OFFICE OF THE STATE INSPECTOR GENERAL

COMMONWEALTH OF VIRGINIA

AUDIT REPORT

Removal of Commonwealth Data from Electronic Storage

Report No. 2022-PA-004

June 23, 2022

Prepared By:

SysAudits | Systems Security Audit Professionals

SysAudits | Systems Security Audit Professionals

COMMONWEALTH OF VIRGINIA

Office of the State Inspector General

Michael C. Westfall, CPA
State Inspector General

P.O. Box 1151
Richmond, Virginia 23218

Telephone 804-625-3255
Fax 804-786-2341
www.osig.virginia.gov

June 24, 2022

The Honorable Glenn Youngkin
Governor of Virginia
P.O. Box 1475
Richmond, VA 23219

Dear Governor Youngkin,

The Office of the State Inspector General engaged SysAudits, LLC to conduct an audit of the Removal of Commonwealth Data from Electronic Storage. The report is included below for your review and information.

OSIG would like to thank Department of General Services Director Joseph Damico and Virginia Information Technologies Agency Chief Information Officer Robert Osmond and their staffs for their cooperation and assistance during this audit.

Sincerely,

Michael C. Westfall, CPA
State Inspector General

cc: The Honorable Jeff Goettman, Chief of Staff to Governor Youngkin
The Honorable Rebecca Glover, Deputy Chief of Staff to Governor Youngkin
The Honorable Margaret McDermid, Virginia Secretary of Administration
The Honorable Emily Brewer, House Chair, Communications, Technology and Innovation Committee
The Honorable George Barker, Senate Chair, General Laws and Technology Committee
Joseph Damico, Director, Department of General Services
Robert Osmond, Chief Information Officer, Virginia Information Technologies Agency
Staci Henshaw, Auditor of Public Accounts

Executive Summary

SysAudits, LLC performed the Removal of Commonwealth Data from Electronic Storage audit on behalf of the Office of the State Inspector General. We conducted this audit from April 20, 2021, through May 31, 2022, in accordance with Government Accountability Office, 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.

The scope of this review included an examination of information technology assets used by executive branch agencies to ensure that agencies and contractors sanitize Commonwealth of Virginia (COV) data as required by Virginia Information Technologies Agency (VITA) Information Technology Resource Management standards and best practices. The audit included assessing data removal contracts issued by Department of General Services (DGS). Our audit methodology included selecting a random and judgmental sampling of 15 executive branch agencies across the Commonwealth. The audit methodology included reviewing agency policy alignment with policies issued by VITA; examining agency and contractor processes for removing data from media; and quality process testing to ensure COV data is removed from media prior to disposal.

In general, we found that some agencies had issued agency policies for data removal, while some had not. We also determined that most agencies rely on VITA to perform data removal services for their respective media. Some agencies that did perform data removal did successfully remove data from laptop computers but did not fully remove data from cell phones. The audit also included site visits to state contractors that perform data removal services. We did not note any contractor exceptions in the data removal processes. The audit identified six areas for improvement and consideration. Although VITA has instituted standards for the removal of Commonwealth data from media storage devices and the processes that agencies are to institute, COV should consider the following recommendations to ensure consistency in the application of the standards and the protection of COV sensitive or confidential data through proper oversight and enforcement:

1. Align agency policies and procedures to VITA SEC501, SEC514-05 data removal requirements.
2. Update COV policy for data removal verification.
3. Use the mandatory DGS vendors for data removal services.
4. Perform contractor quality assurance reviews on vendors that perform data removal services.
5. Implement a documented process to perform quality assurance verification that agencies or contractors removed data from sanitized media.
6. Provide COV agencies with recommended cell phone data removal tools and procedures.

Both DGS and VITA concurred with the report findings.

