restaurants and drinking water and issuing permits for sewage systems, wells, and waterworks operations. Additionally, most local health departments provide a variety of non-mandated healthcare services for persons who cannot otherwise afford them.

FINANCIAL OPERATIONS

Overview

Health received over $400 million in funding during fiscal year 2005 with federal funds representing the largest funding source. The following tables summarize Health's budgeted revenues and expenses compared to actual results for fiscal year 2005.

Analysis of Budgeted and Actual Funding

	Original Budget	Adjusted Budget	Actual Funding
General Fund appropriations	$138,787,326	$136,266,143	$134,623,481
Special revenues	111,916,105	116,996,449	97,022,713
Special dedicated revenue	10,025,922	28,980,482	29,254,527
Federal grants	216,161,964	215,362,419	207,812,605
Total	$472,891,317	$497,605,493	$468,713,326

Source: Original Budget – Appropriation Act Chapter 951, Adjusted Budget – CARS 1419 D1 Report, Actual Funding – CARS 402 Report
Note: Fund classifications were adjusted to mirror those used in the Comptroller's Comprehensive Annual Financial Report

Analysis of Budget to Actual Expenses by Program

Program	Program Expenses Original Budget	Adjusted Budget	Actual Expenses
Community Health Services	$166,847,101	$168,269,398	$163,951,637
Communicable and Chronic Disease Prevention	90,047,059	89,271,276	83,319,070
Nutritional Services	80,736,276	80,803,110	76,847,162
Environmental Resources Management	33,889,310	47,719,904	23,582,782
State Health Services	35,358,780	35,447,662	30,381,897
Emergency Medical Services	21,729,240	22,249,237	18,162,831
Administrative and Support Services	14,053,794	15,559,353	14,258,063
Regulation of Public Facilities and Services	8,119,123	8,188,319	7,272,897
Medical Examiner and Anatomical Services	5,727,691	6,086,424	6,045,812
Special Health Improvement and Demonstration Services	5,226,490	7,704,062	5,379,800
Vital Records and Health Statistics	5,450,986	5,850,986	5,185,310
Health Research, Planning, and Coordination	3,989,324	4,869,245	4,333,760
Regulation of Food	1,877,858	1,909,308	1,905,080
Higher Education Student Financial Assistance	2,104,116	1,804,116	1,486,997
Regulation of Products	1,800,169	1,873,093	1,627,563
Total	$476,891,317	$497,605,493	$443,740,661

Source: Original Budget – Appropriation Act Chapter 951, Adjusted Budget and Actual – CARS 1419 D1 Report

The Safe Drinking Water Revolving fund within the Environmental Resource Management Program, which has general and federal funds under the Safe Drinking Water Act, did not spend $24 million of its budget in fiscal 2005 for two reasons. First, there is a timing difference between the awarding of grants and loans to Waterworks for construction projects and Health's reimbursement of costs. Waterworks, who receives grants and loans, must submit expenses to Health for reimbursement. As of June 30, 2005, the Safe Drinking Water Revolving fund had approximately $12 million in grants and loans outstanding pending reimbursements and another $33 million in unclosed grants and loans that were, therefore, not available to Waterworks for reimbursement.

Second, federal funding under the Safe Drinking Water Act has steadily decreased from $30 million in fiscal 1997 to $9 million in fiscal 2006. Health's management has chosen not to decrease its appropriations in order to ensure sufficient appropriations are available should Health be presented with a large amount of reimbursement requests in a given year.

Major Federal Programs

Health administers three major federal programs: the Nutritional Program for Women, Infants, and Children; the Ryan White CARE Act Title II Grant Program; and the Center for Disease Control and Prevention - Investigation and Technical Assistance. Our audit work focused on testing internal controls surrounding Health's administration of these programs, the allowability of costs, and eligibility of recipients.

Nutritional Program for Women, Infants, and Children

The Nutritional Program for Women, Infants, and Children (WIC) provides supplemental foods and nutritional education to eligible persons through local health departments. Eligible persons include pregnant, postpartum, and breast-feeding women; infants; and children up to their fifth birthday. The program serves as an adjunct to good healthcare during critical times of growth and development in order to prevent the occurrence of health problems and improve the health status of those persons.

Health administers the WIC program through local health departments who determine qualifying criteria for participation in the program. In fiscal year 2005, Health disbursed $77,335,465 in federal funds through this program, which represents approximately 34 percent of Health's total federal expenditures and a three percent increase over fiscal year 2004.

Ryan White CARE Act Title II Grant Program

The Ryan White CARE Formula Grant enables states to improve the quality, availability, and organization of healthcare and support services for low income individuals and families with Human Immunodeficiency Virus (HIV) disease. This comprehensive grant provides drugs under the Virginia AIDS Drug Assistance Program (ADAP) and other services such as essential medical and support services.

