



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES
Dallas/New York Audit Region

July 12, 2016

Control Number
ED-OIG/A02P0006

Dr. Steven R. Staples
Superintendent of Public Instruction
Virginia Department of Education
James Monroe Building
101 N. 14th Street
Richmond, VA 23219

Dear Dr. Staples:

This final audit report, "Protection of Personally Identifiable Information in the Commonwealth of Virginia's Longitudinal Data System," presents the results of our audit. The purpose of the audit was to determine if the Virginia Department of Education (VDOE) has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in the Commonwealth of Virginia's (Virginia) Statewide Longitudinal Data System (SLDS). Our review covered the VDOE's SLDS documentation from May 2014 through September 2015.

BACKGROUND

The Institute of Education Sciences administers the SLDS grant program and monitors grantees' progress toward meeting the final goals of their approved grant applications. The Institute of Education Sciences awarded VDOE two SLDS grants. In fiscal year 2007, it awarded VDOE \$6,054,395 to improve its Educational Information Management System (EIMS), a system that VDOE used to meet the data collection and reporting requirements of the No Child Left Behind Act of 2001. In fiscal year 2009, it awarded VDOE \$17,537,564 in American Recovery and Reinvestment Act (Recovery Act) funds, which allowed VDOE to further develop Virginia's SLDS.

The National Forum of Education Statistics¹ defines an SLDS as a data system that (1) collects and maintains detailed, high-quality, student- and staff-level data that are linked across entities and, over time, provide a complete academic and performance history for each student and

¹ The National Forum of Education Statistics is a component of the National Cooperative Education Statistics System that was established by the National Center for Education Statistics. The National Center for Education Statistics is a component of the Institute of Education Sciences.

(2) makes these data accessible through reporting and analysis tools.² According to this definition, and for the purposes of this audit, we determined that Virginia's SLDS consists of a system to query data from other State systems—the Virginia Longitudinal Data System (VLDS)—and other State systems that contain the data, which include the Single Sign-on Web System (SSWS) that contains K-12 data, including personally identifiable information, and other systems containing postsecondary, employment, and other types of data. For our audit of Virginia's SLDS, our review was limited to the VLDS and the SSWS.

VDOE's 2009 Institute of Education Sciences approved grant application stated that VDOE would create a longitudinal data linking and reporting system with the ability to link data among State agency data sources, including the K-12 system. To accomplish this objective, the application explained that state agencies would continue to house source data in their respective database but additional capabilities were going to be developed to store query results, scrub and prepare the data for linking, and offer and receive data in the desired format. The VLDS query system obtains data from the exposure databases from five State agencies: the VDOE, the State Council of Higher Education for Virginia, the Virginia Community College System, the Virginia Employment Commission, and the Virginia Department of Social Services. Each participating State agency maintains its original data in its system, such as the VDOE's SSWS for K-12 data. Each State agency creates an exposure database that contains the data fields approved by that agency, and that data is used when a VLDS query is run. The VLDS receives data from each State agency's exposure database via a one-way transmission. Before the transmission of data to the VLDS, a one-way hashing algorithm is performed to remove personally identifiable information and create a unique identifier for each individual. Then, when a researcher query is run in the VLDS, a second hashing algorithm removes that unique identifier, and creates a VLDS unique identifier. Consequently, no personally identifiable information resides in the VLDS.

VDOE used grant funds to develop the VLDS to support critical reporting on the quality of Virginia education. The VLDS was activated November 2013. The VLDS is not a centralized database; it is a query system that allows researchers to obtain longitudinal data on students from State agencies to help improve the quality of education in Virginia. VDOE runs the query for the researchers based on the requested data in the application; the results of the query are available to the researchers for 10 days then the results are deleted.

According to VDOE's Director of VLDS, grant funds were used to develop the SSWS exposure database, which was used to provide K-12 data for VLDS queries. Personally identifiable information resides in the SSWS. We reviewed VDOE's SSWS to determine whether it has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in the SSWS. The SSWS is a system through which school division personnel access many of VDOE's data collection processes and other applications. The SSWS is intended to provide a simple, secure, and reliable environment for access to different types of educational information that VDOE's school division manages. The SSWS allows school division personnel to access its data collection processes, as well as other applications, with one single user ID and password through the internet. Security and access to

² The Education Science Reform Act of 2002, Title 2, Section 208 of the "Grant Program for Statewide Longitudinal Data Systems" authorizes the U.S. Department of Education to award grants that enable State agencies to design, develop, and implement Statewide longitudinal data systems to efficiently and accurately manage, analyze, disaggregate, and use individual student data.

data are maintained at the user level, so school division personnel have access only to the information and applications they need.