David Cole, CPA, CISA, CRISC, SysAudits.com LLC

Background

Virginia Information Technologies Agency facilitates development and provides oversight to ensure that agencies use and appropriately manage IT resources within enterprise projects and procurements in support of agency business objectives. VITA's Information Technology Resource Management Policy Manual provides direction and oversight through standards and guidelines to establish rules and ensure the effective and efficient use and management of IT resources. Specifically, VITA's ITRM – Removal of Commonwealth Data from Electronic Media Standard is the framework provided to executive agencies in establishing policies and processes in the removal of electronic media and the standard used for purposes of this performance review. The EMS applies to all electronic media that has a memory such as the hard drives of personal computers, servers, mainframes, routers, firewalls, switches, tapes, diskettes, CDs, DVDs, mobile devices, printers, multi-function devices and USB data storage devices.

IT devices can be disposed of or sanitized through various methods. Agencies and contractors must remove information from IT assets before disposal or they must physically destroy the asset. If the Commonwealth is going to repurpose or reuse an asset, the storage media must undergo sanitization, a method to make the data unrecoverable, such as overwriting, degaussing or encryption.

To ensure the protection of Commonwealth data, agencies and contractors must sanitize properly or physically destroy IT assets at the end of their useful life to prevent unauthorized access to sensitive information.

Controls relating to data sanitization and destruction of IT assets, such as effective policies and procedures, is critical in ensuring the protection of sensitive information during the sanitization and disposal phase of the IT asset management life cycle.

The objective of this review is to ensure that the Commonwealth appropriately removes data from electronic media prior to the surplus or disposal of assets as required by VITA's ITRM standards.

Audit Objectives

The objectives of this audit are to assess whether:

- Executive branch agencies properly identify, track and remove Commonwealth data from all electronic media.
- An independent quality assurance function performs adequate testing of the data removal process.
- The methodologies of vendors identified by DGS to perform data cleaning transfer surplus property and recycling services to state agencies and other public bodies in the Commonwealth to ensure data is removed.
- Agencies and contractors have erased completely, or otherwise made unreadable in accordance with VITA standards, equipment from Surplus Property Management.

- VITA and DGS have proper oversight authority and capability to ensure protection of Commonwealth data related to disposal of assets.

Audit Scope, Methodology, Sampling

Scope

The scope of this review includes an examination of IT assets used by executive agencies to ensure that agencies and vendors have sanitized Commonwealth data as required by VITA ITRM standards and best practices for July 1, 2019, through April 30, 2022.

Methodology

Audit methodology includes:

- Determining if executive agencies comply with VITA ITRM policies for media sanitization and disposal.
- Determining the effectiveness of media sanitization, disposal processes and tools.
- Determining if sanitization vendors and executive agency system administrators are protecting information when disposing of Commonwealth electronic media.
- Determining if inventory records are accurate and complete to ensure that electronic media was sanitized or disposed of.

Sampling

SysAudits performed both random and judgmental sampling in the selection of agencies to be in-scope. The following agencies were selected for audit:

1	DHRM	Department of Human Resource Management
2	DOC	Department of Corrections
3	ESH	Eastern State Hospital
4	DPB	Department Planning and Budget
5	Treasury	Department of Treasury
6	VDOT	Virginia Department of Transportation
7	VSP	Virginia State Police
8	DOA	Department of Accounts
9	DJJ	Department of Juvenile Justice
10	DCJS	Department of Criminal Justice Services
11	ELECT	Department of Elections
12	SVMHI	Southern Virginia Mental Health Institute
13	VSU	Virginia State University
14	VITA	Virginia Information Technologies Agency
15	DMAS	Department of Medical Assistance Services

Finding 1: Agency Internal Policies Did Not Fully Document Removal or Destruction in Accordance with COV Standards

Not all agencies have policies and procedures that address or implement all of the requirements in the standards or agency specific processes in the removal or destruction of COV data in media storage devices. SysAudits identified the following exceptions:

1. Three of the 15 agencies reviewed (DMAS, ELECT, DPB) did not explicitly state in agency policies and procedures that they follow COV ITRM Standard 514. Treasury includes COV SEC514 statement in a separate document (How to Track and Destroy Removable Media) that is not associated with policies and procedures.
2. One of the 15 agencies reviewed (DMAS) did not explicitly state that it follows the standards (SEC501 or SEC514) in agency policies and procedures.
3. Two agencies reviewed (VSP and ELECT) did not remove all Commonwealth data from mobile devices prior to surplus, disposal or destruction of assets. In both instances the information recoverable was text messages and voice mails. VSP collects and secures mobile devices in a locked cabinet until they are destroyed. ELECT performs a factory reset per vendor guidance.

