NCEdCloud IAM Service Contract Amendment Executive Summary – August 2020

Purpose:

In 2013, the NCDPI and Identity Automation partnered to create and implement the NCEdCloud Identity Access Management (IAM) Service. The goal of the NCEdCloud IAM Service was to provide each public school unit (PSU) in North Carolina with an online platform that contains a single account for their staff and student members to access a wide variety of state and local educational resources. Since implementation, over 30 applications have been integrated with the NCEdCloud IAM Service, including ten state-funded applications and more than 20 locally funded applications, totaling over 3,000 individual integrations. Entering its 8th year, the NCEdCloud IAM Service manages over two million active accounts statewide, with over one million daily authentications. In addition to several initiatives included in the cost of the current contract, two offerings are being added to support critical changes to the service.

In the summer of 2020, the NCEdCloud IAM Service Technical Advisory Committee (TAC), which is comprised of PSU Chief Technology Officers and Technology Directors from across the state, ranked the need for application rostering services to facilitate the integration of additional local applications as their highest priority. Identity Automation has offered a rostering solution as a part of the NCEdCloud IAM Service. This rostering solution would provide PSUs and the NCDPI with the ability to quickly send necessary class rostering data from the NCEdCloud IAM Service rostering platform to local and state applications. This solution will increase the speed with which applications can be used by PSUs and reduce the number of resources needed at state and local levels to integrate and access new applications.

Additionally, in 2018, Ernst and Young (EY) published a comprehensive report outlining proposed organizational changes for the NCDPI. The report included a recommendation that all Tier I technical support activities be transitioned to application technology vendors. As directed by the North Carolina State Superintendent and the North Carolina School Board of Education, to align with the EY report recommendations, the NCDPI is including Tier I support services in this contract amendment.

Contract Information:

The NCEdCloud IAM Service's annual price has been $1,500,000.00 since its initial implementation in 2015. In addition to integrating over 3,000 application integrations, since that time, numerous enhancements have been added to the service, such as alternate login options for our youngest learners, multi-factor authentication, active local directory syncing, and federation of local RapidIdentity implementations, and others.

The current contract is structured with a two-year operational term and an optional third year, starting October 1, 2020, and ending September 30, 2021. In the last year of the current contract, the vendor has offered to add several enhancements to the service at no additional cost, including parent accounts for single sign-on, use of PSU alias IDs for logging into the service, and school-level support roles.

The proposed amendment will increase the amount paid to the vendor by $200,000 for the final year of the contract, from $1,500,000.00 to $1,7000,000.00, to add the rostering solution and Tier I support services.

Business Owner: Technology Services, Enterprise Systems

AMENDMENT NUMBER 5
CONTRACT NUMBER NC10062164 (RFP # 40-IAMMS)

Contract Number NC10062164 (as amended, the "Contract") between the North Carolina Department of Public Instruction ("NCDPI") and Identity Automation, LP, 7102 North Sam Houston Pkwy W, Suite 300, Houston, TX 77064 ("Contractor") (collectively, the "Parties") is hereby amended as follows:

1. The term of this Contract is extended beginning October 1, 2020 and ending at 11:59:59 P.M. Eastern Standard Time on September 30, 2021 (the "Extended Term"). NCDPI may, in its sole discretion, extend the Contract for one additional year.

2. During the Extended Term, the Contractor shall:

    a. Continue to perform the obligations set forth in the Contract, Amendment 1, Amendment 2, Amendment 3, and Amendment 4, including but not limited to ongoing IAM Service Operations, Maintenance, and Support.
    b. Perform the additional responsibilities and services described in Attachment A (Statement of Work) to this Amendment 5, which is attached to this Amendment 5 and incorporated herein by reference. For clarity, Attachment A to this Amendment 4 replaces and supersedes Attachment A in Amendment 3 to the Contract.
    c. Continue to provide RapidIdentity software to all PSUs and NCDPI at no cost.

3. During the Extended Term, the NCDPI agrees to pay the Contractor an amount not to exceed $1,700,000.00 per contract year in accordance with the Payment Schedule set forth in Attachment A. The total amount paid by NCDPI to Contractor for obligations performed during the Extended Term shall not exceed $1,700,000.00.

