UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES
New York/Dallas Audit Region

July 10, 2017

Control Number
ED-OIG/A06Q0001

Dr. Jennifer McCormick
Superintendent of Public Instruction
Indiana Department of Education
South Tower, Suite 600
115 West Washington Street
Indianapolis, IN 46204

Dear Dr. McCormick:

This final audit report, "Protection of Personally Identifiable Information in Indiana's Statewide Longitudinal Data System," presents the results of our audit. The purpose of the audit was to determine whether the Indiana Department of Education (IDOE) has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in Indiana's Statewide Longitudinal Data System (SLDS). Our review covered IDOE's internal controls from April 2016 through February 2017.

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 grant program supports the design, development, and implementation of SLDSs. These systems are intended to enhance the ability of States to efficiently and accurately manage, analyze, and use education data as well as facilitate analysis and research to improve student academic achievement.

The Institute of Education Sciences awarded two SLDS grants to IDOE. In fiscal year 2007, IDOE was awarded $5,188,260. IDOE used a portion of the grant funds to develop a data warehouse that it could use to transfer data to the Indiana Workforce Intelligence System. In fiscal year 2012, IDOE was awarded $3,965,160, which was used to develop Indiana's current SLDS, the Indiana Network of Knowledge (INK) system.

2007 SLDS Grant

IDOE's 2007 SLDS grant application stated that it planned to use the grant funds to build on and integrate its current data collection system to create a comprehensive P-20W SLDS.[1] The grant application further stated that this system would allow data integration between State agencies, which would give stakeholders the ability to track and analyze student achievement and attainment from early childhood through higher education and beyond. According to the grant application, IDOE planned to use a portion of the grant funds to expand on its internal data warehouse and create connections to educational and financial resources within IDOE. This data warehouse would then be able to provide data into the Indiana Workforce Intelligence System.

2012 SLDS Grant

In its 2012 SLDS grant application, IDOE stated that the Indiana Workforce Intelligence System would not be suitable as the SLDS for Indiana due to technological constraints, such as (1) intensive labor hours involved in manually matching data, (2) no commonly defined process across agencies to match data, and (3) concerns that the Indiana Workforce Intelligence System data warehouse could be compromised. For that reason, IDOE stated it was developing a new SLDS using the 2012 grant funds.

In 2014, the Indiana General Assembly established the INK system as the State's SLDS that contains educational and workforce information from educational institutions at all levels and information about the State's workforce (Indiana Code § 22-4.5-10 (2014)). The State created an INK Governance Committee to provide administrative oversight of the INK system, with the State Superintendent of Public Instruction, or a designee, being one of six members, and required the appointment of an Executive Director.[2] In February 2015, INK partner agencies, including IDOE, signed the "Indiana Network of Knowledge Data Sharing Agreement and Memorandum of Understanding," which adopted the INK Governance Framework as the data governance framework for the INK program. The INK Governance Framework outlines the roles and responsibilities of the participating Indiana agencies. The INK system receives data from IDOE, the Indiana Department of Workforce Development, the Indiana Commission for Higher Education, and the Family and Social Services Administration.

The National Center for Education Statistics describes two types of SLDSs—centralized and federated. In a centralized SLDS, all participating source systems copy their data into a central system that organizes, integrates, and stores the data. In a federated SLDS, individual source systems maintain control over their own data but agree to share some or all of this information with other participating systems on request. The INK system is a centralized system: Indiana agencies feed their data, which includes personally identifiable information, into the centralized INK system. IDOE uses the data warehouse built using 2007 SLDS grant funds to provide data to the INK system. The IDOE Chief Information Officer stated that the staging area of the INK

[1] The Institute of Education Sciences describes a P-20W SLDS data system as including early learning, kindergarten through 12th grade, postsecondary, and workforce data.

[2] In accordance with Indiana Code § 22-4.5-10-7 (2014), the INK Governance Committee comprises (1) the Indiana Department of Workforce Development Commissioner, (2) the Commissioner of the Commission for Higher Education, (3) the State Superintendent of Public Instruction, (4) one member representing private colleges and universities, (5) one member representing the business community in Indiana appointed by the Governor, and (6) the INK Executive Director.

system contains personally identifiable information that is removed when moved to the production area where reports can be generated.[3]

Indiana's Management and Performance Hub developed the INK system. The Management and Performance Hub is a subcomponent of the Indiana Office of Technology (IOT), which essentially functions as a consulting firm for State agencies. We defined the Management and Performance Hub as a service organization to IDOE for the development of the INK system because, according to the Government Accountability Office's *Standards for Internal Control in the Federal Government*, a service organization is an external party that performs operational processes for an entity. IDOE provided SLDS grant funds to the Management and Performance Hub to develop the INK system and was therefore responsible for oversight and monitoring of system development and implementation as both an SLDS grantee and a member of the INK Governance Committee. A chart illustrating the INK Governance Committee structure and how source system data flow to the INK system can be found in Attachment 2 to this report.

According to the Management and Performance Hub Executive Director, all of the deliverables for the INK system were completed as of July 2016. During our exit conference, Indiana officials stated that the INK system went into production in September 2016.