Overall, agencies do not perform media sanitization and destruction of IT assets prior to media updates and replacements. Agencies rely on the VITA/Ironbow vendor to sanitize according to the standards. Eight of the agencies reviewed (DPB, VSP, DOC, ESH, DCJS, DOE, SVMHI, VSU) have a limited number of agency-owned IT assets and perform some sanitization and destruction of those assets.

Ten of the agencies incorporated COV ITRM Standard SEC 501, Controls MP-1 through MP-6, which have similar requirements to COV ITRM SEC514, but DMAS, Treasury, DPB and ELECT did not directly reference VITA ITRM Standard SEC514-05.1 in internal agency policies and procedures. In addition, VITA supplies and manages IT assets for agency use. Most agencies reviewed under this audit receive media (laptops) support from VITA/Ironbow. Overall, agencies do not perform media sanitization and destruction of IT assets prior to media updates and replacements. Agencies rely on and assume that the VITA/Ironbow vendor properly sanitizes according to the Standards. Eight of the agencies reviewed (DPB, VSP, DOC, ESH, DCJS, DOE, SVMHI, VSU) have a limited number of agency-owned IT assets and perform some sanitization and destruction of those assets.

Not fully implementing policies and procedures can create confusion and information security risks as well as data leakage liability for the COV and agency. In addition, agencies not removing data prior to transferring to support contractors is a risk that support contractors can access data and thereby pose a data leakage risk.

Criteria

VITA ITRM Standard SEC514-05.1 Removal of Commonwealth Data from Electronic Media Standard - A.1 General Steps, states: a) Before electronic media is surplused, transferred (includes reassignment within the agency), traded-in, disposed of, or replaced, all data must be completely erased or otherwise made unreadable in accordance with this standard; however, only after the data has been reviewed and processed for retention in accordance with the agency's records retention policy.

Per COV security standards, all agencies are required to conduct risk assessments that use, as a minimum, controls from SEC501, SEC525, SEC520, NIST Cybersecurity Framework, all application COV security standards and CIS critical controls. Agencies are required to submit the results of those risk assessments to VITA Commonwealth Security for review and are then monitored for acceptable remediation. A properly documented risk assessment would include a review of internal policy deficiencies.

Recommendations

1. Communicate to agencies to include in their annual risk assessment that their internal policies and procedures clearly address SEC501, SEC514-05 data removal requirements and ITRM Standard 514.
2. Clarify and communicate to state agencies that they should remove and sanitize all media prior to disposal, surplus or transfer, including if the state contractor owns and manages the media assets.

VITA's Response

1. VITA will notify agencies that they are required to conduct a Risk Assessment that uses minimum controls from SEC501, SEC525, SEC520, NIST Cybersecurity Framework, all application COV security standards and CIS Critical Controls, including a review of internal policy deficiencies.
2. VITA will communicate to agencies through a general email notification that they must have internal policies and procedures that specifically reference and clearly address data removal requirements specified in SEC501 and in SEC514.

In addition, VITA will review its processes, provide additional guidance, and clarify to agencies that they must ensure compliance with requirements of data removal and media sanitation potentially before (depending on data sensitivity) and after providing equipment to the contractor. They must check and document that full utilization of contractor services meets the requirements.

Estimated Completion Date: November 30, 2022

Finding 2: COV Policy on Verification of Data Removal

The COV policy to verify that agencies and contractors have removed data from media does not ensure that it has taken place. COV policy recommends testing media by booting the device to ensure data is removed from media. The COV needs to update its policy on verification of the data removal process. Booting media only tests whether that process is working properly. Data removal testing and/or validation by booting a system does not ensure agencies and contractors removed data from media and it puts COV at risk of data remaining on media.