Health's Division of HIV/STD provides support to local health districts in the prevention and treatment of HIV, including its complications, through provision of education, information, and healthcare services. Health also contracts with five regional health consortiums to provide AIDS-related services, other than AIDS drugs. In addition, Health has contracted with an outside entity to maintain its ADAP database, which provides utilization and demographic data used for program reporting requirements. In fiscal year 2005, Health disbursed $24,160,451 in federal funds through this program, which represents approximately 11 percent of Health's total federal expenditures.

Center for Disease Control and Prevention - Investigation and Technical Assistance Program

The Center for Disease Control and Prevention - Investigation and Technical Assistance program assists state, local, and other health-related organizations in controlling communicable diseases, chronic diseases and disorders, and other preventable health conditions. Health conducts investigations and evaluation of all methods of controlling or preventing disease and disability; provides epidemic aid, surveillance, technical assistance, consultation, and program support; and coordinates joint national, state, and local efforts.

This program has nine federal grant awards, which funds other state agencies, localities, and other health-related organizations. In fiscal year 2005, Health disbursed $32,521,839 in federal funds through this program, which represents approximately 14 percent of Health's total federal expenditures.

Other Financial Activities

Several of the programs Health administers rely on the collection of special revenues. During fiscal 2005, three programs accounted for over 91 percent ($115 million) of the special revenues received by Health. About $51 million represents the localities' share of funding towards operating costs of local health departments. The Department of Motor Vehicles collected a "$4 for Life" vehicle registration fee and then transferred the resulting $20 million to Health to support, train, and provide grants to local rescue squads. The remaining $44 million represents monies that Health collects for vital statistics (birth and death certificates), medical, septic system permit, and well permit fees, etc.

Health spends the majority of its General Fund appropriations on payroll and related fringe benefit cost ($75 million) and direct payments ($17 million) to support local health departments. These expenses constitute 69 percent of Health's General Fund appropriation.

Information Systems

Health processes federal programs and financially material activities on a variety of information systems that Health manages and maintains. These information systems include the following:

- WICNet, a client-server application that allows for automated tracking and WIC check issuance at the 35 local health districts.

- WebVISION, a patient level enterprise system that manages client registration, encounter processing, immunizations, accounts receivable, community events, central pharmacy/inventory management, and maternity statistics.

- F&A, a financial and administrative system that initially record transactions, so that Health can upload information into the Commonwealth's Accounting and Reporting System.

- HIV1 database, a database used to interface with the Counseling and Testing Services System for the Division of HIV/STD/Pharmacy. Health staff enters screening data into this database and uploads it into the Counseling and Testing Services system.

We tested controls over the systems including user access, change management, disaster recovery and business continuity, server and database administration controls, and Health's general security environment. Our findings are in the section entitled, "Internal Control Findings and Recommendations."

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

December 14, 2005

The Honorable Mark R. Warner
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Lacey E. Putney
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have audited the financial records and operations of the **Virginia Department of Health** for the year ended June 30, 2005. We conducted our audit in accordance with Government Auditing Standards, issued by the Comptroller General of the United States.

Audit Objectives

Our audit's primary objectives were to evaluate the accuracy of Health's financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2005 and test compliance for the Statewide Single Audit. In support of these objectives, we evaluated the accuracy of recording financial transactions on the Commonwealth Accounting and Reporting System and in Health's accounting records; reviewed the adequacy of Health's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

Health's management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and control risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances:

Payments from Localities	Aid to Local Governments
Support for Local Rescue Squads	Year-end Payables
Major Federal Grants and Contracts	Payroll
Network Security	

We performed audit tests to determine whether Health's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws and regulations. Our audit procedures included inquiries of appropriate personnel; inspection of documents, payroll records, WIC check stock, internal audit reports, records, and cooperative agreements; and observation of Health's operations at the central office and selected health districts and local heath departments. We also tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that Health properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System. Health records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System and the Appropriation Act.

We noted certain matters involving internal control and its operation that require management's attention and corrective action. These matters are described in the section entitled, "Internal Control Findings and Recommendations."

The results of our tests of compliance with applicable laws and regulations disclosed no instances of noncompliance that are required to be reported under Government Auditing Standards.

Health has not taken adequate corrective action for one of two audit findings reported in the prior year, "Update Termination of Employee Access Policy," which is repeated in this report.

EXIT CONFERENCE

We discussed this report with management on January 6, 2006. Management's response is included at the end of this report.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia; is a public record; and its distribution is not limited.