Although we did not develop a finding on the VLDS since it did not contain personally identifiable information, we reviewed the Information Technology Security Audit of the VLDS. The independent audit was performed by Impact Maker in May 2014, and identified several control weaknesses in the VLDS. We also reviewed the System Security Plan for the VLDS and determined that VDOE still had not implemented five of the required system controls discussed in the information technology security audit. We identified weaknesses that pose a heightened risk to the data that resides on the VLDS. We list the controls VDOE had not implemented for VLDS in Attachment 2.

AUDIT RESULTS

Our audit objective was to determine if VDOE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in Virginia's SLDS. During our audit, we learned that the VLDS does not contain personally identifiable information. However, the SSWS contains personally identifiable information; therefore, our audit focused on the SSWS portion of the SLDS.

We identified internal control weaknesses in the SSWS that increase the risk that VDOE will be unable to prevent or detect unauthorized access and disclosure of personally identifiable information. Specifically, we found that although VDOE classified the SSWS as a sensitive system, it did not ensure that it met the minimum requirements for a system classified as sensitive, as required in Virginia's Information Technology Resource Management (ITRM) Standards. Because VDOE did not meet the minimum State requirements for systems classified as sensitive, VDOE also was not in compliance with the Institute of Education Sciences SLDS grant requirements.

We determined VDOE has policies and procedures that address reporting and responding to unauthorized access and disclosure of data, including personally identifiable information in its data systems. However, we could not determine whether the procedures were effectively implemented since VDOE has not reported any system breaches in the VLDS or SSWS.

In its comments to the draft report, VDOE stated that our finding was inconsistent with the stated purpose of the audit with regard to a focus on the SSWS. Therefore, VDOE requested all findings related to the SSWS be removed from the report. VDOE stated that it had reclassified the VLDS system as non-sensitive and reasonably concluded the audit was rescinded. In addition, VDOE also provided a list of factual inaccuracies it contends were in the draft report. We include the full text of VDOE's comments on the draft report as Attachment 3 to the report.

We were not requested by VDOE to rescind the audit and we disagree there is any rational basis under *Government Auditing Standards* to rescind the audit or remove the finding on SSWS. We also did not remove references to the VLDS as VDOE acknowledges we explained on an October 1, 2015 conference call because it was classified as a sensitive system through the end of our audit period. We did make changes to the report for clarity as a result of VDOE's response.

Because the objective of our audit was to review the protection of personally identifiable information in Virginia's SLDS, and because the SSWS portion of Virginia's State Longitudinal Data System contained the personally identifiable information, we included the SSWS in our audit scope. Based on the statutory definition of an SLDS, the Virginia State Longitudinal Data System consists of both the query system and the exposure databases provided by the state agencies. Subsequent to our exit conference on September 24, 2015, OIG received an e-mail on October 8, 2015, from the newly appointed Chief Data Security Officer stating that the VLDS was reclassified as a non-sensitive system. While this was after our audit period and not relevant to the audit results, VDOE did not provide documentation to support the reclassification of the VLDS. We also refuted VDOE's claims on inaccuracies in our draft report contained in Attachment 4 to the report.

FINDING NO. 1 – The Single Sign-On Web System Does Not Meet Required State Minimum Security Requirements

We found that VDOE did not ensure that the SSWS met required State standards for systems classified as sensitive. Virginia's ITRM Standards establish the required system controls for Virginia systems that are classified as sensitive. Based on the 2007 SLDS Request for Grant Applications, the grantee must ensure confidentiality of students in accordance with relevant legislation. In addition, VDOE's 2009 approved Recovery Act application stated that VDOE would implement security controls in accordance with Virginia's Information Security Standards. According to the ITRM Standards, VDOE must ensure that applicable systems meet all of the requirements found in the standards. We determined the SSWS did not meet State minimum security requirements. Therefore, VDOE had weaknesses in its system controls designed to prevent and detect unauthorized access and disclosure of personally identifiable information in the SSWS.