Criteria

VITA ITRM Standard SEC514-05.1 Removal of Commonwealth Data from Electronic Media Standard, section B. Quality Assurance Testing of Data Removal requires that, "Test methods may include physical observation if the data removal method was physical destruction, or another method is *attempting to boot up and read data* if the method was overwriting. If testing of a sample reveals a failure in data removal the agency's ISO must be notified and all devices in that lot must be tested."

Recommendation

Update COV policy to enhance the level of verification, such as forensic validation that agencies and contractors have removed data instead of using the media booting process.

VITA's Response

The current process for verification of data removal entails more than a media boot up process. The policy will be clarified and additional guidance will be provided to indicate that agencies must use an appropriate method of media sanitation and data removal, such as the process outlined in VITA ITRM Standard SEC514-05.1 Appendix A.

Estimated Completion Date: November 30, 2022

Finding 3: Unapproved Vendor - Document Destruction of Virginia

Treasury contracted with Document Destruction of Virginia to provide data destruction and disposal of media storage devices without DGS coordination. DGS does not have DDV listed as a contacted vendor under the Office of Surplus Property Management. Treasury personnel were not aware of DGS media sanitization contracts and took the initiative to contract for media data removal services. There is the risk that media is not property sanitized in accordance with COV policies, and that confidential or sensitive data, personally identifiable information, trade secrets, copyrights and other intellectual property remain stored on the electronic media.

Criteria

In accordance with the Agency Procurement and Surplus Property Manual Section 7. Surplus Computers and Related Equipment, "Surplus computers and related equipment often have value in the resale market. Older systems may not have resale value and should be recycled for scrap content. Contact the Director, DGS/OSPM for guidance for resale potential and approved recycling outlets. Agencies must manage their surplus electronics responsibly in order to conform to local, state and federal environmental regulations."

Recommendation

Use only contracted vendors as required by DGS or maintain a record of written approvals by the DGS Director for vendors not approved by the Office of Surplus Management.

Department of Treasury Response:

Treasury had old hard drives (not surplus equipment) that were stored in a locked location at the office and determined the drives were not needed at Treasury and the data was able to be destroyed. Treasury then reached out to VITA to see they had a vendor to help Treasury destroy the drives in compliance with SEC514. The VITA SCM Representative informed the Treasury they did not have any vendors on contract for this purpose and did not lead us to DGS for the services. Treasury then researched the DGS Statewide Contracts Listing from eVA on the DGS Website, and this contract is not on the list, and neither are the vendors.

The media was destroyed completely on-site with Treasury personnel present to witness the entire destruction process and maintain possession until the drives were fed through the shredder. A Treasury staff member observed the output of the devices from the shredder as the drive was crosscut. Treasury did not contract to send any media off-site or surplus the hardware so the risk of data being released as documented in the finding was not deemed a risk.

DGS's Response:

APSPM Chapter 12, section 7 is clear on how to handle the surplus of computers and related equipment. DGS agrees that Treasury should not have created their own contract and rather should have utilized the process outlined in the APSPM. DGS will reach out to Treasury to inform them of the processes in place, and current contracts, for surplus computer equipment.

Estimated Completion Date: June 30, 2022

Finding 4: Contracted Data Removal Oversight

VITA and DGS have established contracts for data removal from COV media. However, they have not established a process for on-site visits and independent verification to ensure that contractors have performed those tasks prior to surplus, sale or destruction in accordance with COV policy. VITA does not perform on-site inspections, but rather relies on SOC Type 2 independent audits. The risks are potential violation of software license agreements, unauthorized disclosure of information such as personally identifiable information, trade secrets, copyrights and other intellectual property that might be stored on the electronic media.

Criteria

Code of Virginia § 2.2-1124 16 states, "Require, to the extent practicable, the recycling and disposal of computers and other information technology assets. Additionally, for computers or information technology assets that may contain confidential state data or personal identifying information of citizens of the Commonwealth, the Department shall ensure all policies for the transfer or other disposition of computers or information technology assets are consistent with data and information security policies developed by the Virginia Information Technologies Agency."