4. The Service Level Agreement ("SLA") contained within the Contract is superseded by the SLA contained within Attachment B of this Amendment 5, which is incorporated by reference.

5. In the event of any inconsistency or conflict between or among the terms and conditions contained in the documents comprising this Contract, any such inconsistency or conflict shall be resolved by giving precedence in the following order: 1) This Amendment 5, including Attachment A and Attachment B; 2) Amendment 4 to the Contract; 3) Amendment 3 to the Contract; Amendment 2 to the Contract; and 4) the list of documents contained in Paragraph 4 of Amendment 1 to the Contract in the order set forth in Paragraph 4 of Amendment 1.

6. Each individual signing below warrants that he or she is duly authorized to sign and bind their respective Party to the terms and conditions of this Amendment Number 5 to the Contract.

IN WITNESS THEREOF, Identity Automation, LP and the North Carolina Department of Public Instruction have signed this **Amendment 5** on the dates set forth below.

NORTH CAROLINA DEPARTMENT OF PUBLIC INSTRUCTION

By: _____

Name: Sharon Barnard

Title: Chief Financial Officer

Date: _____

IDENTITY AUTOMATION, LP

By: _____

Name: James Litton

Title: Chief Executive Officer

Date: _____

By: _____

Name: Mark Johnson

Title: North Carolina Superintendent of Public Instruction

Date: _____

Executed pursuant to Contract Procedure rule CNTR-002, following review and approval by the North Carolina State Board of Education

Attachment A

For Amendment 5: Identity Automation
Contract Number: NC10062164
Year 8 IAM Service Renewal
Statement of Work

A. Introduction

In 2013, the NCDPI and Identity Automation partnered to create and implement the NCEdCloud Identity Access Management (IAM) Service. The goal of the NCEdCloud IAM Service was to provide each public school unit (PSU) in North Carolina with an online platform that contains a single account for their staff and student members to access a wide variety of state and local educational resources. Since implementation, over 30 applications have been integrated with the NCEdCloud IAM Service, including ten state-funded applications and more than 20 locally funded applications, totaling over 3,000 individual integrations. Entering its 8th year, the NCEdCloud IAM Service manages over two million active accounts statewide, with over one million daily authentications. In addition to several initiatives included in the cost of the current contract, two offerings are being added to support critical changes to the service.

In the summer of 2020, the NCEdCloud IAM Service Technical Advisory Committee (TAC), which is comprised of PSU Chief Technology Officers and Technology Directors from across the state, ranked the need for application rostering services to facilitate the integration of additional local applications as their highest priority. Identity Automation has offered a rostering solution as a part of the NCEdCloud IAM Service. This rostering solution would provide PSUs and the NCDPI with the ability to quickly send necessary class rostering data from the NCEdCloud IAM Service rostering platform to local and state applications. This solution will increase the speed with which applications can be used by PSUs and reduce the number of resources needed at state and local levels to integrate and access new applications.

Additionally, in 2018, Ernst and Young (EY) published a comprehensive report outlining proposed organizational changes for the NCDPI. The report included a recommendation that all Tier I technical support activities be transitioned to application technology vendors. As directed by the North Carolina State Superintendent and the North Carolina School Board of Education, to align with the EY report recommendations, the NCDPI is including Tier I support services in this contract amendment.

B. Year 8 IAM Service Operations, Maintenance, and Support

Identity Automation shall continue the IAM Service Operations, Maintenance and Support of the NCEdCloud IAM Service outlined in the Original Contract, Amendments 1 - 4, and as further described below:

1. Support of the NCEdCloud IAM Service includes Identity Automation's response to any service degradation or downtime, user issues escalated to Identity Automation by the NCDPI IAM Service Manager, NCDPI Service Desk, and MCNC, and/or any error that might arise with nightly data processing that impacts the overall integrity of user data or accounts. This would also include Identity Automation's responsibility for changes to, or interruption of, existing integrated target applications.

2. Maintenance of the NCEdCloud IAM Service includes any scheduled operational releases, fixes, or infrastructure improvements needed to keep the service operating per with the Service Level Agreement parameters.

    a. Any maintenance items initiated by Identity Automation shall be approved in writing by NCDPI Executive Sponsor before execution.
    b. Identity Automation shall align all scheduled NCEdCloud IAM Service maintenance tasks to the Home Base maintenance schedule unless an exception is approved in writing by the NCDPI Executive Sponsor. The Home Base Maintenance Schedule can be accessed on the NCDPI website at https://www.dpi.nc.gov/educators/home-base/support-and-maintenance#maintenance-schedule.

