Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

QUALITY SOFTWARE SERVICES, INC., HAD NOT IMPLEMENTED UNIVERSAL SERIAL BUS DEVICE AND PORT CONTROLS

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Kay L. Daly
Assistant Inspector General

June 2013
A-04-12-05045

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

Quality Software Services, Inc., did not sufficiently implement CMS-required information system security controls over USB ports and devices, thus risking exposure of personally identifiable information for over 6 million Medicare beneficiaries.

WHY WE DID THIS REVIEW

Universal Serial Bus devices (USB devices) have become common in the workplace. Many individuals have several USB devices, such as jump drives and smart phones, for use with both their personal and professional computers. Because USB devices connect directly into computers and can store large amounts of data, they can potentially cause serious harm to computers and networks or compromise sensitive data if their use is not properly controlled. In an attempt to limit the risk to personally identifiable information (PII) for Medicare beneficiaries, we assessed the USB device controls at Quality Software Services, Inc. (QSSI), the contractor responsible for testing changes to the Centers for Medicare & Medicaid Services (CMS) Medicare systems and the effect of those changes on beneficiary data.

The objective of our audit was to determine whether QSSI had sufficiently implemented Federal requirements for information system security controls over USB ports and devices.

BACKGROUND

QSSI is a testing contractor for CMS that provides independent testing services for changes to Medicare Part A and B "Fee-for-Service" standard systems. Its test systems maintain data on over 6 million Medicare beneficiaries for testing purposes. QSSI provides related hardware, software, and connectivity required to host test environments and test software changes to the CMS Common Working File, Multi-Carrier System, Fiscal Intermediary Standard System, the Healthcare Integrated General Ledger Accounting System, and the Viable Information Processing System Medicare System.

WHAT WE FOUND

QSSI had not sufficiently implemented Federal requirements for information system security controls over USB ports and devices. Specifically, QSSI had not: (1) listed essential system services or ports in its system security plan or (2) disabled, prohibited, or restricted the use of unauthorized USB device access. QSSI had not implemented USB security controls because management had not updated its USB control policies and procedures. As a result of QSSI's insufficient controls over USB ports and devices, the PII of over 6 million Medicare beneficiaries was at greater risk from malware, inappropriate access, or theft.

WHAT WE RECOMMEND

We recommend that QSSI update and implement sufficient policies and procedures to ensure that USB controls comply with Federal requirements, including *CMS Information Security Acceptable Risk Safeguards.* Specifically, QSSI should:

- list essential system services and ports in its system security plan;
- update its policies and procedures to prohibit the use of unauthorized USB devices on its systems that store or process Medicare information;
- limit USB port access to essential connections; and
- disable, prohibit, or restrict unauthorized USB device access.

QUALITY SOFTWARE SERVICES, INC., COMMENTS AND OUR RESPONSE

In its response to our draft report, QSSI described the corrective actions it had taken and planned to take to address three of our four recommendations.

Specifically, QSSI:

- revised the corporate Network Access Control policy to establish usage restrictions and implementation guidance for mobile devices,
- plans to implement "Read only" restrictions for USB ports in all laptops and to disable the capability for automatic execution of code without user direction, and
- plans to require the scanning of all portable and mobile devices to detect malicious code.

However, QSSI did not address our first recommendation regarding its system security plan. We reiterate that QSSI should update its system security plan to include lists of essential system services and ports.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

Universal Serial Bus devices (USB devices) have become common in the workplace. Many individuals have several USB devices, such as jump drives and smart phones, for use with both their personal and professional computers. Because USB devices connect directly into computers and can store large amounts of data, they can potentially cause serious harm to computers and networks or compromise sensitive data if their use is not properly controlled. In an attempt to limit the risk to personally identifiable information (PII) for Medicare beneficiaries, we assessed the USB device controls at Quality Software Services, Inc. (QSSI), the contractor responsible for testing changes to the Centers for Medicare & Medicaid Services (CMS) Medicare systems and the effect of those changes on beneficiary data.

