STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

OF THE

NORTH CAROLINA COMMUNITY COLLEGE SYSTEM

RALEIGH, NORTH CAROLINA

JUNE 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

OF THE

NORTH CAROLINA COMMUNITY COLLEGE SYSTEMS

RALEIGH, NORTH CAROLINA

JUNE 2004

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of the North Carolina Community College System
Mr. Martin Lancaster, President

Ladies and Gentlemen:

We have completed our information systems (IS) audit of the North Carolina Community College System (NCCCS), which is comprised of the North Carolina Community College Systems Office (Systems Office), 58 Community Colleges, and the NC Center for Applied Textile Technology (Center). The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

This report represents a summary of the general results of our audits. A separate audit report containing the conditions found and recommended corrective action was provided to each individual entity at the conclusion of our fieldwork.

The primary objective of this audit was to evaluate IS general controls at the North Carolina Community College Systems Office, 58 Community Colleges, and the Center. The scope of our IS general controls audit included reviewing for general security policies and evaluating the following: access to student and financial information, security of the networks and critical operating system, Systems Development Life Cycle (SDLC) methodology used to implement critical applications, maintenance of the operating system, physical security over the computer center, and disaster recovery planning. We reviewed controls in the following six areas: general security, access controls, system development, systems software, physical security, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

In early April 2003, the Office of the State Auditor began the review of all the entities within NCCCS. We visited each entity to gather audit information, performed onsite test work, and attempted to penetrate the security of the critical operating system and the networks. These audits were conducted during the period from April 4, 2003 through April 30, 2004. The audits were conducted under the authority granted by *North Carolina General Statute* 147-64.6(c)(18) which states:

> The Auditor shall, after consultation and in coordination with the State Chief Information Officer, assess, confirm, and report on the security practices of information technology systems. If an agency has adopted standards pursuant to

General Statutes 147-33.82(d)(1) or (2), the audit shall be in accordance with those standards. The Auditor's assessment of information security practices shall include an assessment of network vulnerability. The Auditor may conduct network penetration or any similar procedure, as the Auditor may deem necessary. The Auditor may investigate reported information technology security breaches, cyber attacks, and cyber fraud in State Government. The Auditor shall issue public reports on the general results of the reviews undertaken pursuant to this subdivision, but may provide agencies with detailed reports of the security issues identified pursuant to this subdivision which shall not be disclosed as provided in *General Statute* 132-6.1(c).

This report contains an executive summary that highlights the areas where the North Carolina Community College System has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff of all the entities comprising the North Carolina Community College System for the courtesy, cooperation, and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit of the North Carolina Community College System (NCCCS), which is comprised of the North Carolina Community College Systems Office (Systems Office), 58 Community Colleges, and the NC Center for Applied Textile Technology (Center) from April 4, 2003 through April 30, 2004. The primary objective of this audit was to evaluate the IS general controls in place during that period. We did not review the applications on the operating systems under review. Our audit focused on the following six areas of general controls: general security, access controls, systems development, systems software, physical security, and disaster recovery. We also performed scans for known vulnerabilities to determine if unauthorized access to sensitive student and financial information could be gained, and if so, we determined if this information could be read, modified, or even destroyed. Our audit identified general controls within NCCCS that were well defined and effective, as well as, controls that posed extreme security risks. We used a risk approach to define the level of risk associated with a general controls area under review. We classified each area's relative risk level using the following definitions.

- **High Risk**: Defined as a weakness that could cause grave consequences if not addressed and remedied immediately. This type of weakness is evident within the most sensitive portions of the critical operating systems and network. The security posture of the entity offers little protection from various security threats. This weakness could cause the data residing on the critical operating system to be modified or even destroyed by an unauthorized user or circumstance.

- **Medium Risk**: Defined as a weakness that should be addressed within the near future. This weakness could cause the data residing on the critical operating system to be read by an unauthorized user, however no modification or destruction of data can occur if not remedied.

- **Low Risk**: Defined as a weakness that should be fixed; however, it is unlikely that this weakness alone would allow the critical operating system or networks to be exploited.

Based on the tests performed and severity of the control weaknesses identified, we found that the overall combined risk level for NCCCS is **HIGH.** We found that the general controls are not effective for protecting the operating systems for the majority of the entities within NCCCS. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. We found that the Systems Office, 57 of 58 Community Colleges, and the Center had not adopted formal information technology (IT) standards, policies, and procedures for many critical IT areas. However, we did find one community college that had adopted its own standards for information technology. This College's polices and procedures were considered adequate to promote good information technology security. Although almost all NCCCS entities failed to meet the standard controls

for general security, we consider the risk level for this area to be **LOW.** However**,** the absence of good general security policies and management contribute to weaknesses in other control areas.

Access Control involves the implementation of controls to restrict access to computer resources to only those users who have an authorized need to use or know critical information. The access control environment consists of access control software, operating system and network configurations, and the implementation of information security policies and procedures. We reviewed the access controls to the networks and sensitive student and financial information residing on the critical operating systems for the Systems Office, 58 Community Colleges, and the Center. We found several access control weaknesses for all entities under review. Due to the sensitive nature of the conditions found, we have conveyed the details of these findings to management in a separate letter pursuant to the provision of *North Carolina General Statute* 147-64.6(c)(18). We consider the risk level for this area is **HIGH** because access controls are not working and are not effective for the majority of the entities within NCCCS.

Systems development includes the creation of new application systems or significant changes to existing systems. Good system development controls suggest the use of a formal Systems Development Life Cycle (SDLC) Methodology to implement new application systems or modify existing systems. The Systems Office has the primary responsibility to select financial and student application systems and modify existing systems. The Systems Office is the only entity within NCCCS that is responsible for this area. The decisions made by the Systems Office in this area can have a significant impact on how well the other entities within NCCCS operate their critical systems. We found that the Systems Office had adopted a SDLC that included formal policies and procedures to implement the new critical application into the production environment of all the entities within NCCCS. However, the Systems Office did not include in their SDLC any security requirements or security specifications for the critical operating system, which host the critical applications. We evaluated the risk level for this area as **HIGH** because failing to specify security requirements for the critical operating system causes all of the entities within NCCCS to operate the new critical applications on operating systems that may not be secure.