AUDIT RESULTS

Our audit objective was to determine whether IDOE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in Indiana's SLDS. To answer our objective, we reviewed the internal controls of the INK system, a P-20W SLDS that Indiana developed with SLDS grant funds and that contains students' personally identifiable information.

We found that IDOE did not provide adequate oversight of the Management and Performance Hub during the development of the INK system to ensure that the system met the minimum security requirements found in the Indiana Code and the IOT Information Security Framework. Specifically, we found that IDOE did not ensure that the INK system met the following requirements: had a System Security Plan (SSP), underwent a compliance audit and a risk assessment, and had its security level classified. Because IDOE did not ensure that the INK system met the minimum security requirements, IDOE was not in compliance with the Institute of Education Sciences' SLDS grant requirements. There is also no assurance that the INK system contains controls regarding the prevention and detection of unauthorized access and disclosure of information.

In addition, we found that IDOE did not ensure that its data warehouse, which feeds data to INK, met the minimum security requirements identified in the IOT Information Security Framework. Specifically, the IDOE Chief Information Officer stated that there were no written policies and

[3] The staging area of INK is where data from participating State agencies is placed, matched, and de-identified. The production area of INK is where the matched de-identified data from the staging area is kept for analysis, visualization, and reporting.

procedures for the protection of personally identifiable information in IDOE's data warehouse. IDOE did not begin to follow the requirements of the IOT Information Security Framework until December 2016; therefore, there is no assurance that IDOE's data warehouse has the required security controls and IDOE may be unaware of vulnerabilities in its data warehouse.

Because IOT was established in 2005 to be the information technology resource for the State's information technology programs, we reviewed IOT policies and procedures that addressed preventing, detecting, reporting, and responding to unauthorized access and disclosure of personally identifiable information in State data systems. The INK system was not available to the end users at the time of our audit. As such, we could not determine whether the procedures were effective. For IDOE's data warehouse, we could not determine whether procedures were effectively implemented, because IDOE did not have any written documentation to show the controls were implemented.

Subsequent to our audit fieldwork in Indiana, the INK Executive Director notified us that the INK system went live in September 2016. In addition, the Management and Performance Hub provided a document titled "Security Audit and Risk Assessment." We reviewed the assessment, which discussed servers whose names were redacted. The assessment did not identify the INK system or the server it resided on. The assessment identified nine findings and related recommendations. We were also provided the corrective action plan for the assessment, but it too did not refer to the INK system. Furthermore, the corrective action plan did not provide implementation dates for the corrective actions proposed. Based on the assessment, the reviewed servers had weaknesses that may result in IDOE's inability to effectively prevent, detect, report, and respond to breaches.

In its comments on the draft report, IDOE neither agreed nor disagreed with our findings. However, IDOE stated that it is strengthening controls around its own data warehouse and is committed to addressing the Office of Inspector General's (OIG) findings and recommendations regarding the INK system by June 30, 2018. We appreciate IDOE's commitment to correcting the deficiencies identified during the course of this audit, and acknowledge that some work has already begun. We strongly encourage it to prioritize implementation of corrective actions related to the protection of personally identifiable information given the significant risks associated with any weaknesses in controls in this area and to take more immediate action when possible. We summarize IDOE's comments at the end of each finding and include the full text of its comments as Attachment 3.

FINDING NO. 1 – The Indiana Network of Knowledge System Did Not Meet Minimum Security Requirements

We found that IDOE did not provide adequate oversight of the Management and Performance Hub during the development of the INK system to ensure that the system met the minimum security requirements found in the Indiana Code and the IOT Information Security Framework. IDOE's approved 2012 SLDS grant application stated that IDOE would implement security controls in accordance with applicable Federal and State privacy laws.[4]

[4] Effective December 2014, grantees are required to meet the requirements in the Office of Management and Budget's Uniform Guidance (Title 2 of the Code of Federal Regulations §200.303), regarding effective internal

Indiana Code § 22-4.5-10 (2014) establishes the INK system as the State's SLDS and includes specific requirements regarding the security and privacy of data in the system. The IOT Information Security Framework contains detailed policies and procedures that State agencies are required to implement to ensure appropriate system controls are in place for data systems in the State. Because IDOE did not ensure that the INK system met the minimum security requirements, IDOE was not in compliance with the Institute of Education Sciences' SLDS grant requirements and lacked assurance it could prevent and detect unauthorized access and disclosure of information in the INK system.

We found that IDOE did not ensure that an SSP was developed and that compliance audits would be completed for the INK system as required by Indiana Code § 22-4.5-10 (2014). In response to our request for a copy of the INK SSP, the INK Executive Director provided the INK Governance Framework. The INK Governance Framework indicates that a separate document would be developed to function as the SSP; specifically, it states that the INK Security Plan[5] will align with National Institute of Standards and Technology (NIST) 800-53R4, "Security and Privacy Controls for Federal Information Systems and Organizations," which requires an SSP for data systems.[6] Neither the INK Executive Director nor the IDOE Chief Information Officer provided the separate SSP referenced in the INK Governance Framework. Further, the Management and Performance Hub Executive Director stated that the SSP was the IOT Information Security Framework. We reviewed both the IOT Information Security Framework and the INK Governance Framework and determined that neither of these documents contained all of the necessary elements of an SSP as required by NIST 800-18R1, "Guide for Developing Security Plans for Federal Information Systems." For example, neither document met the NIST requirements of documenting the system's security controls and designating a system owner. A system owner is designated as the key point of contact for the system and is responsible for coordinating system development lifecycle activities.