We found that VDOE did not ensure the SSWS met the minimum requirements found in Virginia's ITRM Standards, which consists of 17 system controls. We reviewed the information technology security audit of the SSWS performed by Impact Makers, dated May 2014. The objective of that audit was to determine compliance with Virginia's ITRM Standards. In addition we reviewed, Virginia's Auditor of Public Accounts' June 2014 Department of Education Audit that found "matters involving internal control and its operation necessary to bring to management's attention," and other related documents. The Impact Makers audit report cited issues with all 17 system control areas identified in Virginia's ITRM Standards. For example, VDOE had not updated its risk assessment, did not address vulnerabilities the auditors identified through a vulnerability scan, and did not ensure that the SSWS password policy met the minimum State requirements. VDOE created one corrective action plan that addressed both the May 2014 SSWS security audit and the June 2014 Virginia Auditor of Public Accounts audit. We evaluated VDOE's corrective action plan for the SSWS security audit and the System

Security Plan for the SSWS. The corrective action plan identified the issues to be remedied, planned corrective action, and the status of each finding. The Auditor of Public Accounts corrective action plan also documented whether VDOE concurred with the findings and the due date to remedy the findings. VDOE did not implement the corrective actions to remedy 17 missing system controls. See Table 1 below for the 17 missing system controls.

Table 1. SSWS Security Audit

<u>Control Area</u>	<u>ITRM 501-08 Sections</u>	<u>Control</u>
Access Control	AC-2	Required system access controls to be documented and describes account management principles.
Configuration Management	CM-2 and CM-8	Required baseline configuration and component inventory be documented.
Awareness and Training	AT-1	Required role-based security training.
Audit and Accountability	AU-1	Required that Audit and Accountability polices be documented.
Security Assessment and Authorization	CA-3 and CA-7	Required that a continuous monitoring program be established.
Contingency Planning	CP-1-COV-1 and CP-1-COV-2	Required that based on the Business Impact Analysis and the Risk Assessment the Information Technology Disaster components develop a Disaster Recovery planning activity.
Identification and Authentication	IA-4 and IA-5	Required that user’s identifiers should be disabled (locked) after 90 days of inactivity and Information Technology systems enforce a minimum lifetime password restriction of 24 hours.
Incident Response	IR-2	Required Incident Response Training, which includes incident response controls.
Controlled Maintenance	MA-2	Required the performance and documentation of maintenance and repair of Information System Components.
Media Protection	MP-1	Required the protection of media systems.
Physical and Environmental Protection	PE-1	Required that the list of the physical and environmental controls be reviewed.
Planning	PL-2 and PL-2-COV	Required that the System Security Plan be documented.
Personnel Security	PS-7	Required that the Personnel Security Policy be documented.
Risk Assessment	RA-3	Required that risk assessments be conducted.

<u>Control Area</u>	<u>ITRM 501-08 Sections</u>	<u>Control</u>
System and Services Acquisition	SA-1, SA-3, and SA-3-COV-2	Required that the system design documentation be documented to include the coding practices.
System and Communications Protections	SC-1	Required polices for system and communication protection.
System and Information Integrity	SI-1	Required the documentation of security requirements and integrity-based controls.

While the System Security Plan identified seven security findings, it did not provide any remedies. The System Security Plan was also undated, unsigned, and not approved by a VDOE official, so we were unable to determine when VDOE developed the plan or its effective date. Therefore, VDOE did not take corrective action to address security control weaknesses to ensure the protection of personally identifiable information in the SSWS. During the exit conference with VDOE officials in September 2015, the director of Virginia’s VLDS stated that VDOE hired a Chief Data Security Officer on August 10, 2015, who was working on updating the System Security Plan for the SSWS.

Subsequently, the Auditor of Public Accounts audited the VDOE and identified additional missing system controls from the ITRM Standards. Virginia’s Auditor of Public Accounts reported five system control areas in the SSWS that did not meet the minimum standards identified in the Virginia ITRM Standards. The five missing system controls are listed in Table 2.

Table 2. Auditor of Public Accounts 2014 Audit

<u>Control Area</u>	<u>ITRM 501-08 Sections</u>	<u>Control</u>
Contingency Planning	CP-9 and CP-9-COV	Required that an agency document backup and restoration plans to meet agency requirements.
Configuration Management	CM-3 and CM-6	Required that an agency (1) retains and reviews a record of each configuration controlled change to a system and (2) documents mandatory configuration requirements consistent with system hardening standards.
Risk Assessment	RA-5	Required that an agency scan each sensitive system for vulnerabilities at least once every 90 days.
Information Security Roles and Responsibilities	Section 2.4.1	Required that the Information Security Officer report directly to the agency head.

