Privacy Impact Assessment (PIA)

for the

Charter Online Management and Performance System (COMPS)

March 16, 2023

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Anuritha Bezwada/Information System Owner
Contact Email: anu.bezwada@ed.gov

System Owner

Name/Title: Anuritha Bezwada/Information System Owner
Principal Office: Office of Elementary and Secondary Education (OESE)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Charter Schools Program (CSP) grant program serves the purpose of Section 5201 of the Elementary and Secondary Education Act of 1965 (ESEA), which seeks to expand the number of high-quality charter schools and increase national understanding of the charter school model. The CSP has three core grant programs that administer three types of grants to the following categories of institutions.

- State Entity (SE): A State education agency or State department of education. They can authorize or oversee the authorization of charter schools and charter school creation or expansion within a framework aligned with State priorities. For example, the Massachusetts Department of Education.
- Charter Management Organizations (CMO): A non-profit organization that operates or manages multiple charter schools (either through a contract with the charter schools or as the charter holder) linked by centralized support, operations, and oversight. For example, the Knowledge is Power Program (KIPP), is a network of charter schools throughout the United States.
- Developer: An institution/non-State entity (not SE or CMO) that receives a charter school grant.

The recipients of grants within these programs are known as grantees (i.e., SE grantees, CMO grantees, and Developer grantees). In receiving charter school grants, each grantee must follow certain Federal laws and U.S. Department of Education (Department) policies, as well as adhere to the project objectives and measures the grantee outlined in their grant applications. As part of the conditions of receiving a grant, grantees are subject to yearly monitoring and reporting requirements with CSP.

The Charter Online Management and Performance System (COMPS) is a web-based application designed to assist the Department in conducting compliance and performance monitoring activities for CSP grantees. COMPS allows the Department to monitor CSP grant performance and analyze data related to accountability for academic performance and financial integrity. COMPS accumulates evidence of compliance and performance from grantees, as well as provides the ability to capture previously reported data more securely and efficiently.

COMPS currently consists of the following modules:

1. User Web-access Module: This module provides a central web portal that delivers information (e.g., data submitted by grantees using the Data Collection Module), based on role, to the Department, contractors, SEs, and charter schools. The portal permits users to see only the information that is appropriate for their roles. For example, a grantee project director would only be able to see data regarding their grant. Users can navigate to a user access management page that allows them to edit their name and email address and change their password. While the authentication process is the same for Federal employees, contractors, and grantees, additional rights and privileges are granted to Department employees and contractors that access, maintain, and support the information system.
2. Data Collection Module: This module allows SEs, CMOs, and Developer grantee users to submit charter school data to the Department. The data collection includes grantee award information and charter school sub-award information, funding type, and school enrollment information. SEs and CMOs use the system to view sub-award data reported in previous reporting periods and enter sub-award information for the current period. Developers do not have sub-award data. Grantees are only allowed to view their own grant awards and associated data. The system also supports adding comments to submitted data that contain additional relevant information (e.g., why a school closed during a reporting period).

In the future (estimated late FY 2023), the system will include the following modules:

3. Annual Performance Report (APR) Module: This module will provide CSP stakeholders with the ability to collect, manage, and view grant data and APR details. It will enable SEs, CMOs, and Developers to submit their APRs and access PDF downloads of the submitted information (e.g., narratives on their performance, how many charter schools were opened, and budget details on money spent). The SE APR module will be developed first, followed by CMO, and then Developer.
4. Data Monitoring Module: This module will include a summary of the grantee site visits conducted during the reporting cycle. The Data Monitoring module will be developed based on the monitoring protocols defined by the Department.
5. Corrective Actions Module: This module will provide Department and grantee users with the capability to monitor SE and CMO corrective actions developed because of site visit findings. Developers are not currently part of the roadmap for the Corrective Actions module. As part of CSP, the Department manages grants by monitoring compliance with applicable Federal law and ensuring schools' performance meets targeted educational objectives. If a charter school does not meet

the applicable standards, the Department may implement a corrective action plan. A corrective action is a process to identify the causes of noncompliance and to thoroughly document the resources and steps required to mitigate these issues. The Department works with the associated SE/CMO to document gaps and approve the SE/CMO's plan. The grantees cite their expected date of completion for each indicator and must provide necessary documentation and evidence as to how they have addressed each area of concern. The Department monitors progress towards rectifying the findings and provides reminders as due dates approach. The Department provides a final decision on whether the grantee in question has corrected its non-compliance.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained, or shared.

PII is collected to allow Department and contractor staff, SEs, CMOs, and Developer grantee users access to the COMPS system. PII is used to create unique logins for authorized Department staff, Department contractors, and grantee users. PII is also collected when SEs, CMOs, and Developer grantee users submit charter school data to the Department.

1.3. Is this a new system, or one that is currently in operation?

New System

1.4. Is this PIA new, or is it updating a previous version?

New PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

COMPS is authorized by Section 5201 of the ESEA, allowing the Department to expand the number of high-quality charter schools and increase the national understanding of the charter school model.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

☐ No

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation, and link, or indicate that a SORN is in progress.

☑ N/A

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Information is not retrieved by name or other personal identifier.

Records Management

If you do not know your records schedule, please consult with your records liaison, or send an email to RMHelp@ed.gov

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

Grants:

- GRS 1.2, item 020: Grant and cooperative agreement case files: Successful applications. Retention: Temporary. Destroy 10 years after final action is taken on file, longer retention authorized for business use.
- GRS 1.2, item 021: Grants and cooperative agreement case files: Unsuccessful applications. Retention: Temporary. Destroy 3 years after final action is taken on file, longer retention authorized for business use.
- GRS 1.2, item 030: Final grant and cooperative agreement products or deliverables. Retention: Temporary. Destroy when business use ceases. (Note: If the Department receives any products or deliverables from grantees as part of the grant.)
- GRS 1.2, item 010: Grant and cooperative agreement program management records. Retention: Temporary. Destroy 3 years after final action is taken on file, longer retention is authorized if required. (Note: If the Department maintains any program management records for grants in COMPS.)