All existing NCEdCloud IAM Service Operations, Maintenance, and Support functions will remain in place as is unless requested and authorized by Executive Sponsors from NCDPI and Identity Automation.

C. Statement of Work

1. Identity Automation shall continue to integrate, support, and maintain NCDPI approved target applications from years 1 through 7.

2. Identity Automation shall retain all event logs for a maximum of three (3) years and is authorized to purge those records after-action timestamp falls outside of the required retention window.

3. If a previously approved and integrated target application is deprecated or sunset by NCDPI, Identity Automation will appropriately disable, separate, or un-configure the application from the NCEdCloud IAM Service. Removing such an integrated application does not open a new integration slot of a new application to take its place.

4. Identity Automation shall perform the integration, support, and maintenance of ten (10) new target applications during the period from October 1, 2020, through September 30, 2021, as designated by NCDPI. In addition, for each new target application identified, the NCDPI Division of Enterprise Systems, in collaboration with the NCDPI IAM Service Manager and the Application Business Owner, shall complete the Identity Automation 'Target Application Template' with the required technical details and other appropriate primary contact information for each application in the approved budget applications list.

5. A successfully integrated application means the application has been integrated within the IAM service as outlined in the design, implementation, and testing plan(s) that is approved by the NCDPI IAM Service Manager and Executive Sponsor. The Application Business

Owner, IAM Service Manager, and Executive Sponsor shall sign off on the acceptance of the new application integration only after the completion of acceptance testing by NCDPI Quality Assurance and a determination by NCDPI that the application has been successfully integrated.

6. If NCDPI requests additional target application beyond the ten (10) annual application integrations, Identity Automation will make every reasonable attempt, at no additional cost to NCDPI, to accommodate these requests based on resource availability and integration complexity. If resources do not allow for the accommodation of these additional applications, Identity Automation and NCDPI may agree to alter and reprioritize the current list of approved target applications to make provision for the new request.

7. Increased K-13 Public School Level Granular Controls: Identity Automation shall extend the current NCEdCloud IAM Service to support more granular application access controls for the K-13 Public Schools role, down to the School/Campus, and/or Grade level that can be referenced in any combination to provide the desired user access required. These granular controls shall be requested by the K-13 Public Schools through the NCDPI IAM Service Manager for Identity Automation to implement accordingly. Identity Automation and NCDPI will collaborate to develop a detailed plan for implementing granular access controls to be incorporated into the (IAM Service support documents and approved by the NCDPI and Identity Automation executive sponsors before implementation.

8. Parent Accounts: Identity Automation shall implement the ability for parents to access the NCEdCloud IAM Service for single sign-on purposes to State and/or PSU integrated applications that have a parent/guardian component. Identity Automation will provision/disable parent/guardian accounts into the service daily, based on data received from the agreed-to authoritative data source, via the NCDPI. Parents/guardians will be able to claim their accounts and perform basic account management functions, including username and password recovery/resets, via self-service tools.

9. Alias IDs: Identity Automation shall provision aliases, or local IDs, into the NCEdCloud IAM Service for use by PSUs as their username, in addition to their UID. The requirements associated with this change are as follows:

    a. The Alias IDs will be unique statewide.
    b. Alias IDs will be assigned to a single UID.
    c. There will only be one Alias IDs per user, per PSU.
    d. NCDPI will provide Alias IDs to Identity Automation as a part of nightly data file provisioning.
    e. The Alias ID field in the NCEdCloud IAM Service will be a multi-value field so that PSUs can have more than one Alias ID associated with their record if they are active in multiple PSUs.
    f. PSUs will be able to use their UID or any Alias IDs as their username to login to the NCEdCloud IAM Service.