As noted above, we also found that IDOE did not plan to perform regular audits for compliance on the INK system. According to Indiana Code, the SSP must include the performance of regular audits for compliance with data privacy and security standards. The INK Governance Framework states that such compliance audits should be conducted once every 3 calendar years. Initially, the IDOE Chief Information Officer stated that he had not planned to perform a compliance audit. Subsequently, the IDOE Chief Information Officer and the Management and Performance Hub Executive Director stated that they were in the process of planning to perform a compliance audit.

Lastly, we found that IDOE did not ensure that a risk assessment was completed before system implementation and that the security level of the INK system was classified as required by the IOT Information Security Framework. The IDOE Chief Information Officer stated that he was not aware of the requirement to perform a risk assessment of the INK system. The IDOE Chief

control over Federal awards. This guidance was not applicable to our audit because our audit covered SLDS grants that were awarded before the effective date. However, it does contain new requirements on internal control, specifically as it relates to grantees' responsibilities to meet the grant requirements, address outstanding audit findings for the grant, and ensure the continued protection of personally identifiable information.

[5] According to the INK Governance Framework, the INK Security Plan is the data security and safeguarding plan that is required by Indiana Code § 22-4.5-10 (2014).

[6] NIST is a Federal agency tasked with, among other things, developing standards and guidelines related to computers and information technology.

Information Officer and Management and Performance Hub Executive Director became aware of the risk assessment requirement through discussions with us during the course of our audit. According to the IOT Information Security Framework, State agencies are required to ensure that a risk assessment is conducted on each information system before implementation and then again annually. State agencies are also required to ensure that the security level of each information system is classified appropriately. The IDOE Chief Information Officer was unable to provide documentation that indicated that the security level of the INK system had been classified. The classification of an information system determines the level of security that must be in place to protect the data within that system. According to the IOT Information Security Framework, "[d]ata categorization… drives system designs and operations support methodologies to assure availability and protective requirements are attained."

According to IDOE's 2012 SLDS grant application, IDOE stated that it would ensure the confidentiality of student records by following all applicable Federal and State privacy laws. Based on the evidence above, we found that IDOE 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 law as it assured it would do in its 2012 SLDS grant application.

Indiana Code § 22-4.5-10-5 (2014) requires IDOE and other State agencies that collect data to ensure that there is a provision for a data security plan, including the performance of regular audits for compliance with data privacy and security standards. Indiana Code § 22-4.5-10-6 (2014) states that the administrative oversight of the INK system includes the development and implementation of a detailed data security and safeguarding plan. The IOT Information Security Framework provides policies and procedures for State agencies and contains the responsibilities of system owners to secure their systems. It also requires risk assessments to be performed on information systems before implementation and then annually, instructs agencies to conduct regular compliance audits on these systems, and directs agencies to classify their information.

IDOE did not monitor and oversee the services provided by the Management and Performance Hub during the development of the INK system. IDOE's responsibility as an SLDS grantee is to oversee and monitor system implementation in accordance with the grant requirements. In February 2015, IDOE signed the "Indiana Network of Knowledge Data Sharing Agreement and Memorandum of Understanding" with INK partner agencies agreeing that IOT would be responsible for developing and coordinating the INK system. The Government Accountability Office's *Standards for Internal Control in the Federal Government* states that

> management may engage external parties to perform certain operational processes …Management, however, retains responsibility for the performance of processes assigned to service organizations. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational process and how the service organization's internal control system impacts the entity's internal control system.

Because IDOE did not monitor the development of the INK system, IDOE did not ensure that the INK system met the minimum security requirements in the Indiana Code and the IOT Information Security Framework. IDOE also did not meet the assurances provided in its SLDS grant application that it would comply with Indiana Code and the requirements of the IOT Information Security Framework.

Until IDOE fully implements an SSP that requires the performance of compliance audits, conducts annual risk assessments, and classifies the security levels of information assets, IDOE will not be aware of any potential system vulnerabilities in the INK system and will continue to lack information that can guide it in determining the controls it needs to protect its information assets. As such, IDOE is at an increased risk of a breach and may not be aware if the INK system has been breached, which could compromise any personally identifiable information found in the system.

Recommendations

We recommend that the Commissioner of the National Center for Education Research who has been Delegated the Duties of the Institute of Education Sciences Director require IDOE to—

1.1 Ensure that the system controls identified in the Indiana Code and the IOT Information Security Framework are implemented to ensure the prevention and detection of unauthorized access and disclosure of personally identifiable information in the INK system.

1.2 Ensure that the INK system is in compliance with the terms of the approved SLDS grant and any approved grant extension requests.