Further, VITA ITRM Standard SEC514-05.1 Removal of Commonwealth Data from Electronic Media Standard requires, "The surplus, transfer (including reassignment within the agency), trade-in, disposal, or replacement of electronic media can create information security risks for the agency. This standard applies to all electronic media that has memory such as the hard drives of personal computers, servers, mainframes, mobile devices, routers, firewalls, switches, tapes, diskettes, CDs, DVDs, mobile devices, printers, Multi-Function Devices (MFD), and Universal Serial Bus (USB) data storage devices."

The risks to potential violation of software license agreements, unauthorized disclosure of information such as personally identifiable information, trade secrets, copyrights and other intellectual property that might be stored on the electronic media are high. All electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all Commonwealth data securely removed from the electronic media as specified by this standard before the electronic media is surplused, transferred, traded-in, otherwise disposed of or replaced.

e) The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.

g) The certification process must be completed by an agency authorized official. As such, the agency head or designee must appoint an individual to be responsible for the electronic data removal process.

B. Quality Assurance Testing of Data Removal
The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The quality assurance tester shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable."

Recommendations

Establish a process for COV to perform quality assurance reviews with contracted vendors that perform data removal services for media.

DGS's Response:

In reading the SEC514-05.1 policy, it states that the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The policy appears to require agencies to first remove all data prior to sending to surplus/Powerhouse, who then conducts a second "cleaning" and has various checks in place prior to surplusing the items. It could be interpreted that the data removal vendor is conducting the quality assurance function independent of the organizational unit who initially performed the data removal. However, due to the sensitivity of ensuring the data removal process is conducted in accordance with the required contract terms, DGS will work with VITA to conduct site visits to verify the process.

Estimated Completion Date: December 31, 2022

Finding 5: Agencies Data Removal Process

Agencies are not ensuring that they are removing data from cell phone media. Some agencies perform media data removal internally from laptops and cell phones. SysAudits determined from its analyses and verification, for the four agencies reviewed, of the data removal processes that at:

- DBP - Thirty-eight Surface Pro laptops were reviewed and no data was discovered on the media.
- VSP - Four laptops were reviewed, and no data was discovered on laptops; four cell phones were reviewed and data was discovered on one sanitized phone. VSP secures cell phones until they are destroyed.
- ELECT - Three cell phones were reviewed and data was discovered on sanitized phones.
- VSU - Two laptops were reviewed, and no data was discovered on the laptops; two cell phones were reviewed and no data was discovered on the cell phones.

Contract vendor site visits determined the following:

- Powerhouse Recycling - Two laptops were reviewed and no data was discovered on laptops; two cell phones were reviewed and no data was discovered on the phones.
- C2 Technologies - C2 did not have media to review and stated it had not received any COV media in more than a year.
- Ironbow/Core Technologies - Two laptops were reviewed and no data was discovered on laptops; two cell phones reviewed and no data was discovered on the cell phones.

In addition, the same four agencies (DPB, VSP, ELECT, VSU) performing some level of media sanitization did not have documentation that they performed reconciliation processes to ensure data was removed from media prior to disposal.

Although some agencies properly removed data from media, the agencies did not have a quality assurance test and verification process to ensure that they removed data from sanitized media. In addition, agencies did not provide documentation, as identified in VITA ITRM Standard SEC514-05.1 Removal of Commonwealth Data from Electronic Media Standard, to support the completion of a quality assurance function over the data removal process.

Data not properly removed can be accessed if the media is transferred for re-use, sold for salvage or lost prior to destruction. By not removing all data, the COV is at risk of data leakage and compromise of personal identifiably information or sensitive state data not for public release.

Criteria

VITA ITRM Standard SEC514-05.1 Removal of Commonwealth Data from Electronic Media Standard requires:

B. Quality Assurance Testing of Data Removal.

The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The quality assurance tester shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable.

The testing must be documented including date, tester(s), total number of devices in the lot, number tested, method of testing and the result. Testing must be performed within one week of the data removal. Test methods may include physical observation if the data removal method was physical destruction or attempting to boot up and read data if the method was overwriting. If testing of a sample reveals a failure in data removal the agency's ISO must be notified and all devices in that lot must be tested.