OBJECTIVE

The objective of our audit was to determine whether QSSI had sufficiently implemented Federal requirements for information system security controls over USB ports and devices.

BACKGROUND

Federal Government Information Security Controls and Requirements

The *Federal Information Security Management Act of 2002* (FISMA) and the Office of Management and Budget (OMB) required Federal agencies to comply with the National Institute of Standards and Technology (NIST) standards and guidelines to improve the efficiency and security for Federal information systems. In response to FISMA, NIST published the *Federal Information Processing Standard 200* (FIPS 200), which designates NIST *Special Publication* (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, as amended, to meet FISMA requirements.

To comply with FISMA, CMS incorporated NIST SP 800-53 into its *CMS Information Security Acceptable Risk Safeguards* (*Risk Safeguards*). CMS requires that all of its FISMA-governed systems, including those managed by its contractors, follow these *Risk Safeguards*.

Universal Serial Bus Devices

USB devices include portable data storage devices, commonly known as jump, flash, or thumb drives, and other devices that can store data and connect to systems through USB ports (e.g., external hard drives, iPods, and smart phones). Despite being small and highly portable, USB devices can store and transport large amounts of data, thus creating a vulnerability to computer systems and sensitive data, including proprietary information and PII.

An example of how USB devices can infect computer networks with malicious software (malware) occurred in 2008 when an individual inserted an infected USB device into a military computer. The USB device transmitted malware into the computer, and the malware spread

undetected to other government computer networks. Deputy Defense Secretary William Lynn described that incident as the "most significant breach of U.S. military computers ever." Since then, other publicized incidents of USB device malware transmission included the 2010 "Stuxnet" infection of Iran's nuclear facilities and the "Gauss" malware, which was used to steal information from the banking industry.

An example of how USB devices can contribute to the loss of PII occurred in 2011 when a University of Texas trainee lost an unencrypted USB device on the employee shuttle bus. The unencrypted USB device potentially exposed medical records containing the PII of 2,200 patients. In another recent incident in July 2012, a home burglar in Oregon stole a hospital employee's thumb drive containing data on over 14,000 patients. In many of these cases, it is difficult to determine whether or when anyone will use the breached data in a crime.

Quality Software Services, Incorporated

QSSI is a testing contractor for CMS that provides independent testing services[1] for changes to Medicare Part A and B "Fee-for-Service"[2] standard systems. Its test systems maintain data on over 6 million Medicare beneficiaries for testing purposes.[3] QSSI provides related hardware, software, and connectivity required to host and test software changes to the CMS Common Working File, Multi-Carrier System, Fiscal Intermediary Standard System, the Healthcare Integrated General Ledger Accounting System, and the ViPS Medicare System.[4]

HOW WE CONDUCTED THIS REVIEW

We limited our review to the controls and workstation configurations QSSI established over USB ports and devices. We assessed how QSSI set up its USB ports for 30 judgmentally selected workstations at QSSI's office in Columbia, South Carolina. In addition, we reviewed QSSI's policies for users to follow.

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.

[1] QSSI performs systems, functional, integration, volume regression, and production-ready testing on changes to Medicare standard systems for CMS.

[2] **Fee-for-Service** is a separate payment to a health-care provider for each medical service rendered to a patient.

[3] QSSI's test environment contains all the information necessary to process a Medicare transaction. As of October 9, 2012, this information included 6,667,459 unique Medicare beneficiary records.

[4] Viable Information Processing System Medicare System.

Appendix A contains the details of our audit scope and methodology. Appendix B contains a description of risk levels and the resulting necessary actions.

FINDING

QSSI had not sufficiently implemented Federal requirements for information system security controls over USB ports and devices. Specifically, QSSI had not:

- listed essential system services or ports in its system security plan; or
- disabled, prohibited, or restricted the use of unauthorized USB device access.