AUDITOR OF PUBLIC ACCOUNTS

GS/kva

AGENCY RESPONSE

Auditor's reply to Department of Health Response dated January 9, 2006

Commonwealth of Virginia Information Technology Resource Management Policy 90-1 (COVITRM Policy 90-1) states "It is the policy of the Commonwealth that each agency head is responsible for the security of the agency's information technology resources and that all State agencies shall take appropriate steps to secure their information technology resources and sensitive information through the development of an agency information technology security program." This policy does not allow the Commissioner to assume that either the MOU or VITA will provide sufficient security.

We concur that VITA does have some responsibility in this area; however, the degree of the involvement rests with the Commissioner. As a user of VITA's services, it is incumbent on the Commissioner to determine the level of the risk he is willing to assume and based on this risk, VITA's involvement. This risk should reflect the level of expertise available to the Commissioner and that he is willing to undertake.

COMMONWEALTH of VIRGINIA

Department of Health

ROBERT B. STROUBE, M.D., M.P.H.
STATE HEALTH COMMISSIONER

P O BOX 2448
RICHMOND, VA 23218

TTY 7-1-1 OR
1-800-828-1120

January 9, 2006

The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Sir:

We are providing this letter in response to your report on audit of the financial records of the Virginia Department of Health for the fiscal year ended June 30, 2005.

We confirm that we have reviewed the findings, conclusions and recommendations and have prepared a response and corrective action plan which is attached.

Sincerely,

Robert B. Stroube, M.D., M.P.H.
State Health Commissioner

CC: Department of Accounts

Virginia Department of Health
Management response and corrective action plan for findings, and recommendations in the APA report for the year ended June 30, 2005.

APA Finding # 1
Improve Controls for Removing Systems Access in a Timely Manner and Document Access Authorizations

The Virginia Department of Health (Health) did not remove in a timely manner or properly authorize staff access to critical systems. Health has policies and procedures addressing both deletion and authorization of access, but failed to follow them. In our testing, we found:

- **seven instances where the auditor was not provided with any systems access removal or authorization documentation;**
- **one instance where the system access request form lacked proper authorization signatures;**
- **three instances where the user's actual system access deviated from the documented approved access;**
- **one instance where an account was created, but never used and should have been removed;**
- **thirteen instances where Separating Employee Action forms were incomplete or insufficient separation documentation was provided to the auditor, of which five resulted in untimely removal of account access; and**

In response to last year's management recommendation, "Update Termination of Employee Access Policy," Health implemented the use of the HR-14 Separating Employee Action form in March 2005 and required supervisory personnel to use the form to notify the appropriate areas including the Office of Information Management when an employee leaves the Department.

The failure to follow agency policies and procedures can result in the inappropriate use of systems access thereby compromising system or data integrity. Noncompliance with existing policies and procedures regarding documentation of systems access requests and removals is a significant weakness in the Department's internal control structure as it does not allow for proper communications and accountability of system access.

We recommend that Health enforce its policies and procedures to ensure timely deletion of all system logon accounts upon termination and modify the HR-14 form to include all Health systems. Since the administration of some Health systems are decentralized, the policies and procedures should also provide accountability over these decentralized functions.

Virginia Department of Health Management Response
P. 2

Agency Response to Finding #1

We agree that this prior year's point has not been completely resolved, however we think the security risk was small to begin with and has been further reduced.
VDH implemented these controls proposed last year in response to a similar finding. Those prudent and cost effective controls have apparently not resulted in an error rate acceptable to APA so VDH will implement additional, more expensive, and more disruptive controls. The timing of audit closings and openings is such that there is very little time to create and implement controls between audit years. Given the nature of the proposed additional controls, VDH is concerned that, what should be continuing work on the original 2004 finding, will be represented as not only the existing two management points, but will inevitably be expanded to three points as contemporaneous events will be audited in the next cycle.

As we stated last year, access to applications is impossible if network access, either directly or through dial-up of VPN access has been terminated. In other words, though we aspire to timely termination of all applications accounts, since separated users cannot access the applications, the security risk is minimal. Those network access points already have the main control proposed, which is timing out of access with disuse.
We also note that the number of accounts that were not terminated in a timely fashion was substantially reduced, with WebVISION decreased from 6 to 2 and WICNet from 15 to 1.

Nevertheless, we are imposing strict, and expensive, measures to address this issue. Existing applications will have to be modified to lock accounts after a 45 day period of inactivity (time periods may vary based on application use cycles). Existing applications will also have to be modified to generate a work unit specific report listing users and the work unit will have to certify that those users have the proper authority and are still authorized users. The second phase will be to create the report at the role level with certification at that level.