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center. We found a significant weakness in systems software maintenance controls. We found that procedures used to notify the entities within NCCCS of enhancements or changes to the critical operating system were ineffective. However, we found three colleges that had adopted their own procedures for systems software maintenance and their procedures were effective. We consider the risk level for this area is **HIGH** because system software controls were not maintained at current release levels for the majority of the entities within NCCCS.

Physical security primarily involves the inspection of a computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. We found 10 community colleges' computer centers are not secure from foreseeable and preventable security and environmental threats. Improvements in physical security should be made for the ten colleges identified with physical control weaknesses, however the risk level for this area is **LOW** because physical security controls are working and are effective for the majority of the entities within NCCCS.

Disaster Recovery involves the creation of a plan to enable the recovery from an extended business interruption due to the destruction of the computer center or other assets. A complete disaster recovery plan that is tested periodically is necessary to ensure prompt resumption of computer systems. Fifteen community colleges did not have a formal written disaster recovery plan. Thirty-seven community colleges, the Systems Office, and the Center had disaster recovery plans, however, the plans were inadequate. The remaining six colleges' disaster recovery plans were adequate. In addition, the community colleges are relying on the Systems Office as an alternate disaster recovery site; however, the Systems Office only has enough space on their back-up server to handle a few community colleges at a time. Furthermore, the server has not been tested for remote processing capabilities. We consider the risk level for this area is **HIGH** because disaster recovery controls may not be adequate or effective for the majority of the entities within NCCCS.

This report represents a summary of the general results of our audits. A separate audit report containing the conditions found and recommended corrective actions was provided to each individual entity at the conclusion of our fieldwork. A copy of a specific entity's report can be obtained from the Office of the State Auditor website *http://www.ncauditor.net*.

Auditor's Note: The findings in this report address the operating systems on which applications are installed and the surrounding information technology environment. The findings in this report are not associated with nor can these findings be resolved with the implementation of the Colleague student and financial application. General controls surrounding the operating system have a direct impact on the applications it hosts, therefore, NCCCS needs to ensure that they develop corrective actions apart from the installation of the new application to resolve these findings.

[This Page Left Blank Intentionally]

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the *North Carolina General Statutes* Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. This IS audit was designed to ascertain the effectiveness of general controls at the North Carolina Community College Systems Office, the 58 community colleges and the NC Center for Applied Textile Technology.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, systems development, systems software, physical security, and disaster recovery which directly affect the entities within the NCCCS computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, used questionnaires to interview key administrators and other personnel, developed a program to generate information from the critical operating systems to examine system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer-generated reports, and used security evaluation software in our audit of controls. We performed the following tasks.

PHASE 1 – Information Gathering

In Phase 1, we sent questionnaires to all the entities within the NCCCS. We asked them to provide specific information regarding their critical operating systems, their security policies and procedures, their access and network infrastructure, and their disaster recovery plans. This information was reviewed to determine whether security policies and procedures exist and whether those polices and procedures covered standard areas. We determined whether the maintenance of the critical applications and operating system was current to prevent unauthorized access by individuals using known vulnerabilities. We reviewed the disaster recovery plans to ensure that recovery of critical systems was possible in the event of a disaster.

PHASE 2 – Onsite Review

We then visited each entity to perform tests that could not be performed offsite to confirm suspected weaknesses. We viewed the computer operations of all the entities within the NCCCS. During this examination, we identified conditions that could allow physical security breaches into the computer centers and evaluated environmental concerns of the computing center.

PHASE 3 – Review of Audit Scripts
In Phase 3, we internally developed a program to review the server configurations of the operating systems and the configuration of critical and sensitive files. We ran this program on each critical system of the community college to determine if the server and files were configured to restrict unauthorized access to critical student and financial information.

PHASE 4 – Vulnerability assessment
In Phase 4, we tested for known vulnerabilities, specific to the critical operating system under review, and also tested to see if unauthorized access could be obtained into the critical operating systems. We accomplished this task by using services that come standard with all computers. The overall goal of this phase was to determine if vulnerabilities exist that would allow user level access to the critical operating systems via the internet or internally.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association. [1]

1 In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to *North Carolina General Statute* 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

BACKGROUND INFORMATION

The North Carolina Community College System (NCCCS) is comprised of the North Carolina Community College Systems Office, which is located in Raleigh, North Carolina, 58 community colleges located across North Carolina, and the NC Center for Applied Textile Technology. The mission of the North Carolina Community College System is to open the door to high-quality, accessible educational opportunities that minimize barriers to post-secondary education, maximize student success, and improve the lives and well being of individuals within North Carolina.

The entities within NCCCS share responsibility for information technology. Each entity has a division that is responsible for information technology for their respective entity. The mission of the information technology divisions is to ensure that information technology is utilized and delivered to the students, faculty, and staff to aid them in accomplishing the overall mission of the North Carolina Community College System.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where the North Carolina Community College Systems Office (Systems Office), the 58 community colleges, and the NC Center for Applied Textile Technology (Center) has performed satisfactorily and where recommendations have been made for improvement. A number of conditions were found within the entities that could be strengthened to improve security and general controls in the areas under review. Each area under review was classified according to its relative risk using the following definitions.

