CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security
CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(6): Facility Security

Chesterfield County, Virginia
Internal Audit

9901 Lori Road, Room 142 – P.O. Box 40 – Chesterfield, VA 23832
Phone: (804) 748-1240 – Fax: (804) 768-9346 – Internet: chesterfield.gov

DATE: February 4, 2020

TO: Joseph P. Casey, Ph.D.
County Administrator

Chesterfield County
Board of Supervisors

Mervin B. Daugherty, Ed.D
Superintendent

Chesterfield County
School Board

FROM: Greg L. Akers Greg
Director of Internal Audit

SUBJECT: Accounting ONESolution Enterprise System Security Audit

The Office of Internal Audit completed an audit of Accounting ONESolution Enterprise System Security, and the final report is attached.

We would like to thank Mike Dance, Consuela Wilson, Sandy Graham, and Paula Aldous for their cooperation and assistance during this audit.

Attachment

Copy: Mike Dance, Assistant Director of Accounting
Consuela Wilson, Financial Systems Manager
Barry Condrey, Chief Information Officer
Sandy Graham, Information Security Manager
Paula Aldous, Finance Director (CCPS)
Matt Harris, Deputy County Administrator, Finance and Administration
Vacant, Director of Accounting
Vacant, Chief Finance Officer (CCPS)

Includes Freedom of Information Act (FOIA) exempt material that will be redacted prior to public disclosure.

Accounting ONESolution Enterprise System Security

February 4, 2020

Providing a FIRST CHOICE Community through Excellence in Public Service

CHESTERFIELD COUNTY
Internal Audit

Greg L. Akers, Director
Steve Sanderson, Audit Manager
Khara Durden, Technology Audit Manager
Lora Holland, Senior Auditor
Christopher Meade, Senior Auditor
Terry Parker, Senior Auditor
Jim Boudreau, Staff Auditor
Sandra Fuentes, Staff Auditor
Christian Wingfield, Staff Auditor
Annette Stinson, Administrative Analyst

Accounting ONESolution Enterprise System Security

Highlights

System Management and Access Controls

[redacted]

[redacted]

Change Controls and Threat Management

[redacted]

[redacted]

Application Security Monitoring

[redacted]

[redacted]

Management concurred with 9 of 9 recommendations detailed in the report to be implemented by July 1, 2020. Internal Audit performs annual follow-up with management to confirm implementation status.

INTRODUCTION

BACKGROUND

The County and Schools implemented the current enterprise system (In Focus) in 2008. The In Focus (now CentralSquare Technologies) system currently includes three primary applications:

- **ONESolution –** Financial system resource that includes reporting for: accounts payable, budgetary controls, cash management, cash receipting, fixed assets, general ledger, payroll, and procurement.
- **Timecard Online –** Employee time reporting resource that is used to track, monitor, and pay employees.
- **Employee Online** – Provides employee Human Resource (HR) services that include information for: pay (i.e. direct deposit, W2, deferred compensation), job (i.e. salary history), and benefits (i.e. open enrollment, current health/dental insurance).

ONESolution is the primary financial reporting system for County and Schools. The Accounting In Focus Security (IFS) team, comprised of five employees led by a Financial Systems Manager, provides support for ONESolution's 18,000-plus active user accounts including: providing helpdesk services, ensuring system availability, and maintaining system security documentation. Information Security Technology (IST) provides support (i.e. administration, security, and technical) for multiple systems including ONESolution with 26 employees led by the Chief Information Officer. The School Finance Director serves as a liaison with Accounting to manage ONESolution access for School users.

For FY21, the County plans to select a vendor for a County and School Enterprise Resource Planning Replacement (ERP) Study. If a replacement ERP is identified, funding will be allocated to pursue acquisition and implementation.

OBJECTIVES

Objectives of the audit were to:

- Verify physical and logical control existence.
- Test enterprise system controls operate as intended to restrict unauthorized data access.
- Confirm security management and administration roles and responsibilities have been clearly and appropriately defined for system support.
- Evaluate ONESolution update/patching procedure.
- Review malicious code/attack controls for ONESolution.
- Report the results to Management.

SCOPE

Our audit work covered FY19 and the current operating environment. We considered the following policies, procedures, and standards during our audit:

Accounting 1-19 In Focus Security and Responsibility	*IST 3-1 Security and Safety*
IST 7-3 Information Security Policy	*IST 7-5 Access to Distributed Systems*
IST Security Standard 70.101 Password Management	*National Institute of Standards and Technology (NIST) 800-53 National Vulnerability Database:* • *Access Control (AC)* • *Configuration Management (CM)* • *Physical and Environmental Protection (PE)* • *Security Assessment and Authorization (CA)* • *System Information Integrity (SI)*

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Steve Sanderson, Audit Manager, performed the audit work. Chesterfield County Internal Audit is a department within the organization of Chesterfield County/Schools

METHODOLOGY

Detailed information regarding the methodology can be found in the individual findings listed in the report. Our methodology included the following: interviews, observations, data analysis, and documentation review.

INTERNAL CONTROL CONCLUSION

According to Government Auditing Standards, internal controls, in the broadest sense, encompass the agency's plan, policies, procedures, methods, and processes adopted by management to meet its mission, goals, and objectives. Internal controls include the processes for planning, organizing, directing, and controlling program operations. It also includes systems for measuring, reporting, and monitoring program performance. An effective control structure is one that provides reasonable assurance regarding:

- efficiency and effectiveness of operations;
- accurate financial reporting; and
- compliance with laws and regulations.