1.3 Ensure proper oversight of any service organizations involved in the development of the INK system to ensure that appropriate policies and procedures are implemented over the system.

IDOE Comments

In its response to the draft report, IDOE neither agreed nor disagreed with our finding and recommendations. However, IDOE believes that it will completely address Finding 1 and its recommendations when it completes the work on its action plan. According to IDOE, the action plan it proposed will be completed by June 30, 2018. IDOE stated that it came under a new administration on January 9, 2017. This transition included a new Superintendent of Public Instruction, and the departure of the Chief Information Officer, and project manager for the SLDS grant. IDOE stated that it has been working with the U.S. Department of Education (Department) and the OIG since January 2017 to address the findings and finalize its work on the 2012 SLDS grant. This has included providing to OIG evidence of a recently completed INK system security audit, remediation plan, and a data classification document.

IDOE also stated that Indiana passed new legislation, the House Enrolled Act 1470, which repeals Indiana Code § 22-4.5-10 (2014) and will be effective July 1, 2017. IDOE stated this repeal does not mean that the INK system will go away, but that the transfer of INK to the Management and Performance Hub will be effective July 1, 2017. IDOE believes that with the removal of references to the INK system and to security measures from State law, it is IDOE's duty to ensure that the Management and Performance Hub is ensuring the appropriate security measures for the INK system based on relevant State and Federal laws.

Lastly, IDOE stated that it is working with the Department to extend the grant period to June 30, 2018, so that it can implement its action plan with respect to the INK system. IDOE stated that it will review both State and Federal laws and work with the Management and Performance Hub and IOT to ensure that the INK system conforms to State and Federal data protection and security requirements.

OIG Response

We understand that there was a change in administration at IDOE during the audit and the new administration provided us with a security audit, remediation plan, and the data classification document referenced in its response. The security audit we were provided did not include specific references to the INK system and the related remediation plan did not indicate when the findings would be corrected. We understand that some work has begun to correct those deficiencies; however, we strongly encourage IDOE to work with the Institute of Education Sciences to determine if the documents presented are sufficient to address our finding and recommendations.

During the audit, we identified Indiana Code § 22-4.5-10 (2014) as criteria relevant to our audit objective and requested that IDOE provide sufficient documentation to ensure the protection of personally identifiable information in its SLDS. We understand that House Enrolled Act 1470 repeals Indiana Code § 22-4.5-10 (2014) and becomes effective July 1, 2017. We also agree with IDOE that even though Indiana Code § 22-4.5-10 (2014) is no longer in effect, "it is the duty of the IDOE to ensure the Indiana Management and Performance Hub is ensuring the appropriate security for the INK system based on relevant state and federal laws."

Regarding the no-cost extension, although IDOE stated that it will be completing an action plan to address our findings by June 30, 2018, we again encourage it to take more immediate action whenever possible to provide for the security of the INK system.

FINDING NO. 2 – The IDOE Data Warehouse Did Not Meet Minimum Security Requirements

We found that IDOE did not ensure that the IDOE data warehouse, which was developed using funds from the 2007 SLDS grant, met the minimum security requirements identified in the IOT Information Security Framework. IDOE used part of its Institute of Education Sciences 2007 SLDS grant funds to build a data warehouse that provided data to the Indiana Workforce Intelligence System and provides data to the INK system. IDOE's goals in developing the data warehouse were to integrate its existing databases; build bridges between multiple levels of education; link educator, financial, and student progress data; and promote and facilitate research and evaluation.

IDOE could not provide documentation of its internal controls to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in its data warehouse. We requested any available documentation regarding the security of data maintained in IDOE's data warehouse. The IDOE Chief Information Officer stated that there were no written policies and procedures for the protection of personally identifiable information in IDOE's data warehouse. As such, there is no assurance that the IDOE data warehouse has the required security controls.

Based on the Institute of Education Sciences 2007 SLDS Request for Grant Applications, the grantee must ensure confidentiality of students' data in accordance with the Family Educational Rights and Privacy Act and relevant legislation. In its 2007 SLDS grant application, IDOE agreed that it would comply with this requirement. We identified the IOT Information Security Framework, in place since February 2006, as relevant legislation as it provides State agencies with policies and procedures to ensure appropriate system controls of State systems. However, the IDOE Chief Information Officer stated that IDOE did not follow the IOT Information Security Framework.

The IDOE data warehouse is not part of the INK system; however, it provides data to INK. We also noted that IDOE did not begin to follow the requirements of the IOT Information Security Framework until December 2016. Therefore, there is no assurance that IDOE's data warehouse has the required security controls, and IDOE may be unaware of vulnerabilities in its data warehouse. As such, IDOE is at an increased risk of a breach and may not be aware if its data warehouse has been breached, which could compromise any personally identifiable information found in the system.

Recommendation

We recommend that the Commissioner of the National Center for Education Research who has been Delegated the Duties of the Institute of Education Sciences Director require IDOE to—

2.1 Ensure that the system controls identified in the IOT Information Security Framework are implemented in IDOE's data warehouse to ensure the prevention, detection, reporting, and responding of unauthorized access and disclosure of personally identifiable information.