QSSI had not implemented USB security controls because its management had not updated its USB control policies and procedures. As a result of QSSI's insufficient controls over USB ports and devices, the PII of over 6 million Medicare beneficiaries was at greater risk from malware, inappropriate access, or theft.

UNIVERSAL SERIAL BUS DEVICE SECURITY CONTROLS NOT SUFFICIENTLY IMPLEMENTED

CMS's *Risk Safeguards* require that business owners, including contractors, include essential USB ports in their system security plans and set up their workstations to restrict the use of unnecessary USB ports. The *Risk Safeguards* further require that business owners prohibit the use of unauthorized USB devices in CMS information systems. (For details on the Federal requirements related to controls over USB ports and devices, see Appendix C.)

Although QSSI advised its users against using personal devices on work computers and warned them not to connect USB devices from unknown sources into work computers as part of its Security Awareness training, QSSI had not sufficiently implemented Federal requirements for information system security controls over USB ports and devices. Specifically, QSSI had not:

- listed essential system services or ports in its system security plan; or
- disabled, prohibited, or restricted the use of unauthorized USB device access.

QSSI had not implemented USB security controls because its management had not updated its USB control policies and procedures. QSSI officials maintained that the security guidelines covered during Security Awareness training were not part of QSSI's policies and that QSSI had not required employees to follow those guidelines.

We assigned a risk ranking of "high" to this finding based on the criteria listed in the NIST SP 800-30. (For details on risk ranking criteria, see Appendix B.) Because of insufficient controls prohibiting the use of unauthorized USB device access, QSSI employees had connected a wide variety of personal USB devices to the 30 tested workstations. For example, someone had connected 28 different USB mass storage devices to one workstation, but QSSI was not able to determine whether the 28 devices were authorized. Twenty-nine of the thirty workstations

showed evidence that additional devices had been connected to USB ports, including camcorders, tablets, iPods, eBooks, navigation devices, and smart phones. The uncontrolled USB port access increased the possibility that anyone with physical access to a USB port could have introduced malware to CMS test systems or inappropriately accessed Medicare beneficiary PII, thus putting the PII of over 6 million Medicare beneficiaries at greater risk from malware, inappropriate access, or theft.

RECOMMENDATIONS

We recommend that QSSI update and implement sufficient policies and procedures to ensure that USB controls comply with Federal requirements, including CMS's *Risk Safeguards*. Specifically, QSSI should:

- list essential system services and ports in its system security plan;
- update its policies and procedures to prohibit the use of unauthorized USB devices on its systems that store or process Medicare information;
- limit USB port access to essential connections; and
- disable, prohibit, or restrict unauthorized USB device access.

QUALITY SOFTWARE SERVICES, INC., COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In its response to our draft report, QSSI described the corrective actions it had taken and planned to take to address three of our four recommendations.

Specifically, QSSI:

- revised the corporate Network Access Control policy to establish usage restrictions and implementation guidance for mobile devices,
- plans to implement "Read only" restrictions for USB ports in all laptops and to disable the capability to automatically run applications without user direction, and
- plans to require the scanning of all portable and mobile devices to detect malicious code.

However, QSSI did not address our first recommendation regarding its system security plan. We reiterate that, to comply with Federal regulations, QSSI should update its system security plan to include lists of essential system services and ports.

We included QSSI's comments in their entirety as Appendix D. However, we redacted the names in the "To" field of the email QSSI used for communicating its comments to our report because it contained the names of auditors and program officials not employed by QSSI. We

also redacted the name of the software QSSI stated it plans to use on its portable and mobile devices to detect malicious code and computer viruses.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We limited our review to the controls over QSSI's USB ports and devices and did not evaluate its internal controls as a whole.

Specifically, we determined whether QSSI had policies governing USB device usage on QSSI systems and what logical controls QSSI had over USB port functionality on individual workstations. We also evaluated the number and type of USB devices connected to QSSI workstations at one QSSI office.