<u>Control Area</u>	<u>ITRM 501-08 Sections</u>	<u>Control</u>
Information Technology System and Data Sensitivity Classification	Section 4.2.3	Required that an agency (1) identifies the sensitivity level of a system or data on the basis of low, medium, or high; and (2) determines potential damages as a result of a compromise of sensitive data.

The Auditor of Public Accounts reported that VDOE had not adequately documented some of the system control processes and found no evidence that the system controls were adequate. For example, for the Information Technology System and Data Sensitivity Classification system control area, VDOE did not scan all sensitive systems for vulnerabilities. Based on our review of the corrective action plan, the System Security Plan, and VDOE’s policies and procedures, VDOE has not adequately addressed the findings to ensure that the system controls meet the minimum State standards.

State and Federal Requirements for Protection of Personally Identifiable Information

According to the 2007 SLDS Request for Grant Applications, the grantee must ensure confidentiality of students in accordance with relevant legislation. In addition, VDOE’s 2009 approved Recovery Act application stated that VDOE would implement security controls in accordance with Virginia’s Information Security Standards. Virginia’s ITRM Standards require VDOE to ensure it has appropriate system controls for its sensitive data systems. Since both the VLDS and the SSWS were classified as sensitive systems for our audit period, VDOE must ensure these systems meet ITRM Standards.

Based on our review of the security audits, related policies and procedures, and corrective action plan for the SSWS, we concluded that VDOE had weak system controls to prevent and detect unauthorized access and disclosure of information in the SSWS. In April 2015, we were provided with the corrective action plan dated March 2015, for the May 2014 and June 2014 audits of the SSWS. During the exit conference, which was held in September 2015, VDOE stated it updates its corrective action plan quarterly and was working on updating the System Security Plan for the SSWS. We requested the updates to the corrective action plan and the System Security Plan; however, VDOE did not provide us with any updated documentation to support these assertions.

Due to the system control weaknesses, the SSWS is at an increased risk of a breach. The SSWS contains personally identifiable information, and there is a heightened risk that personally identifiable information is not adequately protected. Therefore, VDOE must ensure it has met the required State minimum security requirements. By not implementing the proper system controls, VDOE was not in compliance with its SLDS grant requirements covering system security.

Recommendations

We recommend that the Director of Institute of Education Sciences work with VDOE to—

- 1.1 Implement the system controls identified in the ITRM Standards to ensure the prevention and detection of unauthorized access and disclosure of information in the SSWS.

1.2 Take appropriate action to determine whether a breach has occurred in the SSWS and if breaches are identified, report and respond to the breaches in accordance with VDOE's policy and procedures.

1.3 Address all outstanding recommendations related to the security and Auditor of Public Accounts audits, and require SSWS to meet minimum State security standards.

VDOE Comments

In its response to the draft report, VDOE requested all findings related to the SSWS be removed from the report. VDOE stated that the scope of the audit was extended beyond the stated purpose to include VDOE's SSWS application portal (exposure database), which is not part of the SLDS and was not developed using SLDS funds.

VDOE identified the VLDS as its SLDS in its response to the draft report. VDOE provided the Office of Inspector General (OIG) with an email stating that VDOE had reclassified the VLDS from sensitive to non-sensitive on October 8, 2015. VDOE stated that it did not receive any additional communication until the draft report was issued and, as a result, reasonably concluded that the audit had been rescinded as the VLDS was not classified as a sensitive system.

VDOE also stated that the OIG incorrectly concluded that its SLDS consists of the VLDS and other State systems that contain personally identifiable information, including the SSWS. It stated that the VLDS and the SSWS are separate and distinct systems.

In addition, VDOE included a list of factual inaccuracies it believes were contained in the draft report. For example, VDOE stated that there have been no reported breaches in the VLDS and the breaches discussed in the "Objective, Scope, and Methodology" section were not related to VDOE. Also, VDOE stated that it used state funds not Federal grant funds to develop the SSWS.

VDOE also expressed concern with certain information contained in the draft report. The full text of VDOE's comments on the draft report is included as Attachment 3 of the report.