IDOE Comments

In response to the draft audit report, IDOE neither agreed nor disagreed with our finding and recommendation. However, IDOE believes that it will completely address Finding 2 and its recommendation when its action plan is completed by June 30, 2018. IDOE stated it is working with the Department to extend the current SLDS grant to June 30, 2018. IDOE will use the extension to review and document the security protocols for the IDOE data warehouse. IDOE stated that the documentation for the data warehouse would mirror the documentation for INK. IDOE plans to migrate all of IDOE data assets to IOT by mid to late summer of this year.

OIG Response

Although IDOE stated that it will be completing an action plan to address our findings by June 30, 2018, we again encourage it to take more immediate action whenever possible to provide for the security of the IDOE data warehouse.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine whether IDOE has internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in Indiana's SLDS. Our review covered IDOE's internal controls from April 2016 through February 2017.

To accomplish our objective, we interviewed officials at IDOE, the Indiana Department of Workforce Development, the Indiana Commission for Higher Education, IOT, the Management and Performance Hub, the INK Governance Committee, the Indiana State Board of Accounts, the Indiana Auditor of State Office, and the Institute of Education Sciences. Additionally, we reviewed:

- IDOE's organizational chart;
- Indiana SLDS 2007 and 2012 approved grant applications;
- the Institute of Education Sciences' Final Performance Review for Indiana's 2007 SLDS grant and the Annual Performance Reviews for Indiana's 2012 SLDS grant;
- the IOT Information Security Framework, which includes policies and procedures over information technology system security and breach response;
- the INK Governance Framework; and
- documents related to IDOE's extension request and the Institute of Education Sciences' approval.

Because the INK Governance Framework indicated that it would align with NIST standards, we compared both the INK Governance Framework and IOT Information Security Framework with the NIST SSP standards to determine whether they aligned with SSP requirements.

Indiana is one of three States that we selected for a series of audits to assess how States' SLDSs protect personally identifiable information. We judgmentally selected three States based on the following characteristics: (1) total amount of SLDS grant 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. We selected Indiana because it received more than $5 million in SLDS funding, one of its two grants was closed, and the Identity Theft Resource Center identified three breaches in Indiana's educational systems. Breaches the Identity Theft Resource Center reported did not specifically identify the Indiana Workforce Intelligence System or INK.

We conducted audit fieldwork from April 11, 2016, through September 15, 2016, at IDOE's office in Indianapolis, IN. We held an exit conference with Indiana State officials on February 14, 2017, 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 IDOE's system control activities through inquiries of Indiana personnel and review of written policies and procedures and documentation. We did not assess the reliability of data in the SLDS because the data did not relate to our audit objective. We identified a lack of internal controls, to include adequately monitoring a service organization, 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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:

Thomas W. Brock
Commissioner, National Center for Education Research
Delegated the Duties of the Institute of Education Sciences Director
U.S. Department of Education
550 12th Street, SW
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/

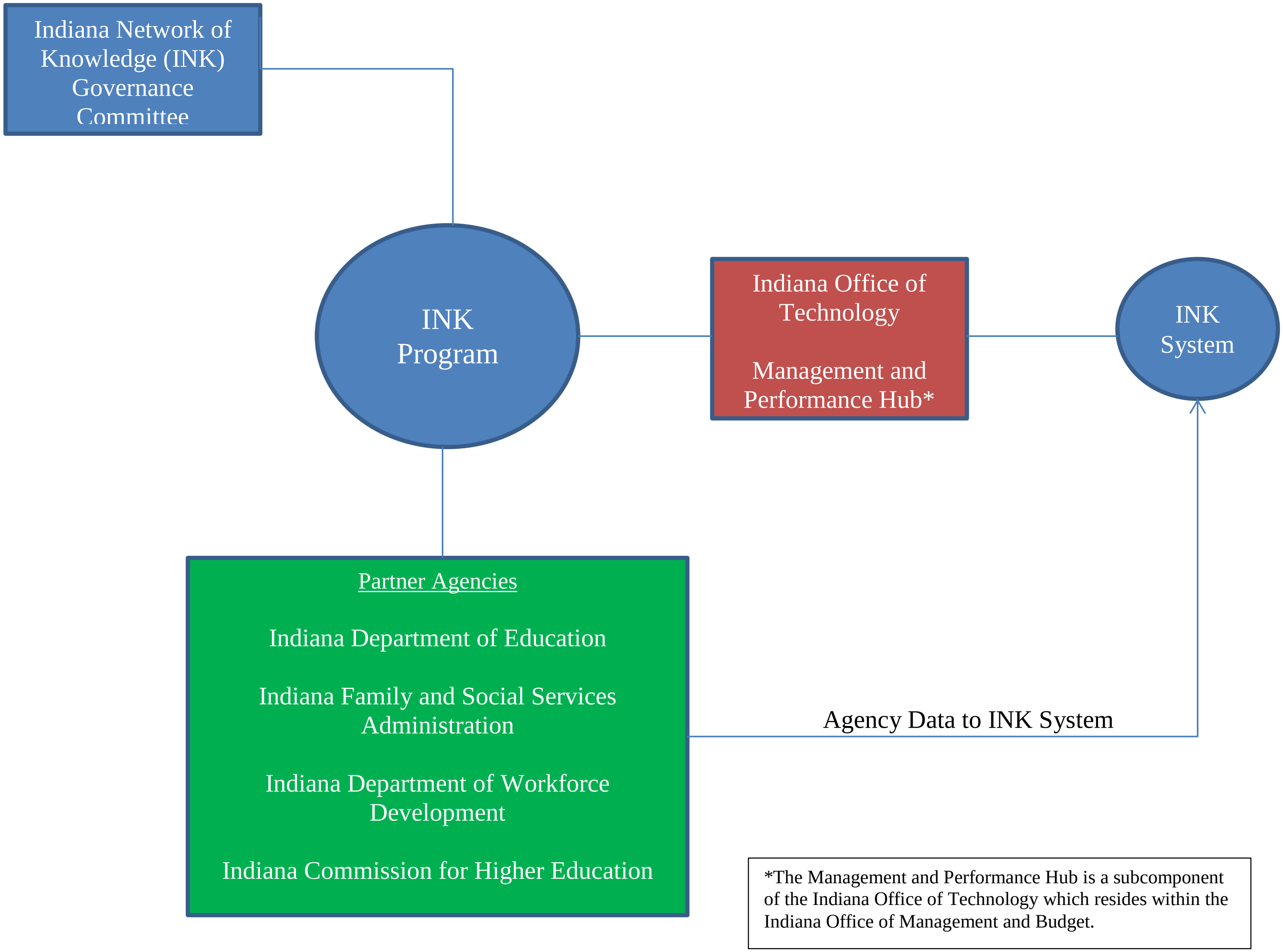
Daniel P. Schultz
Regional Inspector General for Audit