Based on the results and findings of the audit test work, auditors concluded that internal controls were in place, but not consistently followed which could impact their ability to assist management in meeting its missions, goals, and objectives. Recommendations specific to improving these controls can be found in detail further in the audit report.

CLOSING

We would like to thank Accounting, IST, and Schools for their cooperation and assistance during this audit.

FINDINGS, RECOMMENDATIONS, RESPONSES

System Management and Access Controls

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(6): Facility Security

(Point Sheet 3)

CRITERIA:

County Administrative Policy 7-3: IST Information Security Policy establishes employee and system user control processes (i.e. unique identification credential use) to enhance user authorization, accountability, and prevent unauthorized computer access.

County Administrative Policy 7-5: IST Access to Distributed Systems Policy establishes organizational requirement for reporting personnel changes to reduce information security risks.

Chesterfield County IST Department Administrative Policy 3-1: Security and Safety define required physical controls to protect both its primary and remote physical premises from unauthorized access.

Chesterfield County IST Department Security Standard 70.101: Password Management defines required password structure (i.e. length and complexity) and management for Chesterfield County systems and applications requiring a login password.

National Institute Standards and Technology (NIST) Special Publication 800-53 provides technology control guidelines (i.e. best practices) for physical and logical security, that organizations may adopt, including:

- **Physical Access Control**: Enforces facility safeguards (i.e. controlling ingress/egress) to prevent unauthorized physical access where information system components reside (i.e. server rooms). **PE-3**
- **Account Management**: Includes user permission controls for organizational information systems and outlines account disabling/termination procedure. **AC-2**
- **Least Privilege**: Limits user access permissions for required job functions. **AC-6**
- **Configuration Settings**: Describes organizational system settings standards and responsibility for monitoring changes. **CM-6**

CONDITION(S):

[redacted]

[redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES

System Management and Access Controls

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(6): Facility Security

(Point Sheet 3)

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES

System Management and Access Controls

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(6): Facility Security

(Point Sheet 3)

[redacted]

[redacted]

[redacted]

<u>CAUSE(S):</u>

[redacted]

<u>EFFECT(S):</u>

[redacted]

ACTION(S) TAKEN:

[redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES

System Management and Access Controls

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(6): Facility Security

(Point Sheet 3)

RECOMMENDATION(S):

We recommend:

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

MANAGEMENT'S RESPONSE(S):

1. [redacted]

2. [redacted].

3. [redacted].

4. [redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES
Change Controls and Threat Management
CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security
(Point Sheet 2)

CRITERIA:

NIST Special Publication 800-53 provides technology control guidelines (i.e. best practices) for software application security, that organizations may adopt, including:

- **Configuration Change Control**: Includes organized processes to monitor and approve system changes and upgrades. **CM-3**
- **Configuration Management**: Designates key management stakeholders responsible for reviewing and approving proposed information system changes, and personnel that conduct security impact analyses for changes prior to system implementation. **CM-9**
- **Malicious Code Protection**: Includes controls for monitoring organization's computers and servers for viruses, worms, trojan horses, and spyware. **SI-3**
- **Penetration Testing**: A specialized assessment conducted on information systems internally or by third-party to identify vulnerabilities that adversaries may exploit. **CA-8**

CONDITION(S):

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES

Change Controls and Threat Management

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

(Point Sheet 2)

CAUSE(S):

[redacted] [redacted].

EFFECT(S):

[redacted] [redacted]

RECOMMENDATION(S):

We recommend:

5. [redacted]

6. [redacted]

MANAGEMENT'S RESPONSE(S):

5. [redacted]

6.

FINDINGS, RECOMMENDATIONS, RESPONSES

Application Security Monitoring

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

(Point Sheet 1)

CRITERIA:

County Administrative Policy 7-3: IST Information Security Policy establishes organizational security responsibilities (i.e. system abuse reporting, promote business continuity) and control processes (i.e. incident response and environment monitoring) to reduce information security risks.

County Administrative Policy 1-19: Accounting In Focus Security and Responsibilities establishes responsibilities for users accessing financial system data and controls for data housed in the enterprise system (ONESolution).

National Institute Standards and Technology (NIST) Special Publication 800-53 provides technology control guidelines (i.e. best practices) for software application security, that organizations may adopt, including:

- **Security Information and Event Management (SIEM)**: Real-time monitoring, correlation, and analysis of activity in your environment, detecting and alerting on valid threats to your data and devices. **AC-2 & AC-7**
- **Concurrent Logins Using Single Account**: Same user login on multiple machines may pose security threats for the entity. Monitoring helps prevent careless behavior (workstations left unlocked, password sharing), identify stolen passwords, monitor an individual users network actions, and ensure user accountability for all actions including malicious user activity. **AC-10**

CONDITION(S):

[redacted] ngle

CAUSE(S):

[redacted]

EFFECT(S):

[redacted]

FINDINGS, RECOMMENDATIONS, RESPONSES

Application Security Monitoring

CONFIDENTIAL, FOIA EXEMPT §2.2-3705.2(3): System Security

(Point Sheet 1)

RECOMMENDATION(S):

We recommend:

7. [redacted]
8. [redacted]
9. [redacted]

MANAGEMENT'S RESPONSE(S):

7. [redacted].

8. [redacted]

9. [redacted]