OIG Response

We agree that the VLDS and SSWS are distinct systems, but they comprise (along with other State systems) the larger SLDS. The description in our report of how the systems are connected was paraphrased from the Websites of the VLDS and the VDOE, and the VLDS Exposure Database Guidelines. Therefore, we did not remove the finding, but did make changes to the report for clarity as a result of VDOE's response.

The 2009 Institute of Education Sciences approved grant application stated that VDOE would create a longitudinal data linking and reporting system with the ability to link data among State agency data sources. To accomplish this objective, the approved application explained that state agencies would continue to house source data in their respective database but that additional capabilities were going to be developed to store query results, scrub and prepare the data for linking, and offer and receive data in the desired format. Therefore, VDOE had to create an exposure database for the SSWS that contained K-12 data, including personally identifiable information. The SSWS is used when a VLDS query is run. In addition, the Director of the VLDS stated in an interview that the VLDS went into production in November 2013 and that the 2009 grant funds were used to establish the SSWS exposure database.

Because the SSWS provides data to the VLDS via the exposure database, we determined that the scope of our audit encompassed whether VDOE protected the personally identifiable information in the SSWS. We informed the Director of VLDS in March 2015, that our audit work would include the SSWS and performed audit work on the SSWS because that is where the personally identifiable information is located for K-12 data. Therefore, we reviewed the security audits of the system controls for the SSWS to determine whether VDOE had internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information, the stated objective of the audit.

At the time of our site visit, VLDS was classified as a sensitive system, therefore, we included the weaknesses identified in the VLDS's system security plan as background and not as a finding in our audit report because it did not contain personally identifiable information. Subsequent to our exit conference, OIG received an e-mail on October 8, 2015, from VDOE stating that the VLDS was reclassified from a sensitive to a non-sensitive system and removed from the VDOE IT Security Plan. No supporting documentation was sent in that e-mail or in response to our draft audit report.

VDOE stated that the report was inconsistent with the stated purpose of the audit, and incorrectly included the SSWS as part of its SLDS. For the purpose of the audit, and in consideration of the statutory definition of an SLDS³, we determined that Virginia's SLDS is a system to query data from other State systems—the VLDS—and other State systems that contain the data, which include the SSWS exposure database that contains K-12 data, including personally identifiable information, and other systems containing postsecondary, employment, and other types of data. Therefore, we included the SSWS in the scope of our audit since that system contains the personally identifiable information of K-12 student data.

Lastly, OIG disagrees that the audit report contained factual inaccuracies. Attachment 4 of this report provides our response to the remaining claims of factual inaccuracies pointed out by VDOE that we have not already addressed.

³ The Education Science Reform Act of 2002, Title 2, Section 208 of the "Grant Program for Statewide Longitudinal Data Systems" authorizes the U.S. Department of Education to award grants that enable State agencies to design, develop, and implement Statewide longitudinal data systems to efficiently and accurately manage, analyze, disaggregate, and use individual student data.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if VDOE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in Virginia's SLDS. During our audit, we learned that the VLDS does not contain personally identifiable information. However, the SSWS contains personally identifiable information; therefore, our audit focused on the SSWS portion of the SLDS. Our review covered the VDOE's SLDS documentation from May 2014 through September 2015.

To accomplish our objective, we performed the following procedures. We reviewed:

- Virginia's organizational chart and interviewed officials from the VDOE.
- VDOE's security and system documents including:
 - Information Technology Security Policy;
 - Identification and Authentication Policy;
 - Personnel Security Policy;
 - Security Assessment and Authorization Policy;
 - Logical Access Control Policy;
 - Exposure Database Guidelines;
 - System and Communication Encryption Policy;
 - System and Information Integrity Policy;
 - System and Communication Protection Policy;
 - System and Services Acquisition Policy; and
 - the SSWS User Guide.
- Impact Makers reports, "Information Technology Security Audit of Virginia Longitudinal System," dated May 2014 and "Information Technology Security Audit of Single Sign-on Web Systems," dated May 2014 and the related corrective action plan.
- Virginia Auditor of Public Accounts' 2014 Department of Education Audit and the related corrective action plan.
- The VLDS and SSWS System Security Plans for evidence of the resolution of audit findings.
- VDOE's approved SLDS grant applications for 2007 and the Recovery Act.
- The Institute of Education Sciences' annual and final performance reports for Virginia's SLDS grants.