Attachments

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

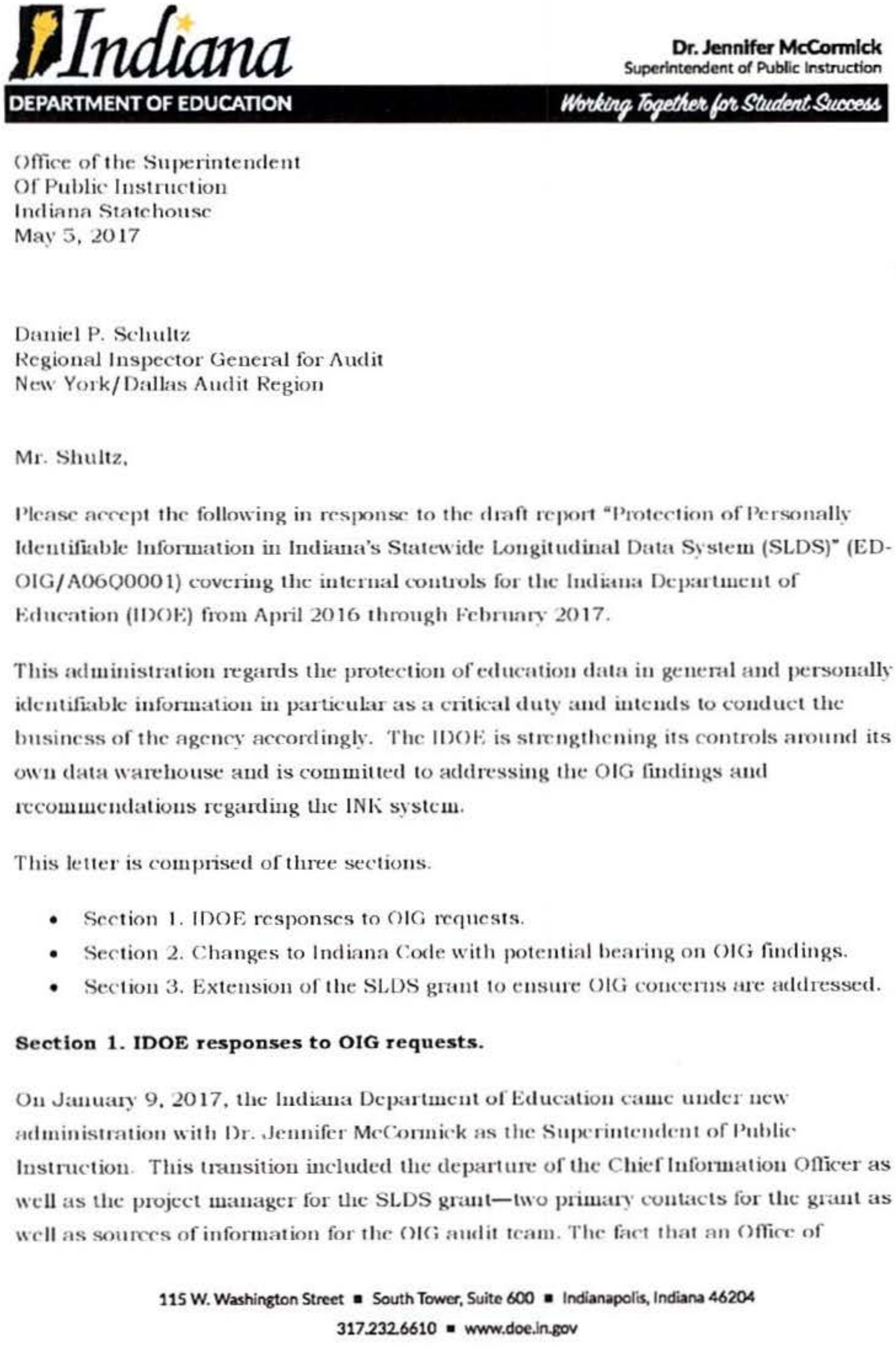
Department	U.S. Department of Education
IDOE	Indiana Department of Education
INK	Indiana Network of Knowledge
IOT	Indiana Office of Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SSP	System Security Plan
SLDS	Statewide Longitudinal Data System