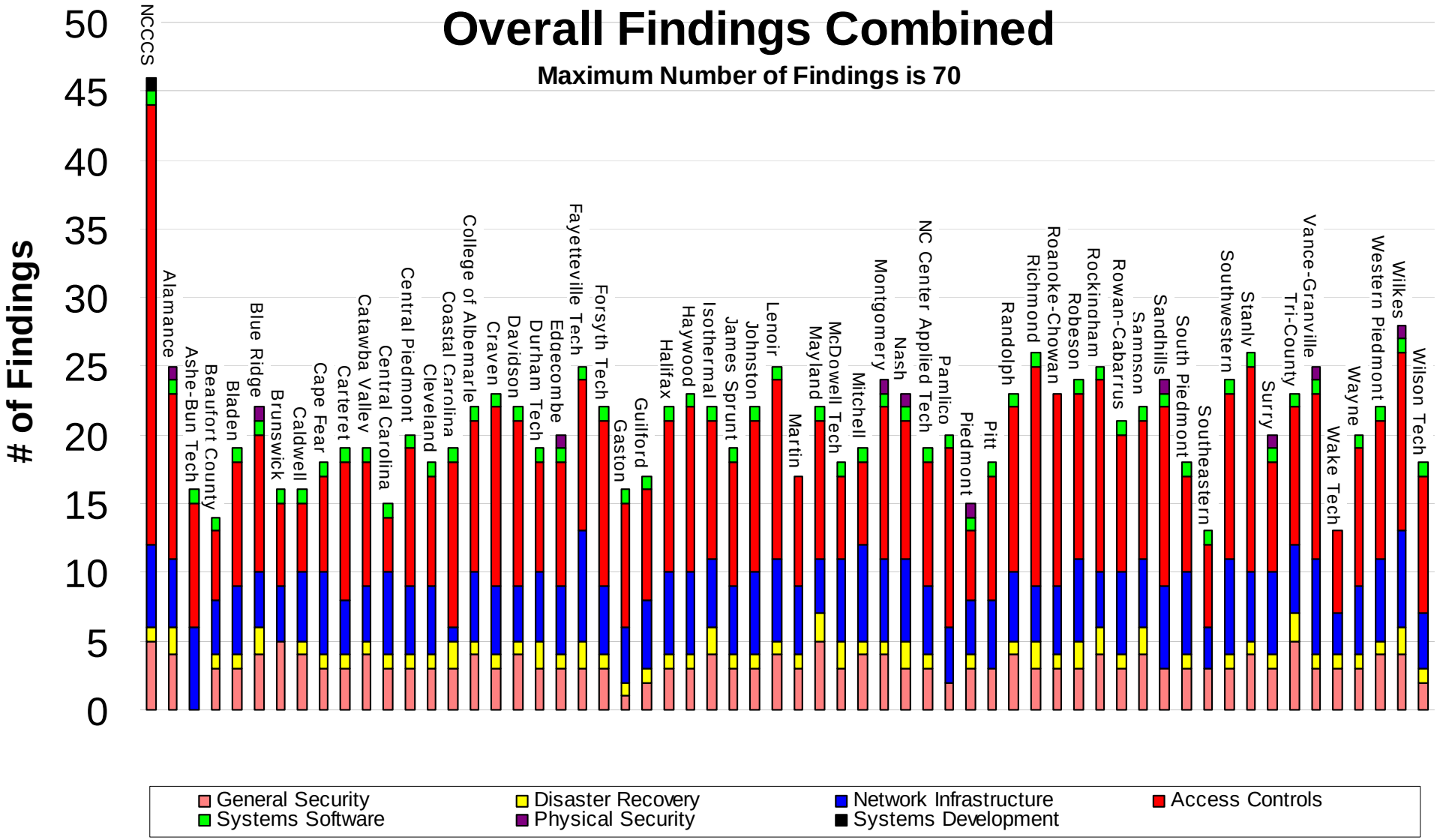
- **High Risk**: Defined as a weakness that could cause grave consequences if not addressed and remedied immediately. This type of weakness is evident within the most sensitive portions of the critical operating systems and network. The security posture of the entity offers little protection from various security threats. This weakness could cause the data residing on the critical operating system to be modified or even destroyed by an unauthorized user or circumstance.

- **Medium Risk**: Defined as a weakness that should be addressed within the near future. This weakness could cause the data residing on the critical operating system to be read by an unauthorized user, however no modification or destruction of data can occur if not remedied.

- **Low Risk**: Defined as a weakness that should be fixed; however, it is unlikely that this weakness alone would allow the critical operating system or networks to be exploited.

OVERALL RISK- HIGH RISK

The overall risk level of the North Carolina Community College System was **HIGH** based on the control weaknesses identified at the Systems Office, the 58 community colleges and the Center, and the level of risk classified for each area under review. The following is a graphical classification of risk and a depiction of the weaknesses found for each area under review. Maximum combined number of findings is 70. The majority of colleges received at least 15 or more findings with the majority of those findings occurring in a high-risk area.