Virginia is one of three States we selected for a series of planned audits to assess how States' Longitudinal Data Systems protect personally identifiable information. We judgmentally selected the three States based on the following characteristics: total amount of SLDS funding, status and extent of grant program participation, and the State's number of reported education system data breaches. The data breaches included any education system breaches that the Identity Theft Resource Center reported. The breaches did not specifically identify the VLDS

and the SSWS. The Identity Theft Resource Center is a nonprofit organization that serves as a national resource on consumer issues related to cyber security, data breaches, social media, fraud, scams, and other issues. We selected Virginia because it received more than \$5 million in SLDS funding, had two SLDS grants that were closed, and the Identity Theft Resource Center reported that Virginia had more than three breaches in educational systems⁴. In addition, we selected Virginia because the Institute of Education Sciences stated that Virginia was a model State for protecting personally identifiable information in their SLDS.

We conducted a site visit at VDOE's office in Richmond, Virginia, during the week of March 23, 2015. We held an exit conference with VDOE on September 24, 2015, to discuss the results of the audit. We also had a follow-up discussion with VDOE on October 1, 2015.

We assessed the internal controls concerning the protection of personally identifiable information in the VLDS and the SSWS. We assessed VDOE's system control activities through inquiries of Virginia personnel; review of written policies, procedures, and documentation; and an analysis of prior audit reports and follow-up on the recommendations included in those reports. Because it did not relate to our audit objective, we did not obtain any data from the VLDS or the SSWS, so we did not assess the reliability of data in those systems. We identified weaknesses in the auditee's SSWS internal controls, which we fully discuss in the audit findings.

The internal controls pertinent to our audit objective were also reviewed by other auditors. Our report, as it relates to VDOE's controls to protect personally identifiable information in the SSWS, was based, in part, on the reports of other auditors. Based on our review of the auditors' qualifications and the audit reports, we determined that the auditors were independent of VDOE and the scope of the work performed was sufficiently reliable as it related to our audit objective.

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.

ADMINISTRATIVE MATTERS

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

⁴ The Identity Theft Resource Center did not identify breaches related to the VLDS.

If you have any additional comments or information that you believe may have a bearing on the resolution of this audit, you should send them directly to the following Department of Education official, who will consider them before taking final Departmental action on this audit:

Ruth Neild
Deputy Director of Policy and Research
Institute of Education Sciences
U.S. Department of Education
555 New Jersey Ave, NW
Room 500e
Washington, DC 20208-5500

It is the policy of the U. S. Department of Education to expedite the resolution of audits by initiating timely action on the findings and recommendations contained therein. Therefore, receipt of your comments within 30 calendar days would be appreciated.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

Sincerely,

/s/

Daniel Schultz
Regional Inspector General for Audit

Attachments

**Attachment 1: Acronyms, Abbreviations, and Short Forms
Used in This Report**

EIMS	Educational Information Management System
ITRM Standards	Virginia's Information Technology Resource Management Standards SEC501-08
OIG	Office of Inspector General
Recovery Act	American Recovery and Reinvestment Act
SLDS	Statewide Longitudinal Data System
SSWS	Single Sign-on Web System
VDOE	Virginia Department of Education
VITA	Virginia Information Technologies Agency
Virginia	Commonwealth of Virginia
VLDS	Virginia Longitudinal Data System

Attachment 2: Minimum Information Technology Resource Management Standards Not Met by VDOE for the VLDS

Table 3. Missing Required System Controls for VLDS

<u>Control Areas</u>	<u>ITRM 501-08 Sections</u>	<u>Control</u>
Risk Assessment	Section 6.2 and RA-5	VDOE did not ensure a risk assessment was performed at least every 3 years and did not ensure a vulnerability scan was performed at least every 90 days.
System and Communication Protection	SC-28	The data stored in the VLDS was not encrypted while sitting idle.
Access Control	AC-7	VDOE did not limit the number of invalid access attempts to an account in the VLDS.
Identification and Authentication	IA-4 and IA-5	VDOE did not ensure passwords were refreshed every 90 days and did not disable accounts after 90 days of inactivity. VDOE did not ensure that the VLDS passwords had a minimum and maximum lifetime, and were not limited to a reuse of 24 generations.
Security Assessment and Authorization	CA-3	VDOE did not document the VLDS' connections to other information systems.