Attachment 2: INK Process Flow


Indiana Network of Knowledge (INK) Governance Committee
INK Program
Indiana Office of Technology
Management and Performance Hub*
INK System
Partner Agencies
Indiana Department of Education
Indiana Family and Social Services Administration
Indiana Department of Workforce Development
Indiana Commission for Higher Education
Agency Data to INK System

*The Management and Performance Hub is a subcomponent of the Indiana Office of Technology which resides within the Indiana Office of Management and Budget.

Attachment 3: IDOE Comments on the Draft Report



Indiana
DEPARTMENT OF EDUCATION

Dr. Jennifer McCormick
Superintendent of Public Instruction
Working Together for Student Success

Office of the Superintendent
Of Public Instruction
Indiana Statehouse
May 5, 2017

Daniel P. Schultz
Regional Inspector General for Audit
New York/Dallas Audit Region

Mr. Shultz,

Please accept the following in response to the draft report "Protection of Personally Identifiable Information in Indiana's Statewide Longitudinal Data System (SLDS)" (ED-OIG/A06Q0001) covering the internal controls for the Indiana Department of Education (IDOE) from April 2016 through February 2017.

This administration regards the protection of education data in general and personally identifiable information in particular as a critical duty and intends to conduct the business of the agency accordingly. The IDOE is strengthening its controls around its own data warehouse and is committed to addressing the OIG findings and recommendations regarding the INK system.

This letter is comprised of three sections.

- Section 1. IDOE responses to OIG requests.
- Section 2. Changes to Indiana Code with potential bearing on OIG findings.
- Section 3. Extension of the SLDS grant to ensure OIG concerns are addressed.

Section 1. IDOE responses to OIG requests.

On January 9, 2017, the Indiana Department of Education came under new administration with Dr. Jennifer McCormick as the Superintendent of Public Instruction. This transition included the departure of the Chief Information Officer as well as the project manager for the SLDS grant—two primary contacts for the grant as well as sources of information for the OIG audit team. The fact that an Office of

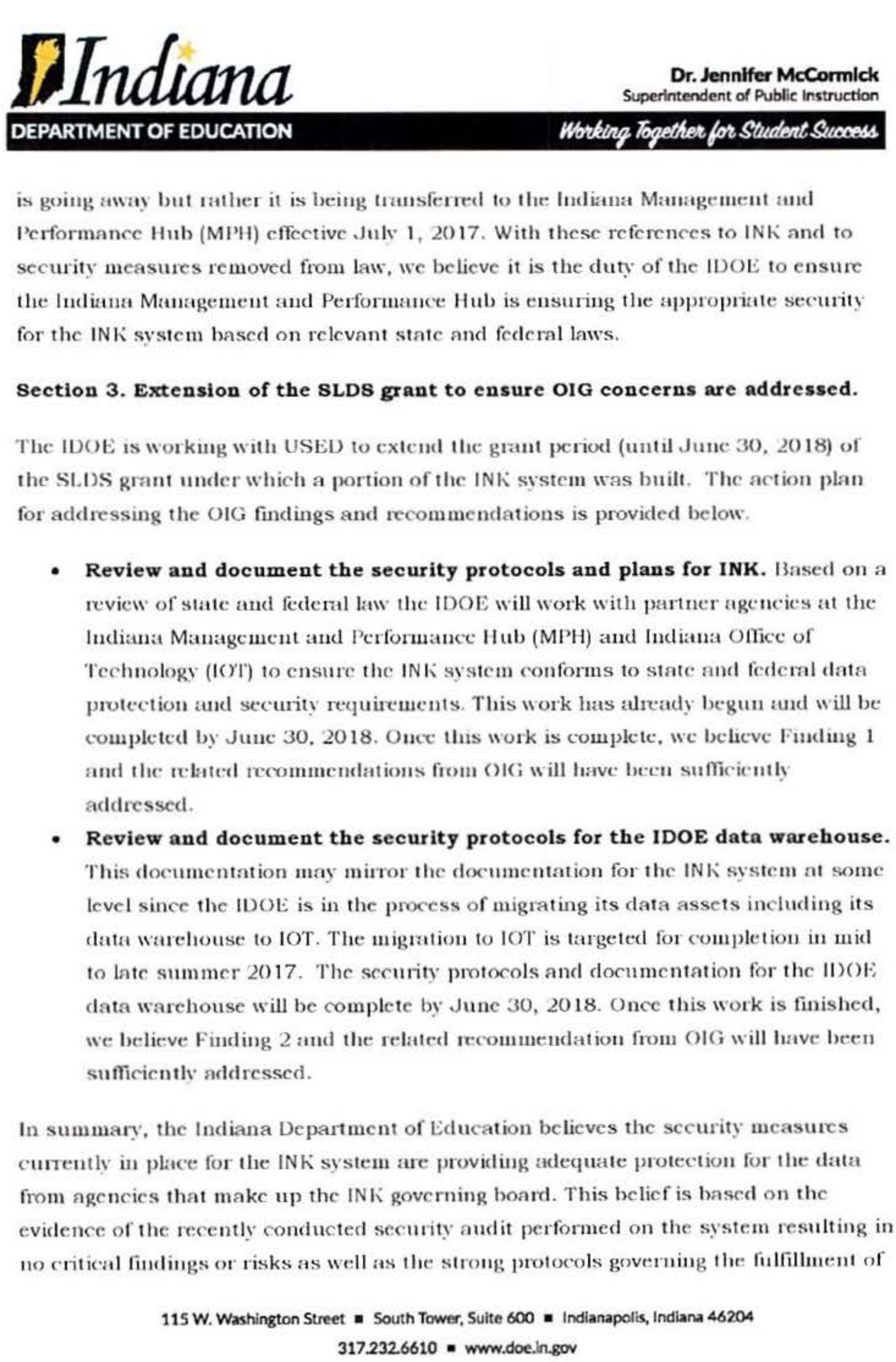
Inspector General (OIG) audit was underway was a surprise to the new administration. While we can only account for the actions of this administration, having a mutual understanding between the federal level and the state level about the data security for the SLDS project prior to its launch would have been preferable to the post hoc approach now being taken.

