UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES
New York/Dallas Audit Region

September 27, 2016

Control Number
ED-OIG/A02P0007

Dr. Salam Noor
Deputy Superintendent of Public Instruction
Oregon Department of Education
255 Capitol St. NE
Salem, OR 97310

Dear Dr. Noor:

This final audit report, "Protection of Personally Identifiable Information in Oregon's Statewide Longitudinal Data System," presents the results of our audit. The purpose of the audit was to determine whether the Oregon Department of Education (ODE) has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in its Statewide Longitudinal Data System (SLDS). Our review covered ODE's internal controls from June 2015 through January 2016.

BACKGROUND

The Institute of Education Sciences administers the SLDS grant program and monitors grantee progress toward meeting the final goals of their approved grant applications. The grant program supports the design, development, and implementation of statewide longitudinal data systems. These systems are intended to enhance the ability of States to efficiently and accurately manage, analyze, and use education data and facilitate analysis and research to improve student academic achievement.

The Institute of Education Sciences awarded three SLDS grants to ODE. In fiscal year 2007, ODE was awarded $4,705,977 for a project referred to as the Direct Access to Achievement project. The purpose of this project was to improve data quality by training teachers and other users how to use data maintained in ODE's SLDS to improve student performance. In fiscal year 2009, ODE was awarded $3,696,615 for a project referred to as the Oregon Formative Assessment Resources project. This project funded curriculum developed at the University of Oregon to train new teachers on how to use data more effectively. ODE also used the project funding to relocate server equipment to the University of Oregon and to implement the Easy

Curriculum Based Measurements[1] formative assessments system. Also in fiscal year 2009, ODE was awarded $10,475,997 in American Recovery and Reinvestment Act funds for a project referred to as the Advancing Longitudinal Data for Educational Reform project. ODE used this project funding to (1) train users to improve data quality, (2) create a link between data on students and teachers, (3) create an early learning/prekindergarten data system, and (4) create an identity resolution system that could link student achievement data with achievement data from higher education and workforce data.

ODE's Director of Enterprise Systems stated that ODE did not have an SLDS during the time of our audit. However, we determined that ODE did have an SLDS system in place during our audit period that ODE applied SLDS grant funds to enhance. The National Forum of Education Statistics[2] defines an SLDS as a data system that collects and maintains detailed, high-quality, student and staff level data that are linked across entities and over time, providing a complete academic and performance history for each student and that makes these data accessible through reporting and analysis tools.[3] According to this definition, and for the purpose of this audit, we determined that ODE's Consolidated Collection System (CCS), its existing kindergarten through twelfth grade State database system, was Oregon's SLDS.

In June 2011, at the request of Oregon's Governor, the Oregon Education Investment Board was created to provide an integrated, statewide, student-based data system that monitors expenditures and outcomes to determine the return on statewide education investments. ODE's Support Service Director stated that in July 2015, ODE transferred control over continued development of an early childhood through postsecondary education SLDS to the Oregon Education Investment Board.[4] The CCS will remain with ODE and house kindergarten through twelfth grade student data and transmit data to the SLDS. ODE's Support Service Director stated that ODE was unaware of when the Oregon Education Investment Board would complete Oregon's early childhood through postsecondary education SLDS.

ODE developed its CCS in the 2003–2004 school year, before receiving its first SLDS grant in 2007. SLDS grant funds were used to provide professional development to enhance CCS stakeholders' use of data and create a link between data on students and teachers within CCS. The CCS contains 81 data stores that contain personally identifiable information and comprise different categories of student data such as math performance, reading performance, graduation rates, and discipline incidents. District staff use the central login on ODE's Web site to access the CCS and enter or view data. The district staff receives login access to the ODE District Web site and permissions to district data from the district security administrator, whom the district superintendent appoints. The district security administrator can provide district staff with the ability to view all data records for the entire district or specific school or can disable an account,

[1] Easy Curriculum Based Measurements is a data warehouse system that allows districts to control exchange of student demographic information and State assessment scores.

[2] 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.

[3] The Education Sciences 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.

[4] The Oregon Education Investment Board was renamed the "Chief Education Office" in July 2015.

preventing a user from accessing district data. In addition, the district security administrator can give users access to read, insert, update, and delete data. According to ODE's District Security Administrator User Guide, district security administrators are to give the least permission assignments needed for each person to do his or her job. Activities within the system are tied to individual users. District security administrators are required to ensure that staff who have been granted access to the central login have a signed permission form and confidentiality agreement on file.

The ODE research office uses information from the 81 data stores to perform research projects. ODE also allows external researchers, such as university staff, to perform research projects with the data from the CCS. Each external requester must fill out a standard external research form, which has two parts: (1) a description of the project and the type of data being requested and (2) data handling and security requirements. ODE's Data Governance Committee approves or denies research requests. External requesters must also sign a confidentiality agreement stating that the researcher cannot disclose personally identifiable information for any purpose other than those stated in the request. The ODE research office assembles the data and sends it to the external requester using a secure file transfer. The assistant superintendent for research and data analysis stated the system uses secure student identification numbers to link students across data sets and time. While the research agreement states an external requester may receive personally identifiable information, the assistant superintendent for research and data analysis stated ODE does not give out specific information such as Social Security numbers, names, and addresses when responding to research requests.