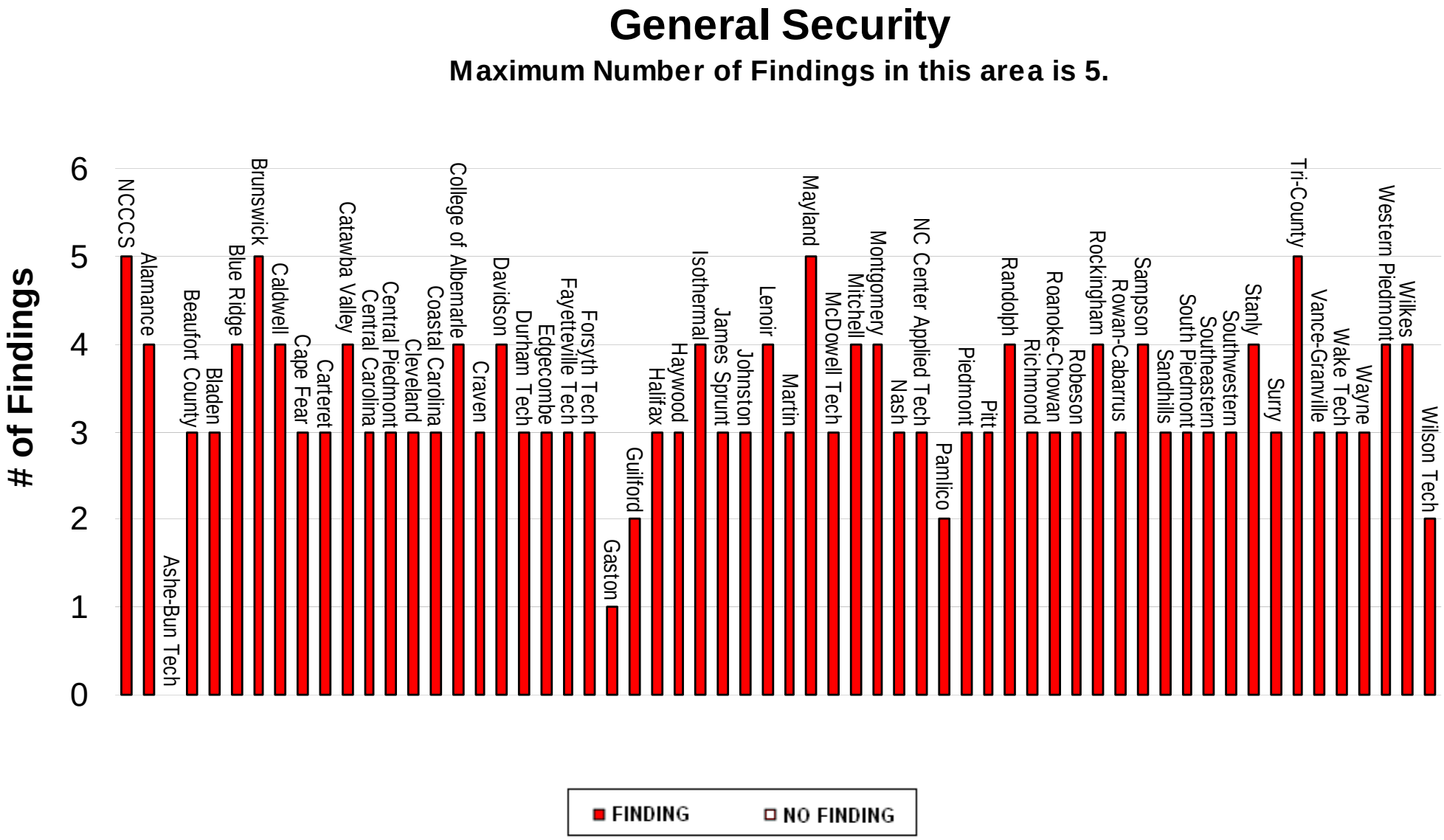

Overall Findings Combined
Maximum Number of Findings is 70
# of Findings
50
45
40
35
30
25
20
15
10
5
0
NCCCS
Alamance
Ashe-Bun Tech
Beaufort County
Bladen
Blue Ridge
Brunswick
Caldwell
Cape Fear
Carteret
Catawba Valley
Central Carolina
Central Piedmont
Cleveland
Coastal Carolina
College of Albemarle
Craven
Davidson
Durham Tech
Edgecombe
Fayetteville Tech
Forsyth Tech
Gaston
Guilford
Halifax
Haywood
Isothermal
James Sprunt
Johnston
Lenoir
Martin
Mayland
McDowell Tech
Mitchell
Montgomery
Nash
NC Center Applied Tech
Pamlico
Piedmont
Pitt
Randolph
Richmond
Roanoke-Chowan
Robeson
Rockingham
Rowan-Cabarrus
Samspon
Sandhills
South Piedmont
Southeastern
Southwestern
Stanly
Surry
Tri-County
Vance-Granville
Wake Tech
Wayne
Western Piedmont
Wilkes
Wilson Tech
General Security
Disaster Recovery
Network Infrastructure
Access Controls
Systems Software
Physical Security
Systems Development

GENERAL SECURITY ISSUES- LOW RISK

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. The Systems Office, 57 community colleges, and the Center have not adopted formal information technology (IT) standards to help them address all critical areas of their IT security environment. One College did have acceptable policies and procedures. Two community colleges did not have any IT polices, while 55 colleges and the Center had IT policies, however, the policies lacked one or more of the following critical policies and procedures.

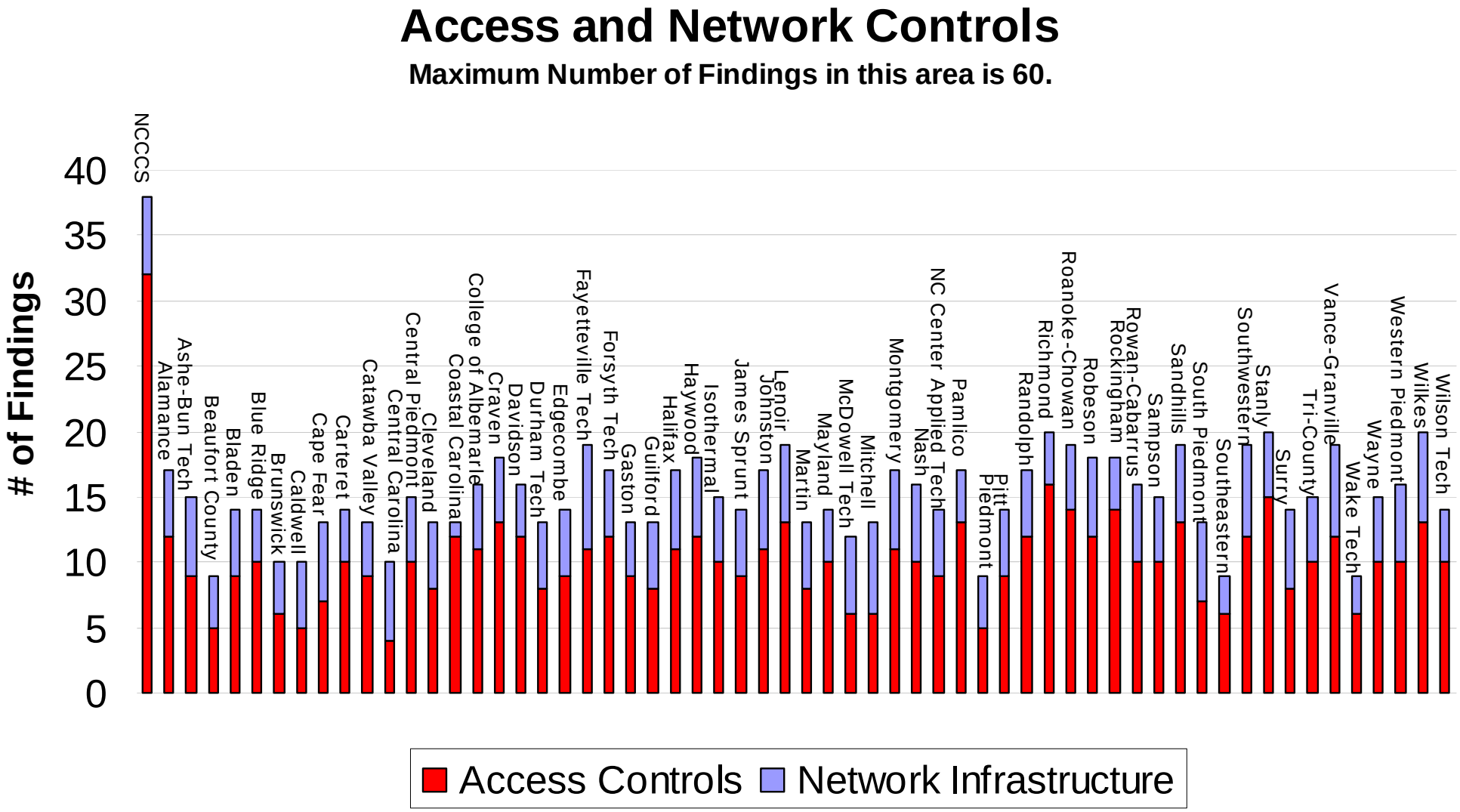
- Organizational-wide security policies;
- User security policies;
- Group assignment and re-assignment polices;
- New accounts and termination policies;
- Monitoring of the critical operating systems and servers;
- How to respond to security threats and incidents;
- How users should securely use the networks;
- Baseline configuration for securing the critical operating system; and
- Risk assessment.