Since learning of the audit, Dr. McCormick's administration has been working with United States Department of Education (USED) and with the OIG's office to address findings and to draw the work of the second round of Statewide Longitudinal Data System (SLDS) grant funding to a close. During the relatively short tenure of this administration the IDOE has fulfilled the following requests from Office of Inspector General:

Information Provided to OIG	Relevant OIG Finding
Security Audit for Indiana Knowledge Network (INK) system	Finding 1
Security Audit Remediation Plan	Finding 1
Data Classification Document for Indiana Network of Knowledge (INK) data elements.	Finding 1
Clarifying Response to Provenance and Authorship of Data Classification Document	Finding 1

Section 2. Changes to Indiana Code with potential bearing on OIG findings.

Since the receipt of the OIG draft audit letter on April 10, Indiana has passed new legislation relevant to the audit. HB 1470 (https://iga.in.gov/legislative/2017/bills/house/1470#document-af23f3bf) was recently signed into law and becomes effective July 1, 2017. This legislation repeals Indiana Code § 22-4.5-10, cited multiple times in the OIG finding of non-compliance (Finding 1). This does not mean that INK or the Statewide Longitudinal Data System



is going away but rather it is being transferred to the Indiana Management and Performance Hub (MPH) effective July 1, 2017. With these references to INK and to security measures removed from law, we believe it is the duty of the IDOE to ensure the Indiana Management and Performance Hub is ensuring the appropriate security for the INK system based on relevant state and federal laws.

Section 3. Extension of the SLDS grant to ensure OIG concerns are addressed.

The IDOE is working with USED to extend the grant period (until June 30, 2018) of the SLDS grant under which a portion of the INK system was built. The action plan for addressing the OIG findings and recommendations is provided below.

- **Review and document the security protocols and plans for INK.** Based on a review of state and federal law the IDOE will work with partner agencies at the Indiana Management and Performance Hub (MPH) and Indiana Office of Technology (IOT) to ensure the INK system conforms to state and federal data protection and security requirements. This work has already begun and will be completed by June 30, 2018. Once this work is complete, we believe Finding 1 and the related recommendations from OIG will have been sufficiently addressed.
- **Review and document the security protocols for the IDOE data warehouse.** This documentation may mirror the documentation for the INK system at some level since the IDOE is in the process of migrating its data assets including its data warehouse to IOT. The migration to IOT is targeted for completion in mid to late summer 2017. The security protocols and documentation for the IDOE data warehouse will be complete by June 30, 2018. Once this work is finished, we believe Finding 2 and the related recommendation from OIG will have been sufficiently addressed.

In summary, the Indiana Department of Education believes the security measures currently in place for the INK system are providing adequate protection for the data from agencies that make up the INK governing board. This belief is based on the evidence of the recently conducted security audit performed on the system resulting in no critical findings or risks as well as the strong protocols governing the fulfillment of data requests from the INK system. We believe that a state level review and formal documentation of the security measures in place for the INK system is warranted due to the concerns raised by OIG and as a result of the new legislation (HB1470) and will work with all agencies involved to complete that review and documentation by June 30, 2018.

Sincerely,

John B. Keller

Dr. John B. Keller

Chief Technology Officer

Indiana Department of Education