AUDIT RESULTS

Our audit objective was to determine whether ODE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in its SLDS. To answer our objective, we reviewed ODE's CCS, a kindergarten through twelfth grade SLDS containing students' personally identifiable information that ODE enhanced with SLDS grant funds.

We identified a lack of documented internal controls in the CCS that increases the risk that ODE will be unable to prevent or detect unauthorized access and disclosure of personally identifiable information. Specifically, we found that ODE did not ensure that the CCS met the minimum requirements in Oregon's Department of Administrative Services (DAS) State Standards, which require the system controls and documentation of those controls. Since ODE did not meet the minimum State requirements, ODE was not in compliance with the Institute of Education Sciences SLDS grant requirements.

In addition, ODE has policies and procedures that address reporting and responding to unauthorized access and disclosure of personally identifiable information in its data system. However, we could not determine whether the procedures were effective because ODE has not reported any system breaches in the CCS.

In its comments to the draft report, ODE stated that since the audit was conducted, the Office of Information Technology had a change of leadership and that it had identified additional information that was not previously provided at the time of the audit. ODE did not concur with the finding that the CCS did not meet minimum State system security requirements. ODE stated that an Information Security Plan was implemented in December 2010 and incorporated into its 2010 Information Security Policy. In addition, ODE stated its Internal Auditor conducted annual risk assessments every year except 2015. Lastly, ODE stated that it handles data stored in the CCS as level 3 in accordance with its Information Asset Classification policy. We reviewed the additional information and determined that ODE did not provide sufficient evidence to support that it implemented an Information Security Plan, conducted annual risk assessments, and classified security levels of the CCS as level 3. See Attachment 3 for OIG's response to each of the documents ODE provided. Although ODE did not concur with the finding, it agreed with our recommendations and identified actions it has taken or plans to take to address them. We summarize ODE's comments and our response at the end of the finding and provide the full text of ODE's comments in Attachment 2. We did not make any changes to the finding based on ODE's comments.

FINDING NO. 1 – The Consolidated Collection System Did Not Meet Minimum State System Security Requirements

We found that ODE did not ensure that the CCS met the minimum system security requirements in DAS State Standards. ODE did not develop and implement an Information Security Plan, conduct annual risk assessments, and classify the security levels of the CCS as required by DAS standards. The Information Security Plan is the foundation of information security and identifies the appropriate security controls over agency data systems. Also, as part of an Information Security Plan, ODE was required to conduct an annual risk assessment and classify the security levels of system assets. Annual risk assessments are a critical control designed to identify, quantify, and prioritize risks against criteria established by ODE for risk acceptance and objectives. The results determine appropriate actions and priorities for managing information security risks and for designing and implementing controls that protect information assets. Information asset classification is critical to ensure that information assets have a level of protection corresponding to the sensitivity and value of the information asset. Because ODE did not design and implement these key controls, it had significant weaknesses in its system controls designed to prevent and detect unauthorized access and disclosure of personally identifiable information in the CCS.

ODE's Chief Information Security Officer stated that he is the only staff member at ODE who works on the security of the system and that ODE needs a full-time security person to ensure ODE meets all security requirements and policies. We determined that this staffing shortage is a contributing factor to ODE's control measures we noted. Before our audit, ODE had not developed and implemented an Information Security Plan as required by DAS. ODE's Chief Information Security Officer stated that he was aware of the deficient security measures but did not have the necessary staff to create an Information Security Plan. As a result of our audit, ODE created an Information Security Plan, signed January 20, 2016, that ODE's interim chief information officer provided to us. However, the Information Security Plan noted several controls were currently not in place and that ODE was developing plans to implement new controls throughout 2016. For example, controls currently not in place include implementing software to detect unauthorized access, documenting malware response procedures and training staff on them, and assigning security level classifications of information assets. Because these controls are not yet in place, ODE did not have software to monitor accounts for unusual activity and alert systems administrators or automatically mitigate potentially malicious behavior. ODE purchased this software in January 2016 and plans to implement it in 2016.

Because ODE has not performed an annual risk assessment, we could not be certain that the controls listed in ODE's January 20, 2016, Information Security Plan were appropriate. ODE did not conduct the required annual risk assessments nor did it classify the security levels of system assets as required by DAS. When asked about the required annual risk assessments, the Chief Information Security Officer stated that ODE had not conducted any risk assessments of the CCS. ODE's Support Service Director stated that ODE started a project plan to classify security levels of data in July 2012; however, ODE did not fund the plan because the projected cost was greater than anticipated.