10. Rostering: Identity Automation shall deliver the RapidIdentity Rostering platform for NCDPI and PSUs of North Carolina to provide secure, timely, reliable sharing, and bi-

directional syncing of student roster, grades, and performance data, as well as staff roster and location data, with third-party online educational resources. The Rostering service will support the data management tasks of the NCEdCloud IAM Service platform and provides NCDPI and PSUs the ability to meet the increased demand for secure data exchange required by the disparate applications. The service will provide a variety of integration methods, data formats/schemas/standards, and delivery frequencies for the current infrastructure framework and associated processes. The specific task items associated with this Rostering Service enhancement are as follows:

a. **Pilot:** Identity Automation and NCDPI shall coordinate on a list of pilot PSUs to use the new Rostering Service. Upon completion of the pilot period, NCDPI and Identity Automation will make any necessary adjustments to the procedures and/or other business processes supporting the Rostering service. Any specific service enhancements can be documented and considered by the product team but not guaranteed to be immediately implemented as part of the service. At this stage, NCDPI can authorize and approve the Rostering service for full production status or request an additional Pilot period if desired.

b. **Test and Production Environments:** As with the NCEdCloud IAM Service core system, Identity Automation will provide a test and the production environment for Rostering with production environment being architected with fault tolerance. Each environment will be Kubernetes driven, multi-tenant instance running in Amazon AWS. The core Rostering service, components like MetaVerse and Central Audit/Configuration databases, will be clustered and/or replicated. The self-service UI's will have multiple, active instances running at all times. Network load balancers will be in place to provide load balancing and to limit interruptions when outages do occur. The test environment is established for internal testing needs by Identity Automation. The scope of the test environment does not permit open-ended testing by PSU users. However, Identity Automation does permit controlled and prearranged testing for PSUs and NCDPI on an as-requested basis.

c. **Audit Logging:** Identity Automation shall retain all-action event logs related to Rostering for a maximum of 3 years and is authorized to purge those records after-action timestamp falls outside of the required retention window. This audit retention policy matches that of the NCEdCloud IAM Service. Processes, people, and status will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

d. **Service Opt-In and Request:** The NCEdCloud IAM Service Rostering will be offered to PSUs of North Carolina on an Opt-In basis unless otherwise designated by NCDPI. PSUs will submit an online request via the NCEdCloud IAM Service MCNC website. Upon review and approval, Identity Automation will provision a Rostering tenant for the requesting PSU and initiate the onboarding process outlined in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

e. **Catalog of Application Artifacts:** Identity Automation shall provide a catalog of Application Artifacts that enable NCDPI and PSU Roster Administrators to perform integrations with a variety of Data Consumers and Producers. Artifacts refer to a set of instructions that RapidIdentity uses to programmatically and dynamically create the proper interface for an administrator to setup and configure ETL Flows between

the two systems. The Rostering solution supports integrations with providers and consumers using the IMS Global OneRoster™ 1.1 Standard. Any application/system integration requested outside of the standard is evaluated on a case by case basis for effort level.

f. **Application Providers and Consumers:** Identity Automation shall provide an approved catalog of templates for a variety of Application Providers and Consumers. PSU administrators select the desired application provider and/or consumer and then complete the configuration form to define the specific connection systems, record definitions, and other specific parameters for how the data will be consumed, processed, and provided between endpoints. All Provider and Consumer information will be provided, managed, and supported by PSU Administrators.

   i. Once application providers and consumers are defined, PSU administrators can enable each to process data on a schedule. It will be the PSU administrator's responsibility to correctly schedule each per any technical and/or business policies as defined by NCDPI or the producer/consumer applications themselves.

   ii. **All North Carolina PSU facing Providers and Consumers for Rostering of the NCEdCloud IAM Service shall be vetted and approved by NCDPI**.

g. **PSU Roster Administrators:** Each PSU will have designated Roster Administrators that will be responsible for the provider and consumer integrations of relevant applications/systems of its tenant. Identity Automation will create and manage the catalog of applications and artifacts that support PSU integrations. Processes, people, and responsibilities of all parties will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

h. **NCDPI Roster Administrators:** NCDPI will have designated Roster Administrators that will be responsible for the provider and consumer integrations of relevant applications/systems of its tenant. Identity Automation will create and manage the catalog of applications and artifacts that support PSU integrations. Processes, people, and responsibilities of all parties will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan

i. **Service Monitoring, Alerts, and Notifications:** The NCEdCloud IAM Service Rostering shall provide monitoring and appropriate alert notifications to NCDPI and impacted PSU for defined and agreed upon critical service components and data processing functions. Identity Automation shall provide NCDPI with key availability metrics for uptime. Identity Automation and NCDPI will collaborate to develop a detailed plan for the Service Monitoring, Alerts, and Notification frequency and audience. Processes, people, and status will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

j. **Communications:** Identity Automation will coordinate with NCDPI to create appropriate content for communications to NCDPI and PSU staff members about the Rostering service, associated process changes, and other service announcements (current and future) for this enhancement.