Attachment 3: VDOE's Comments on the Draft Report



COMMONWEALTH of VIRGINIA

Steven R. Staples, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION
P.O. BOX 2120
Richmond, Virginia 23218-2120

Office: (804) 225-2023
Fax: (804) 371-2099

April 11, 2016

Mr. Daniel Schultz
U.S. Department of Education
Office of Inspector General
Regional Inspector General for Audit
32 Old Slip - 26th Floor
New York, New York 10005

Dear Mr. Schultz:

The Virginia Department of Education (VDOE) is in receipt of the draft audit report, "Protection of Personally Identifiable Information in the Commonwealth of Virginia's Longitudinal Data System," Control Number ED-OIG/A02P0006. The U.S. Department of Education's Office of Inspector General (US DOE-OIG) review covered the VDOE's SLDS documentation from May 2014 through September 2015. The VDOE thanks the US DOE-OIG for the opportunity to comment on the findings, recommendations and other information contained in the draft audit report. Note: The SLDS will hereinafter be referenced as the VLDS (Virginia Longitudinal Data System).

The VDOE's last communication to the US DOE-OIG prior to receiving the OIG draft audit report Control Number ED-OIG/A02P0006 was an e-mail to Tracie Goff-Smith, Auditor on October 8, 2015, in which the VDOE provided evidence that the VLDS had been reclassified from a sensitive to a non-sensitive system. In the e-mail, the VDOE asked if the US DOE-OIG required any further information. The VDOE did not receive any further communications until receipt of the draft audit report approximately six months later. Reasonably, the VDOE had concluded that the audit was rescinded as the VLDS was not classified as a sensitive system.

Notwithstanding, the VDOE finds the report to be inconsistent with the stated purpose of the audit:

"to determine if the Virginia Department of Education (VDOE) has internal controls in place to prevent, detect, report, and respond to unauthorized access and

Mr. Daniel Schultz
Page 2
April 11, 2016

disclosure of personally identifiable information in the Commonwealth of Virginia's (Virginia) Statewide Longitudinal Data System (SLDS)."

Specifically, the scope was extended to include the VDOE's Single Sign-on for Web System (SSWS) application portal which is not part of the SLDS and was not developed with the Federal LDS grant or other federal funds. The VDOE respectfully requests that all findings related to the SSWS be removed from the report. The draft audit report also states:

"no personally identifiable information resides in the VLDS."

Furthermore, the VDOE contends that the US DOE-OIG incorrectly concluded that Virginia's SLDS consists of the VLDS and other state systems that contain PII data, including the VDOE's Single Sign-on for Web System (SSWS). The US DOE-OIG draft audit report Control Number ED-OIG/A02P0006 states:

"The VLDS query system obtains data from the exposure databases from five State agencies: the VDOE, the State Council of Higher Education for Virginia, the Virginia Community College System, the Virginia Employment Commission, and the Virginia Department of Social Services. Each participating State agency maintains its original data in its system, such as the VDOE's SSWS for K-12 data. Each State agency creates an exposure database that contains the data fields approved by that agency, and that data is used when a VLDS query is run. The VLDS receives data from each State agency's exposure database via a one-way transmission. Prior to the transmission of data, a one way hashing algorithm is performed to remove personally identifiable information and create a unique identifier for each individual prior to transmission to the VLDS. Then, when a researcher query is run in the VLDS, a second hashing algorithm removes that unique identifier, and creates a VLDS unique identifier. Consequently, no personally identifiable information resides in the VLDS."

The VLDS and the SSWS are separate and distinct systems.

The VDOE would like to address various factual inaccuracies in the report as follows:

- The Educational Information Management System (EIMS) was state-funded, not federal grant-funded.
- The EIMS was not developed to meet the data collection and reporting requirements of the No Child Left Behind Act of 2001.
- The EIMS was not a predecessor to the SSWS, it was a separate system developed after the SSWS.
- The EIMS has been retired and is no longer in production.

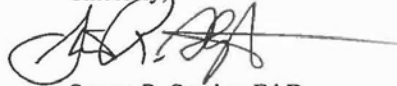
Mr. Daniel Schultz
Page 3
April 11, 2016

- The data collection and reporting requirements of the No Child Left Behind Act of 2001 were completed by 2003, well before the VDOE received the SLDS grant.
- The fiscal year 2009 grant was not used to make improvements to the EIMS.
- The SSWS predates the EIMS by a number of years.
- The SSWS is not populated with data from the EIMS.
- The SSWS was developed using state funds, not federal grant funds.
- The VDOE has not reported any system breaches in the VLDS because there have not been any.
- The data breaches referenced in footnote #4 of the audit report are not related to the VDOE and should be removed from the audit report.
- The VLDS went into production in August of 2014, not November.
- The VLDS is not classified as a sensitive system.