According to the 2007 and 2009 SLDS requests for grant applications, grantees were required to ensure the confidentiality of students in accordance with relevant State legislation. In its fiscal year 2007 and 2009 SLDS grant applications, ODE stated it will ensure the confidentiality of student records by following Oregon Revised Statutes and Oregon Administrative Rules. Oregon Revised Statute 182.122 requires agencies to follow information security standards, policies, and procedures established by DAS. Based on the evidence above, we found that ODE not only failed to document and perform the minimum State system security controls to detect and prevent unauthorized access and disclosure of personally identifiable information in its SLDS, but also did not comply with State regulations as it assured it would do in its fiscal year 2007 and 2009 SLDS grant applications.[5]

According to DAS Policy 107-004-052, each agency must develop and implement an Information Security Plan, policies and procedures that protect its information assets from the time of creation through useful life and through proper disposal. Additionally, DAS Policy 107-004-050 states that each agency must identify and classify its information assets. Agencies must implement proper levels of protection to protect these assets relative to the classifications. Each information asset classification should have a set or range of controls, designed to provide the appropriate level of protection of the information proportionate with the value of the information in that classification. In addition, the DAS Information Security Plan for the State of Oregon, September 2009, requires each agency to conduct an annual risk assessment in accordance with the International Organization for Standardization 27001. After identifying risks, agencies must apply the appropriate controls to their information and information systems security.

By not previously developing and implementing an Information Security Plan, ODE did not ensure that it met the assurances provided in its SLDS grant applications that it would comply with DAS information security policies, standards, and processes. Until ODE fully implements its Information Security Plan, conducts an annual risk assessment, and classifies security levels of information assets, ODE will not be fully aware of the system vulnerabilities in its CCS and

[5] The Uniform Administrative Requirements in Title 2, Code of Federal Regulations, replaced Title 34, Code of Federal Regulations, for new and continuation awards that the Department issued on or after December 26, 2014, and also consolidated requirements contained in a number of Office of Management and Budget circulars. The Uniform Administrative Requirements are not applicable to our audit because our audit covered SLDS grants that were awarded before the effective date.

will continue to lack information that can guide it in determining controls it needs to protect information assets. As such, ODE is at an increased risk of a breach and may not be aware if breaches have occurred to its CCS, which could compromise the personally identifiable information of students in the State of Oregon.

Recommendations

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

1.1 Ensure the system controls identified in ODE's Information Security Plan are implemented to detect and prevent unauthorized access and disclosure of personally identifiable information in its CCS.

1.2 Conduct annual risk assessments and classify security levels of data in the CCS, and ensure the CCS meets minimum State security standards.

1.3 Take appropriate action to determine whether a breach occurred in the CCS, and if breaches are identified, report and respond to the breaches in accordance with ODE's policy and procedures.

ODE Comments

ODE did not concur with our finding and stated that it had identified additional information that was not previously provided during our audit. However, ODE agreed with the recommendations and stated that they were entirely reasonable and representative of good security practices.

ODE stated that its first Information Security Plan was implemented in December 2010 in accordance with DAS requirements. It stated that ODE incorporated the required elements of a DAS Information Security Plan into its 2010 Information Security Policy. ODE stated that the controls identified as currently not in place in its Information Security Plan, dated January 20, 2016, are designed to close gaps in existing controls. ODE asserted that activities identified in the plan for the first half of 2016 have been completed and that the remaining activities are scheduled to be completed by the end of 2016. In addition, ODE stated DAS did not, in their information security plan guidance, require that agencies conduct a risk assessment prior to writing a security plan.

ODE stated that DAS required that agencies include in their Information Security Plan a way to conduct an annual risk assessment and it is included in its 2010 Information Security Policy. ODE stated that its Internal Auditor has conducted annual independent risk assessments every year except 2015. ODE provided its Internal Audit Charter policy to demonstrate that the Internal Auditor may conduct risk assessments. Also, ODE stated that it hired Microsoft in 2011–2012 to conduct a risk assessment of the SQL environment in which the CCS is built and maintained. ODE provided an executive summary, dated May 2011, of the risk assessment performed. In addition, ODE provided a list of audits and risk assessments to be completed in 2016.

ODE also stated that it handled data in the CCS in accordance with ODE Policy 581-309, Information Asset Classification. ODE stated that the policy specifies the classification level of data for student information, including data stored in the CCS, as level 3. ODE stated that all ODE databases containing student information are handled in accordance with level 3 requirements. ODE claimed that it classified data based on the type of data, and it identified and implemented handling standards based on the classification level. To support the classification of data in the CCS, ODE provided its Information Asset Classification policy and a project plan summary.

Lastly, ODE stated that information security staffing has increased since November 2015 from one full-time employee to 3.75 full-time employees. The full text of ODE's comments on the draft report is included as Attachment 2 of the report.