Although, the majority of the entities within NCCCS received a finding in this area, we believe the overall risk level for this area is **LOW** because the nature of the weaknesses found in this area alone would not allow the critical operating system or networks to be exploited


General Security
Maximum Number of Findings in this area is 5.
# of Findings
0
1
2
3
4
5
6
NCCCS
Alamance
Ashe-Bun Tech
Beaufort County
Bladen
Blue Ridge
Brunswick
Caldwell
Cape Fear
Carteret
Catawba Valley
Central Carolina
Central Piedmont
Cleveland
Coastal Carolina
College of Albemarle
Craven
Davidson
Durham Tech
Edgecombe
Fayetteville Tech
Forsyth Tech
Gaston
Guilford
Halifax
Haywood
Isothermal
James Sprunt
Johnston
Lenoir
Martin
Mayland
McDowell Tech
Mitchell
Montgomery
Nash
NC Center Applied Tech
Pamlico
Piedmont
Pitt
Randolph
Richmond
Robeson
Roanoke-Chowan
Rockingham
Rowan-Cabarrus
Sampson
Sandhills
South Piedmont
Southeastern
Southwestern
Stanly
Surry
Tri-County
Vance-Granville
Wake Tech
Wayne
Western Piedmont
Wilkes
Wilson Tech
FINDING
NO FINDING

ACCESS CONTROLS- HIGH RISK

Access Control involves the implementation of controls to restrict access to computer resources to only those users who have an authorized need to use or know critical information. The access control environment consists of access control software and operating system and network configurations, and the implementation of information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. We reviewed the access controls for the NCCCS critical operating systems. We found several significant weaknesses in access controls. At the time of our testing, the majority of the entities within NCCCS had significant weaknesses in this area. Therefore, we believe the overall risk level for this area is **HIGH**. Subsequently, these security enhancements have been acted upon.