k. **Rostering Service Access and Authority:** As the executive sponsor of the NCEdCloud IAM Service Rostering functions, NCDPI has specific Access and Authority rights of that service.
    i. NCDPI has full authority to request access to all audit data and corresponding materials related to the NCEdCloud IAM Service Rostering solution.
    ii. Identity Automation will provide information as requested and be responsible for reporting any matters of concern regarding security, privacy, and/or safety to NCDPI immediately.
    iii. Identity Automation understands that NCDPI has the authority to intervene in any data transfer/access matters as it deems appropriate and directs the vendor's actions accordingly.
    iv. Identity Automation understands that NCDPI has the authority to request the granting and revoke of rostering services to any PSU personnel at its discretion. Processes, people, and status will be maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

l. **Documentation and Training:** Identity Automation shall create, deliver, and maintain all detailed documentation of all operations, support, and maintenance efforts of the core Rostering service, release management plans, and integrated catalog of artifacts (current and future). Identity Automation shall ensure that corresponding training materials will remain updated, available, and properly aligned to the functionality of the Rostering Service. Identity Automation shall also provide and document any additional specific information regarding the service as requested by the NCDPI executive sponsor. Processes, people, and status will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

m. **NCEdCloud IAM Service Rostering Technical Implementation Plan:** Identity Automation shall document and maintain comprehensive policies and procedures matters for the NCEdCloud IAM Service Rostering functions in a Technical Implementation Plan. This process is consistent with how other functions and processes are documented for NCEdCloud IAM Service components.

11. Tier I Support Services: Identity Automation will provide Tier 1 support services to NCEdCloud IAM Service for each PSU and NCDPI. The Tier 1 support services would be extended to designated Administrators from each PSU and NCDPI and enable NCDPI to transition primary IAM customer support responsibilities from the NCDPI Technology Support Center to Identity Automation. Each designated PSU and NCDPI staff member will receive access to the Identity Automation Customer Support Community.

    a. PSUs and NCDPI shall have access to a variety of support resources, including at a minimum:
        i. Phone, Email, Chat and Web Support Portal
        ii. Customer Community for FAQ and Knowledge Base Articles
        iii. RapidIdentity Product Guides, Integrations Guides, and Release Notes
        iv. Standard RapidIdentity Training Videos
        v. Product and Service Feature Request Portal
        vi. Downloads to RapidIdentity Installer Files and Browser Plug-Ins

vii. Reporting Metrics

b. **Customer Support Community Access:** Identity Automation shall create and distribute accounts and access to the Identity Automation Customer Support Community for authorized individuals as designated by NCDPI. Identity Automation will coordinate with NCDPI to establish an appropriate process for managing these support accounts in accordance with NCDPI policies. Processes, people, and status will be maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

c. **Reporting Metrics:** Identity Automation and NCDPI shall define the type, frequency, target audience, and communication medium of the desired reporting metrics for Support Services. Specific details for reporting metrics shall be recorded and maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

d. **Service Monitoring, Alerts, and Notifications:** The NCEdCloud IAM Service Support shall provide monitoring for all support services and appropriate notifications to NCDPI and impacted PSUs for any issues that arrive with the core service and/or other support components. Identity Automation shall provide NCDPI with key availability metrics for uptime. This report will be provided monthly. Identity Automation and NCDPI will collaborate to develop a detailed plan for the Service Monitoring, Alerts, and Notification frequency and audience. Processes, people, and status will be maintained in the NCEdCloud IAM Service Rostering Technical Implementation Plan.