OIG Response

We reviewed the additional information that ODE provided and determined that the documentation was insufficient to support ODE's contention that it had implemented an Information Security Plan, conducted required risk assessments, and identified and properly classified information assets. Despite multiple requests for documentation throughout our audit as well as at an exit briefing where we confirmed our findings with ODE officials, no ODE official had claimed that an Information Security Plan was created and implemented, annual risk assessments were performed, or information asset classification had been properly conducted. In ODE's response to our draft report it is now claiming to have complied with DAS standards, but only provided policies with no evidence that these activities had been carried out. Therefore, we did not make any changes to the finding based on ODE's comments.

Specifically, we disagree that ODE's 2010 Information Security Policy qualifies as an Information Security Plan in accordance with DAS standards. While ODE stated in its response that its first Information Security Plan was implemented in 2010, the Chief Information Security Officer informed us during our audit that ODE did not have an Information Security Plan. We had previously been provided ODE's policy, and it lacks many components of an Information Security Plan. For example, DAS standards stated that an Information Security Plan should include, among other things, safeguards to detect, prevent, and respond to attacks or system failures, to identify reasonably foreseeable internal and external risks, and to assess the risks in network and software design. ODE's 2010 Information Security Policy did not contain these fundamental safeguards, among others.

While ODE had policies for conducting risk assessments, it did not provide any documentation that any of the required annual risk assessments for 2014 and prior years were conducted. While ODE stated in its response that it conducted annual risk assessments with the exception of the 2015 year, the Chief Information Security Officer informed us during our audit that annual risk assessments had not been performed. ODE provided policy documents on how risk assessments were to be conducted along with its response to our draft report, but produced no evidence that annual risk assessments were conducted.

Furthermore, ODE did not provide documentation to support its assertion that it had classified security levels of data in CCS. According to DAS Policy 107-004-050, Information Asset Classification, each agency will identify and classify its information assets. ODE provided the 2010 Information Asset Classification policy and a summary of an information asset classification project to support that information stored in the CCS is handled as level 3.

However, the policy and project summary was for information assets in general at ODE and was not specific to the CCS. ODE did not provide documentation that data in CCS was classified as level 3.

Attachment 3 provides a more detailed assessment of the additional documentation ODE provided in response to the draft report to support it had an Information Security Plan in place since 2010, conducted annual risk assessments, and classified security levels of the CCS as level 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine whether ODE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in its SLDS. Our review covered ODE's internal controls from June 2015 through January 2016.

To accomplish our objective, we interviewed officials from ODE and reviewed

- ODE's organizational charts,
- ODE SLDS approved grant applications,
- the Institute of Education Sciences' Final Performance Report Reviews for the Oregon 2007 and 2009 SLDS grants and the Annual Performance Report Review for the American Recovery and Reinvestment Act SLDS grant, and
- ODE's policies and procedures over information technology system security and breach response.

Oregon is one of three States we selected for a series of audits to assess how States' SLDS protect personally identifiable information. We judgmentally selected three States based on the following characteristics: (1) total amount of SLDS funding, (2) status and extent of grant program participation, and (3) 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 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. Breaches the Identity Theft Resource Center reported did not specifically identify the CCS. We selected Oregon because it received more than $5 million in SLDS funding, two of its three grants were closed, and it had three breaches related to educational systems.

We conducted a site visit at ODE's office in Salem, Oregon, during the week of June 9, 2015. We held an exit conference with ODE on January 6, 2016, to discuss the results of the audit.

We assessed the internal controls designed for the protection of personally identifiable information in the SLDS. We assessed ODE's system control activities through inquiries of Oregon personnel and review of written policies and procedures and documentation. We did not assess the reliability of data in the SLDS systems because the data did not relate to our audit objective. We identified a lack of documented internal controls, which we fully discuss in the audit findings.

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.

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 U.S. Department of Education official, who will consider them before taking final Departmental action on this audit:

Ruth Neild
Deputy Director of Policy and Research
Delegated Duties of the Director
Institute of Education Sciences
U.S. Department of Education
400 Maryland Avenue SW
Room 4109
Washington D.C. 20202

It is the policy of the U.S. Department of Education to expedite the resolution of audits by initiating timely action on the finding 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

CCS	Consolidated Collection System
DAS	Department of Administrative Services
ODE	Oregon Department of Education
SLDS	Statewide Longitudinal Data System

Attachment 2: ODE's Comments on the Draft Report

Oregon Department of Education
Kate Brown, Governor

Office of the Deputy Superintendent
255 Capitol St NE, Salem, OR 97310
Voice: 503-947-5600
Fax: 503-378-5156

July 8, 2016

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

Reference: Audit Control Number ED-OIG/A02P0007

Dear Mr. Schultz,

We've reviewed the draft audit report and have prepared comments on each of the findings and responses to each recommendation. In the time since the audit was conducted, the Office of Information Technology (OIT) at the Oregon Department of Education (ODE) has had a change in leadership. Susie Strangfield is now the Chief Information Officer and Amy McLaughlin is now the Director of IT Operations. After receiving the draft report, and with the institutional knowledge Amy McLaughlin brought to her new role, we've identified additional information that was not previously provided at the time of the initial audit.