C. Certification and Auditing

The data remover must document *and certify that the data has been effectively removed*.

Recommendations

1. Implement a documented process to perform quality assurance verification that agencies or contractors removed data from sanitized media.
2. Provide agencies with recommended tools and procedures that ensure that agencies and contractors remove data from COV cell phones.

VITA's Response

VITA will assist agencies with ensuring that they are able to obtain the necessary documentation from the supplier, whether Iron Bow or another supplier. VITA will also review its processes and offer additional guidance concerning phone sanitization.

Estimated Completion Date: November 30, 2022

Appendix I – VITA & DGS Corrective Action Plan

VITA Corrective Action Plan

Finding No.	Recommendation	Corrective Action	Deliverable	Estimated Completion Date	Responsible Position
1	1. Communicate to agencies to include in their annual risk assessment that their internal policies and procedures clearly address SEC501, SEC514-05 data removal requirements and ITRM Standard 514. 2. Clarify and communicate to state agencies that they should remove and sanitize all media prior to disposal, surplus or transfer, including if the state contractor owns and manages the media assets.	1. VITA will notify agencies that they are required to conduct a Risk Assessment that uses as a minimum controls from SEC501, SEC525, SEC520, NIST Cybersecurity Framework, all application COV security standards and CIS Critical Controls, including a review of internal policy deficiencies. 2. VITA will communicate to agencies through a general email notification that they must have internal policies and procedures that specifically reference and clearly address data removal requirements specified in SEC501 and in SEC514. VITA will also review its processes, provide additional guidance, and clarify to agencies how to use the platform and tools, including full utilization of contractor services to document and comply with media sanitation and data removal requirements.	Communication reiterating Commonwealth Security standard requirements for required Risk Assessment Email notification to agencies to reference and address data removal requirements in SEC501 and in SEC514	November 30, 2022	Ed Miller, Director, IT Governance

Finding No.	Recommendation	Corrective Action	Deliverable	Estimated Completion Date	Responsible Position
2	Update COV policy to enhance the level of verification, such as forensic validation that agencies and contractors have removed data instead of using the media booting process.	The current process for verification of data removal entails more than a media boot up process. The policy will be clarified and additional guidance will be provided to indicate that agencies must use an appropriate method of media sanitation and data removal, such as the process outlined in VITA ITRM Standard SEC514-05.1 Appendix A.	Clarified policy and guidance to agencies that they must use an appropriate method of media sanitation and data removal, such as the process outlined in VITA ITRM Standard SEC514-05.1 Appendix A.	November 30, 2022	Ed Miller, Director, IT Governance
5	1. Implement a documented process to perform quality assurance verification that agencies or contractors remove data from sanitized media. 2. Provide agencies with recommended tools and procedures that ensure that agencies and contractors remove data from COV cell phones.	1. VITA will assist agencies with ensuring that they are able to obtain the necessary documentation from the supplier, whether Iron Bow or another supplier. 2. VITA will review its processes and offer additional guidance concerning phone sanitization.	1. VITA will assist agencies to obtain necessary documentation from the supplier. 2. VITA will provide additional guidance regarding phone sanitization.	November 30, 2022	Ed Miller, Director, IT Governance

DGS Corrective Action Plan

Finding No.	Recommendation	Corrective Action	Deliverable	Estimated Completion Date	Responsible Position
3	Use only contracted vendors as required by DGS or maintain a record of written approvals by the DGS Director for vendors not approved by the Office of Surplus Management.	DGS will reach out to Treasury to inform them of the processes in place and current contracts in place for surplus computer equipment.	Document discussion and outcome. Assist agency as necessary.	6/30/2022	DGS/DPS Floyd Coburn
4	Establish a process for COV to perform quality assurance reviews with contracted vendors that perform data removal services for media.	DGS will work with VITA to establish a process for periodic quality assurance reviews with contracted data removal vendors.	Policy/process on conducting periodic qualify assurance reviews with contracted data removal vendors.	12/31/2022	DGS/DPS Floyd Coburn in conjunction with appropriate VITA personal