e. **Communications:** Identity Automation will assist NCDPI to create appropriate content for communications to NCDPI and PSU staff members about the new Support Services and associated process changes for this enhancement. Historically, NCDPI has been the primary point of contact to PSUs for all NCEdCloud IAM Service matters but the new Support Service creates a direct link between PSUs and Identity Automation. As such Identity Automation will coordinate with NCDPI to define the appropriate time, content, and frequency of communications directly between Identity Automation and PSU. Processes, people, and status will be maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

f. Support Service Access and Authority. As the executive sponsor of the NCEdCloud IAM Service Support functions, NCDPI has specific Access and Authority rights of that service.

   i. NCDPI has full authority to request access to any and all support case content and materials related to the NCEdCloud IAM Service.

   ii. Identity Automation will provide information as requested and be responsible for reporting any matters of concern regarding security, privacy, and/or safety to NCDPI immediately.

   iii. Identity Automation understands that NCDPI has the authority to intervene in support matters as it deems appropriate and directs the vendor's actions accordingly.

   iv. Identity Automation understands that NCDPI has the authority to request the granting and revoke of support services to any PSU personnel at its discretion. Processes, people, and status will be maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

g. **Documentation and Training:** Identity Automation shall create, deliver, and maintain all detailed documentation of all operations, support, and maintenance efforts of the core Support Services. Identity Automation shall ensure that corresponding training materials will remain updated, available, and properly aligned to the functionality of the Support Services. Identity Automation shall also provide and document any additional specific information regarding the service as requested by the NCDPI executive sponsor. Processes, people, and status will be maintained in the NCEdCloud IAM Service Support Technical Implementation Plan.

h. **NCEdCloud IAM Service Support Technical Implementation Plan:** Identity Automation shall document and maintain comprehensive policies and procedures matters for the NCEdCloud IAM Service Support functions in a Technical Implementation Plan. This process is consistent for how other functions and processes are documented for NCEdCloud IAM Service components.

12. Analytics and Data Dashboard: Identity Automation shall provide an analytics and data dashboard in the NCEdCloud IAM Service, that is accessible to State and PSU users that have the approved roles. The analytics and data dashboard will provide visual, easy to understand, representations of data related to user logins and user activity within the service. Data that supports the analytics and data dashboard should also be accessible, sortable, and be able to be downloaded. The Analytics and Data Dashboard enhancement shall include the following features:
    a. The Analytics and Data Dashboard will display user login data and visual trends in summary form and be sortable by person type (staff/student), PSU, school, grade, role, and login date.
    b. The dashboard will show ranked data regarding which applications users are attempting to access from within the service.
    c. The dashboard will provide customizable reports that show user login and application accessing information. Users will be able to view these reports within the tool and/or download them in a tabular format.
    d. Data will be refreshed nightly, at a minimum.
    e. Be accessible to approved NCDPI staff that have the State Help Desk roles. These users will have access to statewide data.
    f. Be accessible to approved Privileged Role users at the PSU level and see data associated with their specific PSU.
    g. Be accessible to approved school-level staff and see data associated with their specific school or schools.

13. Documentation and Training: Identity Automation shall continue to maintain, update, and make available all detailed documentation of all operations, support, and maintenance efforts of core service, release management plans, and integrated target applications (current and future). Identity Automation shall ensure that corresponding training materials will remain updated, available, and properly aligned to the functionality of the NCEdCloud IAM Service. Identity Automation shall also provide any additional specific use case information regarding the service as requested by the NCDPI executive sponsor.

14. NCEdCloud IAM Service Technical Implementation Plan: Identity Automation shall continue to maintain and update the comprehensive IAM Service Technical Implementation

Plan for all changes associated with architectural infrastructure components and operational functional changes.

D. Amendment 5 Spending Plan and Payment Schedule

The Amendment 5 payment schedule shall be as follows:

a. Due in quarterly installments 30 days after receipt and approval of invoice. Invoice dates shall be October 1, 2020 for $800,000.00, January 1, 2021, for $300,000.00, April 1, 2021, for $300,000.00, and June 1, 2021, for $300,000.00.
b. Notes: includes operations, maintenance, and support as outlined in the original Contract, Amendments 1-4, and in Section B of this SOW. This also includes ten (10) new target applications for Year 8 (October 1, 2020 — September 30, 2021) of this Contract.

This Space Intentionally Left Blank.