OIG Audit Response

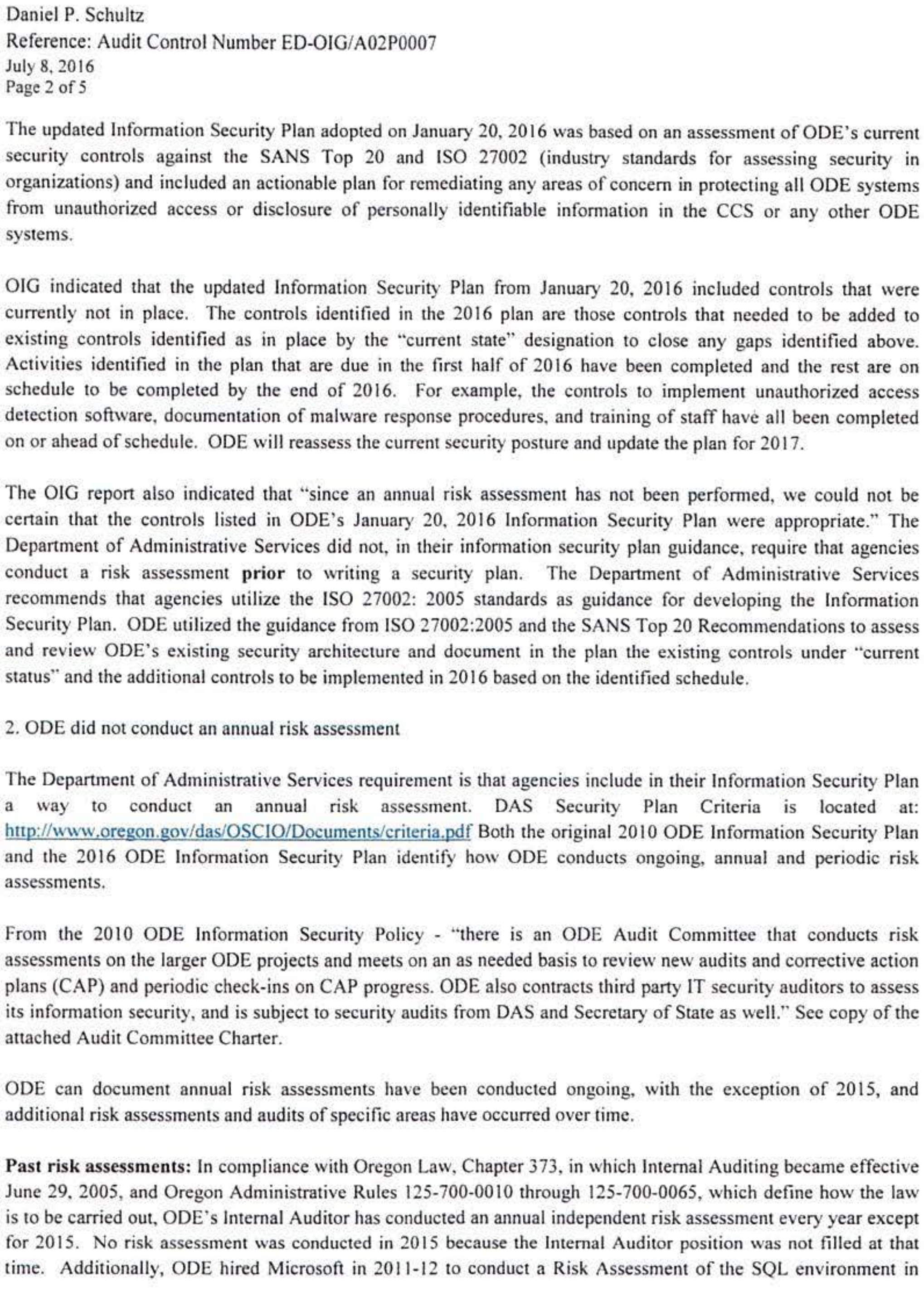
Finding No 1 - The Consolidate Collection System Did Not Meet Minimum State System Security Requirements

ODE does not concur with the finding that the Consolidated Collection System (CCS) did not meet minimum State system security requirements. Using the explanation OIG has provided to explain this finding, ODE has responded below to each point OIG provided to support this finding.

1. ODE did not develop and implement an Information Security Plan.

ODE clearly demonstrated existing and revised plans that met the Department of Administrative Services requirement for creating an Information Security Plan.

The ODE's first Information Security Plan was implemented in December 2010 in accordance with the DAS requirement at the time and developed using the DAS security plan template for guidance. The Information Security Plan was adopted and identified for action at ODE by incorporating it into ODE's policy structure and assigning it the name Policy 581-310 (Information Security Policy). Some of the confusion about this is due to the fact that ODE incorporated the required elements of a DAS "security plan" into the policy document 581-310.