System Information:

- For any logs, etc. follow GRS 3.1, item 020: Information technology operations and maintenance records. Retention: Temporary. Destroy 3 years after activity is completed, but longer retention is authorized for business use.
- For passwords/user profiles follow GRS 3.2, item 030: System access records; Systems not requiring special accountability for access. Retention: Temporary. Destroy when business use ceases.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Name, work email address, work phone number (optional), username, password, role,

and organization are captured during the creation of user accounts. Name, email address, and phone number are also collected when SEs, CMOs, and Developer grantee users submit charter school data to the Department. Names and timestamps are displayed if/when a user decides to comment within the data collection module.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The PII collected and maintained is the minimum amount required by COMPS to establish user accounts for the purpose of collecting evidence of compliance and performance from grantees as part of yearly monitoring and reporting requirements with CSP. The system allows the Department to monitor CSP grant performance and analyze data related to accountability for academic performance and financial integrity in accordance with Section 5201 of the ESEA. If individuals do not provide the required PII, it may prevent users from gaining access to COMPS. The system collects users' phone numbers as an optional field in case users prefer to be contacted via phone instead of email.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The information is provided by Department employees, Department contractors, and grantees, and captured when new accounts are created for access to the system. Grantees can also add comments to submitted data that contain additional relevant information. Names and timestamps are displayed if/when a user decides to comment within the data collection module.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

COMPS account administrators identify users that require access to COMPS. Account administrators first collect PII via encrypted email from grantees or Department employees or contractors for the creation of user accounts. The account administrators then send an access request form, which includes the user's name, email address, role, and organization, to the COMPS system owner, who reviews the request. Users with more than one role will be assigned the role with the highest access level. If approved, the request is sent to the COMPS application administrator. The application administrator then creates the requested user account and adds it to the assigned security group within the COMPS website.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The online form in the Data Collection module has restricted form filling and field validation during the information collection process in the user access management module. Information is validated by the Department yearly, requesting COMPS users certify if information is still accurate, and user access is revoked when users leave their grantee organizations.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

PII is provided by Department employees, Department contractors, and grantees, which is used to create new accounts for access to the system. The information is necessary to create unique logins for authorized Department/contractor and grantee users. PII is also collected when SEs, CMOs, and Developer grantee users submit charter school data to the Department.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Public notice is provided through the publication of this PIA. COMPS account administrators identify users that require access to COMPS. PII collected for the creation of user accounts is first collected via email from grantees or Department employees or contractors, providing the information identified in question 3.1 to a COMPS administrator to create an account for access. Since information collection is done through email, notice is provided to the COMPs users while the collection is happening through email.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

Under the authority in Section 5201 of the Elementary and Secondary Education Act of 1965, the U.S. Department of Education is collecting your personally identifiable information to create an account for access to the COMPS system. Failure to provide any of the requested information may result in an account not being created for COMPS access.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Participation in the Charter Schools Program is voluntary; however, information must be submitted to COMPS to participate in the program.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

External

5.4. Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☑ N/A

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

If an individual requires access to their information maintained in COMPS, they may obtain access by logging into their online account through the website.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

A user can edit their account (e.g., change name/add phone number) within the system. However, if a user wants to change their email address, they would need to contact the COMPS system owner by email to make this change.

6.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are notified about procedures to correct their information through directions located on the COMPS website.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Low

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access to the system is limited to authorized COMPS program personnel and contractors responsible for administering the CSP program. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), COMPS must receive a signed ATO from a designated official. FISMA controls implemented by COMPS are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read, and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

Accounts with no activity for 365 days are marked as deactivated by COMPS. Accounts can also be deactivated by a modification request or employee termination or transfer. When a system administrator receives a notification that a user has been terminated, transferred, moved, or their job function requires a different access level, the administrator can modify or delete accounts as required. Unless the account has already

been removed, deactivated accounts can be reactivated by contacting system administrators and going through the modification process.

COMPS maintains a list of all user accounts with their related access privileges. This list is reviewed annually for compliance with account management requirements. Privileged accounts are reviewed and recertified quarterly.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

COMPS is required to obtain and maintain an ATO. This process includes a tri-annual independent assessment of all required security and privacy controls and produces Plans of Action and Milestones (POA&Ms) to ensure any deficiencies are remediated. COMPS will also participate in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security controls are in place and working properly. COMPS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

In addition, COMPS has a system security plan that ensures the application is secure and monitored on a timely basis. As part of normal user access, the OESE Account Administrator identifies users that need access to COMPS and initiates the request for access to the system. Accounts that are inactive for more than 90 days are marked as disabled. Disabled accounts can be reactivated by contacting the system administrator. Accounts with no activity for 365 days are marked as deactivated. Accounts can also be deactivated by a modification request or because of employee termination or transfer.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner conducts periodic audits to ensure that PII is used in accordance with this PIA. The system owner ensures that the system security and access control plans are being executed correctly and works with the OESE CSP staff to ensure the current access lists are up to date. For example, COMPS maintains a list of all user accounts with their related access privileges. This list is reviewed annually for compliance with account management requirements. Privileged accounts are reviewed and recertified quarterly.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with COMPS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include embarrassment or loss of credentials that are used to gain access to other resources. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.