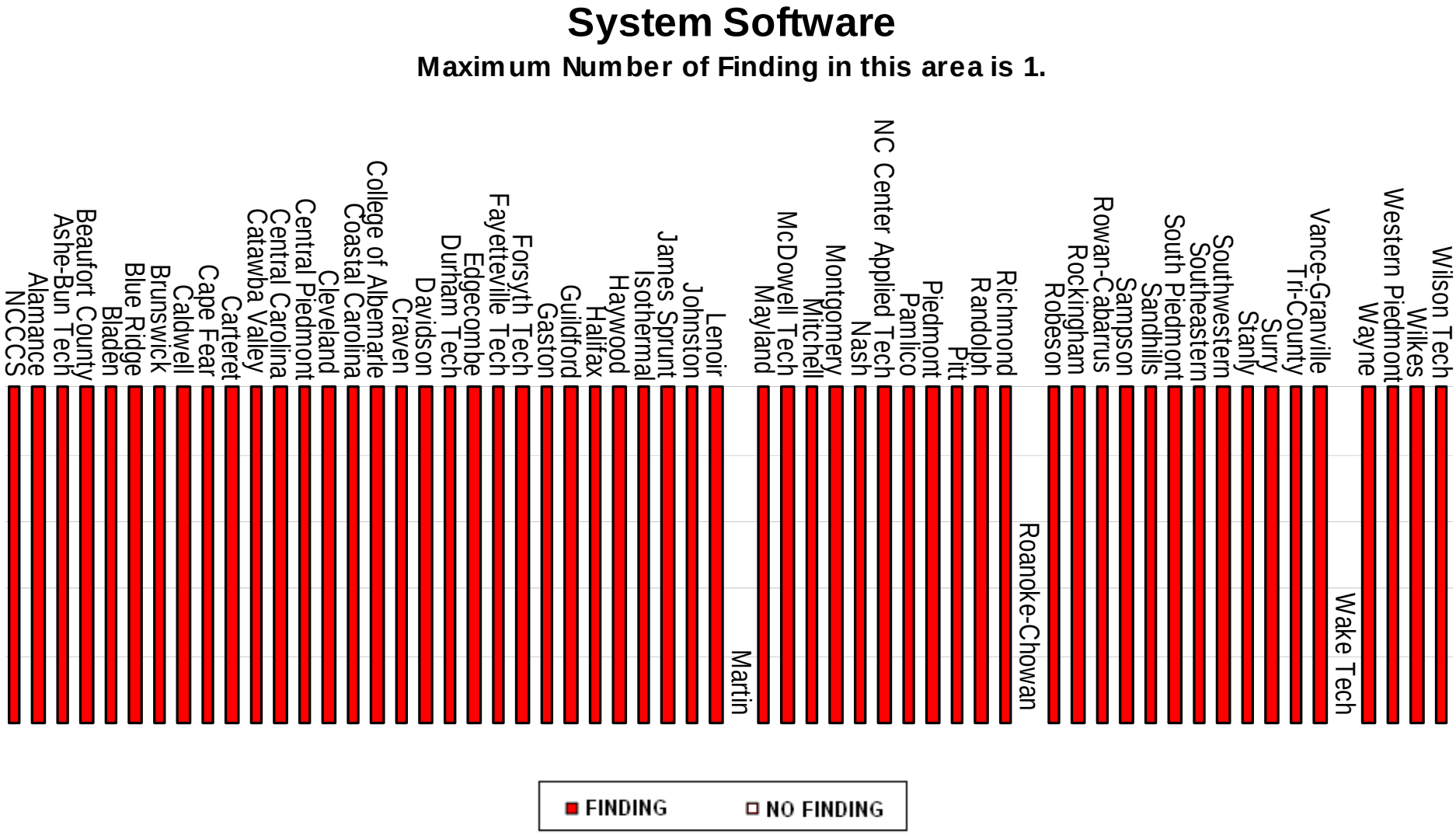

Access and Network Controls
Maximum Number of Findings in this area is 60.
# of Findings
0
5
10
15
20
25
30
35
40
NCCCS
Alamance
Ashe-Bun Tech
Beaufort County
Bladen
Blue Ridge
Brunswick
Caldwell
Cape Fear
Carteret
Catawba Valley
Central Carolina
Central Piedmont
Cleveland
Coastal Carolina
College of Albemarle
Craven
Davidson
Durham Tech
Edgecombe
Fayetteville Tech
Forsyth Tech
Gaston
Guilford
Halifax
Haywood
Isothermal
James Sprunt
Lenoir
Johnston
Martin
Mayland
McDowell Tech
Mitchell
Montgomery
Nash
NC Center Applied Tech
Pamlico
Pitt
Piedmont
Randolph
Richmond
Roanoke-Chowan
Robeson
Rockingham
Rowan-Cabarrus
Sampson
Sandhills
South Piedmont
Southeastern
Southwestern
Stanly
Surry
Tri-County
Vance-Granville
Wake Tech
Wayne
Western Piedmont
Wilkes
Wilson Tech
Access Controls
Network Infrastructure

SYSTEMS DEVELOPMENT- HIGH RISK

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include comprehensive documentation so that the users, operators, and programmers each have the information they need to do their jobs. The Systems Office has been delegated the authority of selecting new application systems or modify existing systems, which process the financial and student data for all of the entities within NCCCS. The Systems Office is the only entity within NCCCS that is responsible for this area. We reviewed the phases of the Systems Development Life Cycle for Systems Office and found that no security requirements were defined for the critical operating system under review. This weakness has a significant impact on how well the other entities within NCCCS operate their critical systems. Therefore, the overall risk level for this area is **HIGH**.

SYSTEMS SOFTWARE- HIGH RISK

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. At the time of our testing, the majority of the entities within NCCCS had significant weaknesses in this area. However, we found three colleges who had adopted their own procedures for systems software maintenance and their procedures were effective. Therefore, we believe the overall risk level for this area is **HIGH**.

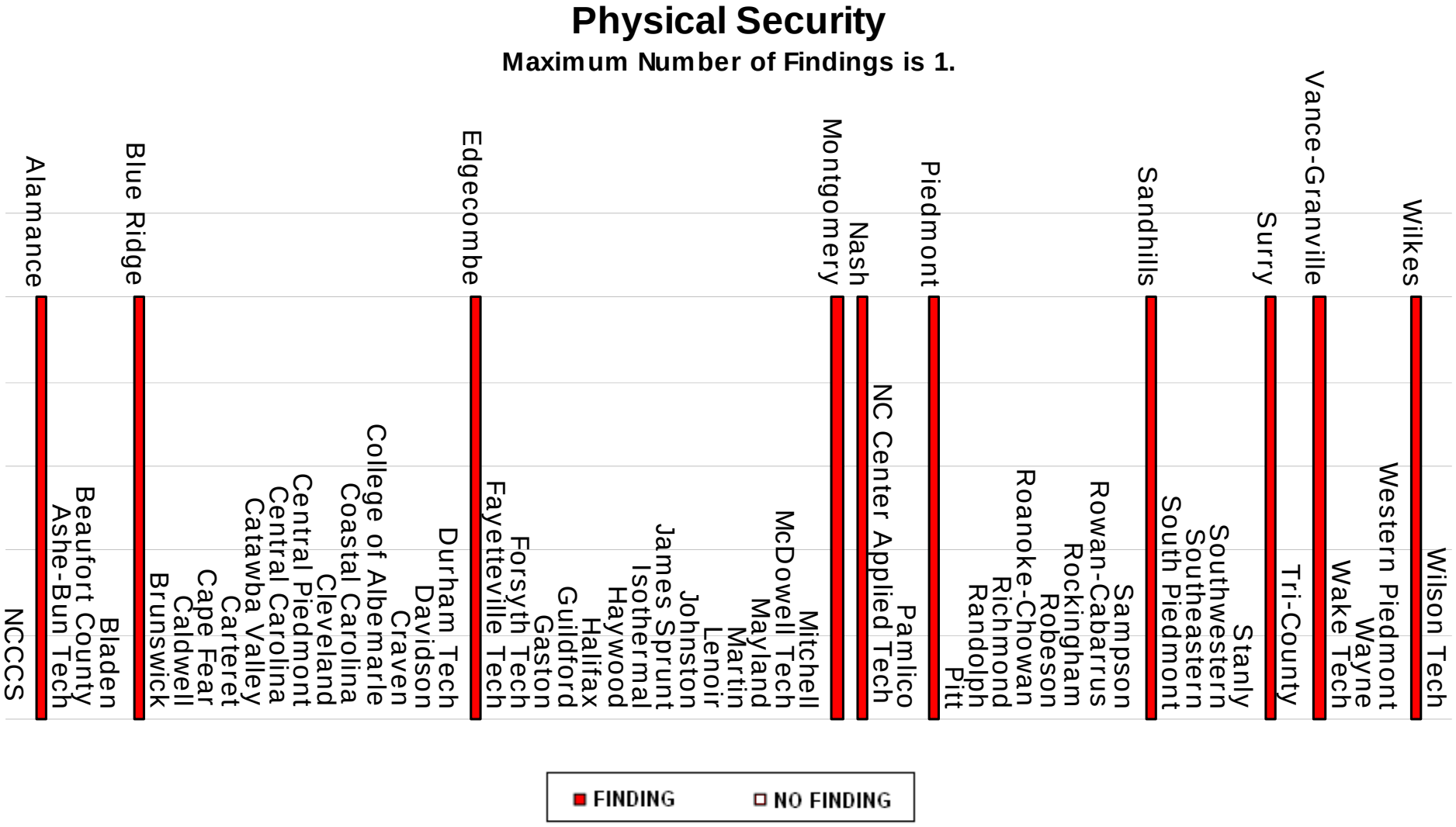

System Software
Maximum Number of Finding in this area is 1.
Wilson Tech
Wilkes
Western Piedmont
Wayne
Wake Tech
Vance-Granville
Tri-County
Surry
Stanly
Southwestern
Southeastern
South Piedmont
Sandhills
Sampson
Rowan-Cabarrus
Rockingham
Robeson
Roanoke-Chowan
Richmond
Randolph
Pitt
Piedmont
Pamlico
NC Center Applied Tech
Nash
Montgomery
Mitchell
McDowell Tech
Mayland
Martin
Lenoir
Johnston
James Sprunt
Isothermal
Haywood
Halifax
Guildford
Gaston
Forsyth Tech
Fayetteville Tech
Edgecombe
Durham Tech
Davidson
Craven
College of Albemarle
Coastal Carolina
Cleveland
Central Piedmont
Central Carolina
Catawba Valley
Carteret
Cape Fear
Caldwell
Brunswick
Blue Ridge
Bladen
Beaufort County
Ashe-Bun Tech
Alamance
NCCCS
FINDING
NO FINDING

PHYSICAL SECURITY- LOW RISK

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. Ten community colleges did not have computer centers that were secure from foreseeable and preventable security and environmental threats. At the time of our testing, the ten community colleges had a **HIGH** risk level in this area. Physical Security Controls are ineffective for only those community colleges. Of these 10 community colleges, we found the following types of physical security weaknesses.