The updated Information Security Plan adopted on January 20, 2016 was based on an assessment of ODE's current security controls against the SANS Top 20 and ISO 27002 (industry standards for assessing security in organizations) and included an actionable plan for remediating any areas of concern in protecting all ODE systems from unauthorized access or disclosure of personally identifiable information in the CCS or any other ODE systems.

OIG indicated that the updated Information Security Plan from January 20, 2016 included controls that were currently not in place. The controls identified in the 2016 plan are those controls that needed to be added to existing controls identified as in place by the "current state" designation to close any gaps identified above. Activities identified in the plan that are due in the first half of 2016 have been completed and the rest are on schedule to be completed by the end of 2016. For example, the controls to implement unauthorized access detection software, documentation of malware response procedures, and training of staff have all been completed on or ahead of schedule. ODE will reassess the current security posture and update the plan for 2017.

The OIG report also indicated that "since an annual risk assessment has not been performed, we could not be certain that the controls listed in ODE's January 20, 2016 Information Security Plan were appropriate." The Department of Administrative Services did not, in their information security plan guidance, require that agencies conduct a risk assessment **prior** to writing a security plan. The Department of Administrative Services recommends that agencies utilize the ISO 27002: 2005 standards as guidance for developing the Information Security Plan. ODE utilized the guidance from ISO 27002:2005 and the SANS Top 20 Recommendations to assess and review ODE's existing security architecture and document in the plan the existing controls under "current status" and the additional controls to be implemented in 2016 based on the identified schedule.

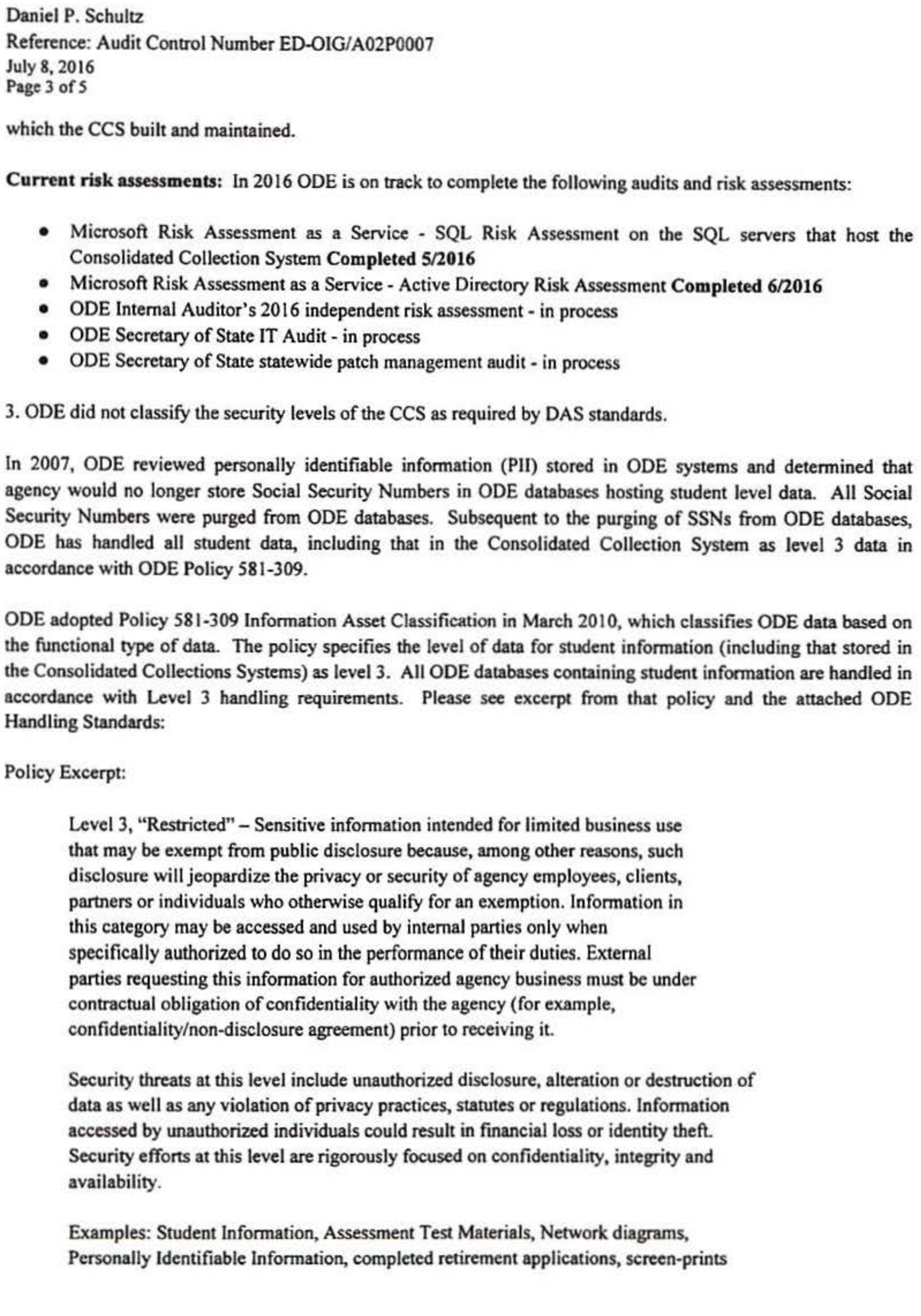
2. ODE did not conduct an annual risk assessment