We performed our fieldwork at QSSI's facility located in Columbia, South Carolina, during May 2012.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal laws, regulations, and guidance;
- assessed QSSI policies for control over USB devices;
- interviewed QSSI staff about USB device controls and information system configurations; and
- judgmentally selected 30 workstations with access to the QSSI network to assess their USB port configurations and determine all previous USB devices connected to those workstations.

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 objective.

APPENDIX B: RISK SCALE AND NECESSARY ACTIONS

RISK RANKING CRITERIA

We have assigned risk ranking to our finding based on the criteria listed in the NIST SP 800-30, dated July 2002, Table 3-7, entitled *Risk Scale and Necessary Actions* (below). To assign the risk ranking, we considered the Likelihood Level (Table 3-4) and Magnitude of Impact (Table 3-5), both also in SP 800-30. We limited our assessment of Magnitude of Impact to the risks associated with QSSI's Medicare testing program and, specifically, with the confidentiality of Medicare beneficiary data. The risk scale shown below represents the degree or level of risk to which an IT system can be exposed if a vulnerability is exploited.

Table 3-7. *Risk Scale and Necessary Actions*

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's Designated Approving Authority must determine whether corrective actions are still required or decide to accept the risk.

APPENDIX C: FEDERAL REQUIREMENTS FOR UNIVERSAL SERIAL BUS CONTROLS

FISMA and OMB required Federal agencies to comply with NIST standards and guidelines to improve the efficiency and security for Federal information systems. In response to FISMA, NIST published FIPS 200, which designates NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, as amended, to meet FISMA requirements.

To comply with FISMA, CMS incorporated NIST SP 800-53 into its *Risk Safeguards*.

The CMS *Risk Safeguards* (Rev.1, 05-24-11) *Scope* states:

> All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions and performing work on behalf of CMS shall observe the baseline policy statements described in the … [Policy for the Information Security Program] and the complementary controls defined in the … [*Risk Safeguards*] as the minimum security requirements for all CMS information and information systems.

CMS *Risk Safeguards, Rev.1, 05-24-11, Appendix B*: *CMS Minimum Security Requirements for Moderate Impact Level Data,* Section 5.0, *Configuration Management (CM) – Operational - CM-7 – Least Functionality (Moderate) Control* states:

> The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the … [system security plan]; all others will be disabled.

CMS *Risk Safeguards, Rev.1, 05-24-11, Appendix B*: *CMS Minimum Security Requirements for Moderate Impact Level Data,* Section 1.0, *Access Control (AC) – Technical - AC-19 – Access Control for Mobile Devices (Moderate) Controls* states:

> The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative.
>
> AC-19 (1) – Enhancement (Moderate)
>
> The organization restricts the use of writable, removable media in CMS information systems.

AC-19 (2) – Enhancement (Moderate)

The organization prohibits the use of personally owned, removable media in CMS information systems.

AC-19 (3) – Enhancement (Moderate)

The organization prohibits the use of removable media in CMS information systems when the media has no identifiable owner.

Appendix D: QUALITY SOFTWARE SERVICES, INCORPORATED COMMENTS

From: Anh Tran
[redacted]
Subject: RE: A-04-12-05045 written comments not received
Date: Friday, January 11, 2013 1:43:45 PM

Beverly,

Thank you for the follow-up. Please see below our comment to the finding:

QSSI has revised the corporate Network Access Control policy to establish usage restrictions and implementation guidance for mobile devices. Accordingly, QSSI plans to implement a group policy that enforces "Read' only access right for USB ports in all STC laptops and disables the capability for automatic execution of code without user direction; all portable and mobile devices must be scanned using [redacted] software to detect malicious code and computer virus.

Please let me know should you have any questions.

Thank you!

Anh Tran
ATran@QSSInc.com
[redacted]