- The offsite storage area and the computer area are not restricted to authorized personnel. As a result, the physical security over the community college's back-up tapes and computing resources is weakened and could allow unauthorized tampering of the data stored on the back-up tapes and unauthorized access to computer hardware.
- The System Administrator leaves the door unlocked to the computer room. Because the critical operating system, which host the financial and student information, resides in this computer room, unauthorized personnel could directly access the main console and modify, delete, and corrupt data, or interrupt the community college's computer processing capabilities.
- The computer room is not equipped with smoke detectors, automated fire suppression system, or hand-pulled fire alarms. Therefore, the community college is not protected from an environmental hazard, such as, fire.
- The computer room has water leaks in the ceiling that can drip onto servers below, thus the critical server is not protected from water damage. Water is an environmental hazard to computer servers and can cause a computer to malfunction. Since the critical server resides in the computer room, this server is subject to water damage, which would cause the community college to lose computer-processing capabilities.
- The computer room is not protected from electrical hazards. Therefore, the community college is susceptible to electrical fluctuations or power outages. Electrical fluctuations and power outages can cause data on a computer server to become non-useable. Electrical fluctuations and power outages are another environmental hazard that could cause the community college to lose computer-processing capabilities.

The Systems Office, the other 48 community colleges, and the Center's computer centers appear secure from foreseeable and preventable security and environmental threats. We found no significant weaknesses in physical security for these entities. Therefore, the overall risk level for this area is **LOW**.

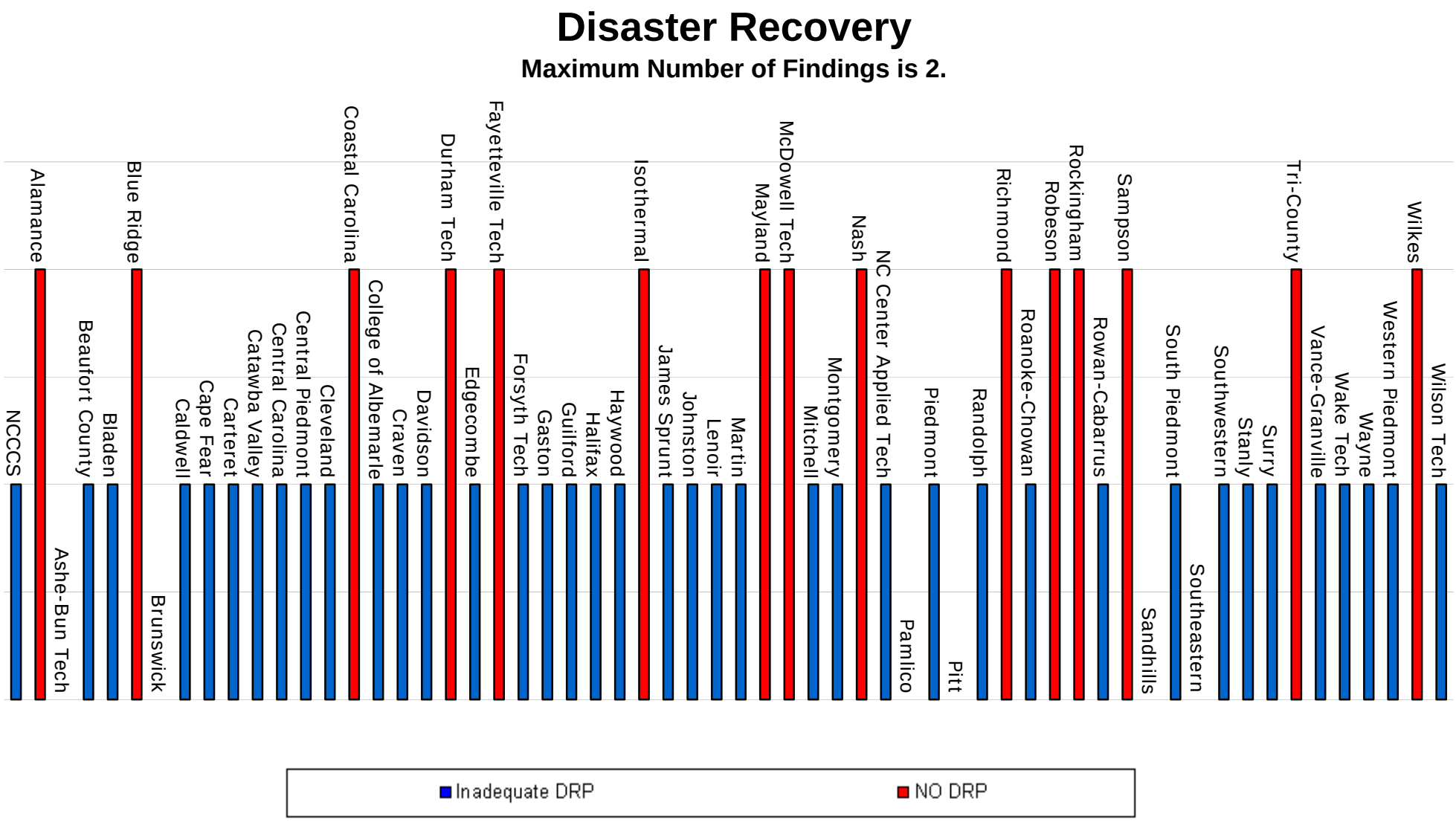

Physical Security
Maximum Number of Findings is 1.
Wilkes
Western Piedmont
Wayne
Wake Tech
Vance-Granville
Tri-County
Surry
Stanly
Southwestern
Southeastern
South Piedmont
Sandhills
Sampson
Rowan-Cabarrus
Rockingham
Robeson
Roanoke-Chowan
Richmond
Randolph
Pitt
Piedmont
Pamlico
NC Center Applied Tech
Nash
Mitchell
McDowell Tech
Mayland
Martin
Lenoir
Johnston
James Sprunt
Isothermal
Haywood
Halifax
Guildford
Gaston
Montgomery
Forsyth Tech
Fayetteville Tech
Edgecombe
Durham Tech
Davidson
Craven
College of Albemarle
Coastal Carolina
Cleveland
Central Piedmont
Central Carolina
Catawba Valley
Carteret
Cape Fear
Caldwell
Brunswick
Blue Ridge
Bladen
Beaufort County
Ashe-Bun Tech
Alamance
NCCCS
FINDING
NO FINDING