The Department of Administrative Services requirement is that agencies include in their Information Security Plan a way to conduct an annual risk assessment. DAS Security Plan Criteria is located at: http://www.oregon.gov/das/OSCIO/Documents/criteria.pdf Both the original 2010 ODE Information Security Plan and the 2016 ODE Information Security Plan identify how ODE conducts ongoing, annual and periodic risk assessments.

From the 2010 ODE Information Security Policy - "there is an ODE Audit Committee that conducts risk assessments on the larger ODE projects and meets on an as needed basis to review new audits and corrective action plans (CAP) and periodic check-ins on CAP progress. ODE also contracts third party IT security auditors to assess its information security, and is subject to security audits from DAS and Secretary of State as well." See copy of the attached Audit Committee Charter.

ODE can document annual risk assessments have been conducted ongoing, with the exception of 2015, and additional risk assessments and audits of specific areas have occurred over time.

Past risk assessments: In compliance with Oregon Law, Chapter 373, in which Internal Auditing became effective June 29, 2005, and Oregon Administrative Rules 125-700-0010 through 125-700-0065, which define how the law is to be carried out, ODE's Internal Auditor has conducted an annual independent risk assessment every year except for 2015. No risk assessment was conducted in 2015 because the Internal Auditor position was not filled at that time. Additionally, ODE hired Microsoft in 2011-12 to conduct a Risk Assessment of the SQL environment in



which the CCS built and maintained.

Current risk assessments: In 2016 ODE is on track to complete the following audits and risk assessments:

- Microsoft Risk Assessment as a Service - SQL Risk Assessment on the SQL servers that host the Consolidated Collection System **Completed 5/2016**
- Microsoft Risk Assessment as a Service - Active Directory Risk Assessment **Completed 6/2016**
- ODE Internal Auditor's 2016 independent risk assessment - in process
- ODE Secretary of State IT Audit - in process
- ODE Secretary of State statewide patch management audit - in process

3. ODE did not classify the security levels of the CCS as required by DAS standards.

In 2007, ODE reviewed personally identifiable information (PII) stored in ODE systems and determined that agency would no longer store Social Security Numbers in ODE databases hosting student level data. All Social Security Numbers were purged from ODE databases. Subsequent to the purging of SSNs from ODE databases, ODE has handled all student data, including that in the Consolidated Collection System as level 3 data in accordance with ODE Policy 581-309.

ODE adopted Policy 581-309 Information Asset Classification in March 2010, which classifies ODE data based on the functional type of data. The policy specifies the level of data for student information (including that stored in the Consolidated Collections Systems) as level 3. All ODE databases containing student information are handled in accordance with Level 3 handling requirements. Please see excerpt from that policy and the attached ODE Handling Standards:

Policy Excerpt:

> Level 3, "Restricted" – Sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency (for example, confidentiality/non-disclosure agreement) prior to receiving it.
>
> Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as any violation of privacy practices, statutes or regulations. Information accessed by unauthorized individuals could result in financial loss or identity theft. Security efforts at this level are rigorously focused on confidentiality, integrity and availability.
>
> Examples: Student Information, Assessment Test Materials, Network diagrams, Personally Identifiable Information, completed retirement applications, screen-prints

> containing SSN and name, employee and retiree address, telephone and other nonfinancial membership records and employee financial records maintained by ODE, disability information, security audit reports, and other information exempt from public records disclosure.

ODE has classified data based on the type of data and identified and implemented handling standards. Since the CCS contains student information and other related PII it is handled and protected as a Level 3 asset.

4. The audit identified inadequate staffing as an issue for maintaining the information security program at ODE. At the time of the audit, the security unit was understaffed due to staffing and organizational changes. Staffing of information security has increased since November 2015 from 1 FTE to 3.75 FTE.

Recommendations:

While ODE did not concur with the findings of the audit for the reasons noted above, the recommendations of the audit are entirely reasonable and representative of good security practices. ODE concurs with the recommendations and has identified what actions ODE is taking that align with the recommendations provided.

Recommendation 1.1 Ensure the system controls identified in ODE's Information Security Plan are implemented to detect and prevent unauthorized access and disclosure of personally identifiable information of personally identifiable information in its CCS.