Again, the VDOE finds the report and its scope to be inconsistent with the stated purpose of the audit, a point that the VDOE emphasized on an October 1, 2015, conference call with the US DOE-OIG. In a March 2016 conversation, Mr. Schultz expressed that the US DOE-OIG draft audit report Control Number ED-OIG/A02P0006 is a "point in time" audit, meaning that the US DOE-OIG is focusing on the system classification at the time of the entrance conference, which is no longer relevant as the system is non-sensitive, also a point that the VDOE asserted on the October 1, 2015, conference call. The VDOE respectfully requests that all findings regarding the SSWS be removed from the report and recognize that the VLDS is a non-sensitive system by removing the Required System Controls from the report. The VDOE also requests the removal of any references to data breaches since the breaches listed in the report were not related to the VDOE, and which were acknowledged in the report as not being specific to the VLDS or the SSWS.

Again, thank you for the opportunity to provide comments in response to the draft audit report.

Sincerely,



Steven R. Staples, Ed.D.
Superintendent of Public Instruction

SRS/bvg

Attachment 4: OIG Response to VDOE’s claim of Factual Inaccuracies

Table 4. OIG Response

Inaccuracies According to VDOE	OIG Response
<p>The EIMS was state-funded, not federal grant-funded.</p>	<p>Based on information we were provided by VDOE we determined that SLDS funds were used for the EIMS. As stated in the report the 2007 SLDS grant funds were used to improve the EIMS. VDOE’s 2007 Institute of Education Sciences approved grant application states that “VDOE proposes to add two products from Triand Incorporated, easyCONNECT and easySTUDENT to the existing decision support tools provided by the EIMS program.”</p>
<p>The EIMS was not developed to meet the data collection and reporting requirements of the No Child Left Behind Act of 2001.</p> <p>The data collection and reporting requirements of the No Child Left Behind Act of 2001 were completed by 2003, well before VDOE received the SLDS grant.</p>	<p>We reviewed VDOE’s 2007 Institute of Education Sciences approved grant application, which states: “[t]he VDOE is entering the fourth year of development of its Student Information Program; the core of the program is the EIMS. The EIMS is Virginia’s solution to meeting the data collection and reporting requirements of the No Child Left Behind Act of 2001, leveraging the data requirements to provide rich decision support tools to Virginia school district personnel.”</p>
<p>The EIMS was not a predecessor to the SSWS, it was a separate system developed after the SSWS.</p> <p>The SSWS predates the EIMS by a number of years.</p> <p>The SSWS is not populated with data from the EIMS.</p>	<p>OIG was informed by the Director of the VLDS, in March 2015 that the EIMS was a predecessor system to the SSWS, and the SSWS was populated with data from the EIMS. However, for the final report we have deleted the footnote that contained the information.</p>
<p>The EIMS has been retired and is no longer in production.</p>	<p>We agree that the EIMS is retired. As stated in the draft report, the EIMS ceased operation on July 1, 2014, when the vendor’s contract expired.</p>

<p>The fiscal year 2009 grant was not used to make improvements to the EIMS.</p>	<p>We obtained a document dated May 2, 2013 from VDOE’s website, which states: “[t]he development of VLDS was funded through a Longitudinal Data Systems Grant awarded to Virginia under the American Recovery and Reinvestment Act of 2009. The federal grant allowed the commonwealth to build on VDOE’s state-funded EIMS and put additional high quality data into the hands of teachers, administrators, researchers, policymakers and the public — while safeguarding the privacy of students and adults.”</p>
<p>The VDOE has not reported any system breaches in the VLDS because there have not been any.</p> <p>The data breaches referenced in footnote #4 of the audit report are not related to VDOE and should be removed from the audit report.</p>	<p>We did not state that data breaches reported by the Identity Theft Resource Center impacted the VLDS or SSWS. We further clarified in the final audit report the information obtained from the Identity Theft Resource Center was only used to help the OIG select states to be audited and was not of VLDS.</p>