DISASTER RECOVERY- HIGH RISK

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many college services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center. Our audit identified fifteen community colleges that did not have disaster recovery plans. The Systems Office, thirty-seven community colleges, and the Center have disaster recovery plans (DRP); however, the disaster recovery plans are incomplete and have not been tested. We found six community colleges that had no significant weakness in their disaster recovery plan. For the entities that had plans we looked for the following critical components:

- Executive management's signature of approval of the plan;
- Statement of the assumptions, such as the maximum time without computing, underlying the plan;
- Identification of critical applications in each user department and the priority in which these applications will be restored if resources are limited;
- Identification of key personnel and their assignments during the restoration of processing;
- Alternate user department procedures to manage their workloads until processing resumes;
- An inventory of equipment, special stock and arrangements to acquire replacement equipment; and
- A procedure to update the plan when there are major changes to the environment or at least annually.
- The disaster recovery plans are not tested annually.

Because the majority of the entities within NCCCS did not have adequate plans, we believe the overall risk level for this area is **HIGH**.


Disaster Recovery
Maximum Number of Findings is 2.
Wilkes
Western Piedmont
Wayne
Wake Tech
Vance-Granville
Tri-County
Surry
Stanly
Southwestern
Southeastern
South Piedmont
Sandhills
Sampson
Rowan-Cabarrus
Rockingham
Robeson
Roanoke-Chowan
Richmond
Randolph
Pitt
Piedmont
Pamlico
NC Center Applied Tech
Nash
Montgomery
Mitchell
Martin
Lenoir
Johnston
James Sprunt
Isothermal
Haywood
Halifax
Guilford
Gaston
Forsyth Tech
Fayetteville Tech
Edgecombe
Durham Tech
Davidson
Craven
College of Albemarle
Coastal Carolina
Cleveland
Central Piedmont
Central Carolina
Catawba Valley
Carteret
Cape Fear
Caldwell
Brunswick
Blue Ridge
Bladen
Beaufort County
Ashe-Bun Tech
Alamance
NCCCS
Inadequate DRP
NO DRP

NORTH CAROLINA COMMUNITY COLLEGE SYSTEM
H. Martin Lancaster, President

June 15, 2004

Mr. Ralph Campbell, Jr.
State Auditor
2 S. Salisbury Street
20601 Mail Service Center
Raleigh NC 27699-0601

Dear Mr. Campbell,

We have reviewed the results of the information systems (IS) audit described in your June, 2004 report, including the Audit Results. Our responses to each of the areas that were reviewed are as follows:

1. Overall Risk (High): We concur with the conclusions based on the number of weaknesses that were identified, and have initiated a collaborative effort with the 58 community colleges to identify necessary corrective actions.
2. General Security Issues (Low): Although the report stated that the nature of the weaknesses would result in a low risk, we are working collaboratively with the 58 colleges to identify standards and policies that will address the need for sound security management.
3. Access Controls (High): We concur with the conclusions in this area and have initiated efforts in collaboration with the 58 community colleges to develop policies, procedures and configurations to ensure that adequate access controls are implemented and maintained.
4. Systems Development (High): As stated in our response to Mr. Martin Vernon's letter of May 14, 2004, we concur with audit Finding on the Baseline for the Critical Operating System and will work to implement it.
5. Systems Software (High): We concur with the conclusions in this area and are working in collaboration with the 58 community colleges to develop effective procedures for system software maintenance.
6. Disaster Recovery (High): We concur with the conclusions and are working with the 58 community colleges' information systems and business administrators to develop effective business continuity plans.

Sincerely,

H. Martin Lancaster

cc: Dr. Saundra W. Williams

MAILING ADDRESS: 5001 MAIL SERVICE CENTER ~ RALEIGH, NC 27699-5001
Street Address: 200 West Jones ~ Raleigh, NC 27603-1379 ~ 919-807-7100 ~ Fax 919-807-7164
AN EQUAL OPPORTUNITY EMPLOYER

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with General Statutes 147-64.5 and 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller
Mr. Martin Lancaster	President, North Carolina Community College System

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore	Speaker of the House
Senator Marc Basnight, Co-Chair	Representative James B. Black, Co-Chair
Senator Charles W. Albertson	Representative Richard T. Morgan, Co-Chair
Senator Patrick J. Ballantine	Representative Martha B. Alexander
Senator Daniel G. Clodfelter	Representative Rex L. Baker
Senator Walter H. Dalton	Representative Bobby H. Barbee, Sr.
Senator Charlie S. Dannelly	Representative Harold J. Brubaker
Senator James Forrester	Representative Debbie A. Clary
Senator Linda Garrou	Representative E. Nelson Cole
Senator Wilbur P. Gulley	Representative James W. Crawford, Jr.
Senator Fletcher L. Hartsell, Jr.	Representative William T. Culpepper, III
Senator David W. Hoyle	Representative W. Pete Cunningham
Senator Ellie Kinnaird	Representative W. Robert Grady
Senator Jeanne H. Lucas	Representative Joe Hackney
Senator Stephen M. Metcalf	Representative Julia C. Howard
Senator Anthony E. Rand	Representative Joe L. Kiser
Senator Eric M. Reeves	Representative Edd Nye
Senator Robert A. Rucho	Representative William C. Owens, Jr.
Senator R. C. Soles, Jr.	Representative Wilma M. Sherrill
Senator Scott Thomas	Representative Thomas E. Wright

Other Legislative Officials

Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647