ODE Response: ODE agrees with this recommendation. ODE has already implemented, on schedule all the controls identified in the 2016 plan that are scheduled to be completed by July 1, 2016 and is continuing to implement other identified controls on schedule. In addition to existing controls, the following controls from the 2016 Information Security Plan have been fully implemented:

- Varonis monitors and detects unauthorized access - implementation completed 4/2016
- Websense internet filtering upgrade to block known signatures for security risks implementation completed 5/2016
- Antivirus installation on specific servers implementation completed 1/2016

Recommendation 1.2 Conduct annual risk assessments and classify security levels of data in the CCS, and ensure the CCS meets minimum State security standards.

ODE Response: ODE agrees with this recommendation. As noted in the response to the findings, ODE has conducted an annual risk assessment every year except 2015 and ODE has already conducted three risk assessments in 2016. ODE also currently classifies all student data as level 3 data and protects it as such as noted in the response to the findings, however, ODE will conduct a more granular review of the data elements in the CCS and classify them more specifically. ODE will continue to protect the CCS based on the highest level of classification of the data within the system. In accordance with the ODE Information Security plan and ODE policies, ODE will continue to ensure that CCS meets the minimum State security standards.

Recommendation 1.3 Take appropriate action to determine whether a breach occurred in the CCS, and if breaches are identified, report and respond to the breaches in accordance with ODE's policy and procedures.

ODE Response: ODE concurs. ODE continuously maintains its network, servers and systems with current security patching and monitoring tools, and the Office of Information Technology monitors networks and systems for security breaches and responds to alerts that may indicate a potential breach. ODE is continuing to expand our capability in monitoring and responding to security threats. Staffing for security has increased to 3.75 FTE in the last eight months.

If there are any additional questions or concerns with ODE's responses, please contact Susie Strangfield or Amy McLaughlin. Their contact information is below.

Susie Strangfield
Chief Information Officer
503-947-5705
susie.strangfield@state.or.us

Amy McLaughlin
Director of IT Operations
503-947-5771
amy.mclaughlin@state.or.us

Respectfully,

Salam A. Noor, Ph.D.
Deputy Superintendent of Public Instruction

Attachment 3: Analysis of ODE's Supporting Documentation

ODE's Supporting Documentation	**OIG's Review of the Documentation**
2010 Information Security Policy	We found that ODE's 2010 Information Security Policy did not identify the specific controls ODE had implemented or planned to implement to mitigate risks over its information assets. In its response, ODE stated that the 2010 Information Security Policy was its Information Security Plan. However, during our fieldwork, the 2010 Information Security Policy, along with other ODE policies, was provided by ODE's Support Services Director as policy documentation. According to DAS Policy 107-004-052, Information Security, agency information security plans should include safeguards in which the agency: • Identifies reasonably foreseeable internal and external risks; • Assesses the sufficiency of safeguards in place to control the identified risks; • Assesses risks in network and software design; • Assesses risks in information processing, transmission and storage; • Detects, prevents and responds to attacks or system failures; and • Regularly tests and monitors the effectiveness of key controls, systems and procedures The 2010 Information Security Policy did not document ODE's assessment of risk, controls in place to mitigate risk, or the planned implementation of controls to mitigate risks. In addition, it did not document ODE's safeguards to detect, prevent and respond to system failures or monitor the effectiveness of key controls, systems and procedures.

Risk and Health Assessment Program for Microsoft SQL Server	The Risk and Health Assessment Program for Microsoft SQL Server was the only documentation of a prior risk assessment that ODE provided. The risk assessment did not identify whether it was specifically for ODE, and we would consider it to be only a fraction of an overall risk assessment. Further, the May 2011 risk assessment did not provide evidence that it followed the International Organization for Standardization 27001, as required by DAS standards for conducting annual risk assessments. For example, the following elements of the International Organization for Standardization 27001 are to be considered (1) identify assets and the associated information owners, (2) identify the threats to those assets, (3) identify the vulnerabilities that might be exploited by the threats, (4) determine whether the risks are acceptable, (5) apply appropriate controls, and (6) accept or avoid the risks. These steps were not demonstrated in the Risk and Health Assessment Program for Microsoft SQL Server provided by ODE.
Internal Audit Charter	ODE provided its Internal Audit Charter policy to demonstrate that the Internal Auditor may conduct risk assessments. While the policy states an Internal Auditor may conduct a risk assessment, no documentation of a risk assessment performed by the Internal Auditor was provided.
Information Asset Classification Policy	ODE provided the 2010 Information Asset Classification policy to support that information stored in the CCS is handled as level 3. The document states ODE’s policy providing descriptions and examples of the different asset classification levels, information asset protection, information owner responsibilities, labeling, handling, and disposal. However, the document provides only ODE’s policy and not the classification itself of ODE’s information assets, including the CCS.

Information Asset Classification Project	ODE provided a summary of an information asset classification project to support that information stored in the CCS is handled as level 3. The document stated that the purpose of the project was to develop and implement processes that continually allow for information on ODE's file server to be assessed, classified, and managed. However, the result of neither the project nor the classification itself of ODE's information assets, including the CCS, was provided.