New applications must use Lightweight Directory Access Protocol, LDAP, an Internet protocol that email and other programs use to look up information from a server, as part of user authentication, so removal of a user from LDAP will terminate access to those applications using LDAP authentication.

VDH continues to search for a commercial off-the-shelf application that will allow management of the access authorization and termination process – a search that has been unsuccessful so far. This would address the apparent deficiencies in the HR-14 forms noted in this point. Since those forms are currently generated and processed by individual work units, multiple copies exist and they are not collected centrally. Consequently, the copies provided for audit do not reflect the work in the various work units as they process an individual user. VDH is also reviewing the HR-14 process to determine areas in the manual process that can be enhanced.

Person responsible for Corrective Actions: Jim Burns, M.D., VDH Deputy Commissioner, and CIO

Virginia Department of Health Management Response
P. 3

APA Finding # 2
Obtain Assurance over Security of Information Technology Infrastructure

State policy makes the State Health Commissioner responsible for the security and safeguard of all of Health's databases, information, and information technology assets. Over the past two years, the Commonwealth has moved the information technology infrastructure supporting these databases and information to the Virginia Information Technologies Agency (VITA). As part of this transfer, Health also transferred many of the staff, who had the expertise to advise the Commissioner on these matters.

In addition to responsibilities under state policy, Health must also comply with the Health Information Portability and Protection Act (HIPPA) and Homeland Security. HIPPA mandates actions and protections that anyone obtaining and maintaining medical information must take to safeguard and secure the data. In addition, Homeland Security has additional layers of security for data protection.

We believe that Health cannot solely ensure that their data has the proper level of security to protect it from unauthorized changes, disclosure, or loss. Since VITA has assumed responsibility for the information technology infrastructure, the Commissioner must have VITA provide assurance that their infrastructure would provide the safeguards to protect the databases and information under not only state policy, but HIPPA and Homeland Security requirements.

The Commissioner needs to evaluate Health's capabilities for determining the level of assurance needed from VITA. Since Health retains ownership and maintains the application systems and databases that gather information, the Commissioner's internal staff has full responsibility for access controls to these systems. If these systems operate in a shared environment, the provider of the services would need to inform the Commissioner of the adequacy of those controls. This shared environment is the same as the mainframe data center operation that VITA and its predecessors offered.

However, for the transmission of information to and from the database, the Commissioner must address whether Health has the expertise to assess this issue. Inherent within this question is whether Health has the resources to maintain the level of expertise capable of adapting to the changing infrastructure environment. There are two potential approaches to this issue. The first assumes Health has the expertise and the resources to understand the changing infrastructure and can, therefore, specifically address all security needs. The second approach only requires that Health explain, in detail, the security needs for each of its systems and databases along with the access controls it currently provides. VITA then must provide the Commissioner assurance that the infrastructure provides the level and depth of security necessary to meet state policy, HIPPA, and Homeland Security.

Under the second approach, VITA and the Commissioner clearly share responsibility for the security of information and databases. It is our opinion that while Health may currently have the resources to undertake the first approach, the long-term change at VITA dictates that the Commissioner use the second approach. Additionally, we believe that VITA should at least annually provide these assurances in writing, so the Commissioner and Health can fulfill their responsibilities under HIPPA and Homeland Security requirements.

Virginia Department of Health Management Response
P. 4

Agency Response to Finding #2
We disagree with this point.
This issue is controlled by VITA. VITA initiated an MOU process with expectations that a draft would be signed by the end of December, 2005. This was the first opportunity for agencies to formally communicate service standards to VITA. We have signed the MOU and included a statement about VDH's security expectations. Additional attempts will be made to elicit security certification from VITA.

Since its inception, VITA's focus has been on the transition process and administrative planning while the actual IT work has continued to be performed by employees who formerly worked for VDH. These employees continue doing the same work, on the same equipment, with the same standards to this day. VITA is just starting the process for agencies to communicate standards to them so they can start assuming full responsibility for the IT infrastructure. That change will not be completed for at least another year.

Person responsible for Corrective Actions: Jim Burns, M.D., VDH Deputy Commissioner, and CIO

VIRGINIA DEPARTMENT OF HEALTH

Robert B. Stroube, MD, MPH
State Health Commissioner

BOARD OF HEALTH
As of June 30, 2005

Jack O. Lanier, Dr. P.H., MHA, FACHE
Chair

Julie L. Beales, MD
W. Scott Burnette
Jean M. Donovan, PhD
James H. Edmondson, Jr.
Katherine Elliot
Barry I. Griffin, DDS
Richardson Grinnan, MD
Frederick J. Hannett
Bennie Marshall, RN, EdD
Bhushan Pandya, MD
Craig A. Reed, DVM
Ed D. Spearbeck