Attachment B

NCEdCloud IAM Service Level Agreement for Identity Automation

SLA Approvers

Approver Name	Approver Signature	Approval Date	Approval Title
NCSBE – State			
Michael Nicolaides			CIO
Julien Alhour			Director, Enterprise System
Jordan Kincaid			IT Manager
Identity Automation – Service Provider			
James Litton			Executive Chairman
Michael Webb			CTO

Table of Contents

1. Introduction

This Service Level Agreement ("SLA") sets forth the framework and service levels thereunder that Identity Automation LP ("Identity Automation" or "Service Provider") shall provide to the North Carolina Department of Public Instruction ("NCDPI" or the "State") for the hosting, operation, and support of the NCEdCloud IAM Service. This SLA shall be deemed an exhibit to the Agreement by and between Identity Automation and NCDPI, dated _____, 2020. Identity Automation and NCDPI or the State are hereinafter collectively referred to as the "Parties." "Service Provider" refers to Identity Automation and/or its third-party hosting facility provider. This SLA sets forth provisions for how the levels of service provided by Identity Automation for the NCEdCloud IAM Service ("NCEdCloud" or the "Service") will be measured, define when Identity Automation will respond to issues within the Service, and define how the State will accrue credit in the event that issues within the Service are not resolved within the agreed to timeframes. This SLA shall immediately supersede any previous SLAs that have been agreed to by the Parties and shall control over any contradictory or ambiguous service level provisions contained with the Contract.

This document is organized into the following four sections:

- Section 1 - Introduction
- Section 2 - Hosting Services
- Section 3 - System Maintenance and System Support Services
- Section 4 - Application Support Services

1.1 Service Level Agreement Changes

The Parties agree that no alteration of the terms of this SLA shall be valid unless made in writing, which is attached hereto and incorporated herein by reference. No oral understanding or contracts are incorporated herein, and no alteration or variations of the terms hereof shall be binding on either party unless made in writing and signed by both Parties. Approved changes to this SLA will be effective as of date of the last executing signature to the applicable SLA. All such amendments serve to modify this SLA and in the event of any conflict between the terms of this SLA and an SLA Amendment, the terms of the SLA Amendment will take govern.

1.2 Period of Agreement

The Parties agree to review this SLA prior to any contract amendment or extension, at a minimum. The time, place, and date of the review shall be as mutually agreed upon by the Parties. The review will cover services provided, service levels and procedures. Any changes to this SLA resulting from such review must be approved by both Parties and reduced to writing in the form of an SLA Amendment as described in Section 1.2 above.

1.3 Review Procedure

The time, place, and date of the review shall be as mutually agreed upon by the Parties. The review will cover services provided, service levels and procedures. Any changes to this SLA resulting from such review must be approved by both Parties and reduced to writing in the form of an SLA Amendment as described in Section 1.2 above.

1.4 Definitions

The following definitions shall apply to this SLA. All capitalized terms not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement:

a. **"Account Credit"** is the sum of the monetarily expressed credit calculations for the NCEdCloud IAM Service Uptime each invoice period.

b. **"Annual Not-To-Exceed Amount"** is defined as the total monetary amount due under this Amendment 5 in exchange for the services provided during Year 8 of the IAM Service Renewal.

c. **"Current Invoice Amount"** is defined as the total monetary amount due for the current scheduled payment period, as described in the Amendment 4 SOW.

d. **"Credit Percentage"** is used in the calculation of credits accrued by NCDPI due to Contractor's failure to meet the Uptime objective and is set forth in the Section 1.3. Availability Service Credits.

e. **"Disputed Account Credit"** is defined as the sum of all Account Credits in dispute, as detailed in the process below in Section 6.4.

f. **"Emergency Maintenance"** is defined as activity critical to the usability of the NCEdCloud IAM Service, including but not limited to, applying urgent security vulnerability fixes, preventing an imminent outage, and restoring the Services from a service disruption. Contractor shall notify NCDPI of Emergency Maintenance in advance. Reasonable efforts will be made to ensure Emergency Maintenance is conducted outside of normal business hours.

g. **"Excluded Events"** are events that affect the accessibility of the NCEdCloud IAM Service that are outside of Contractor's control. Such events are limited to a failure of NCDPI's or PSU's network infrastructure, or failure of NCDPI's or a PSU's connection to the internet.

h. **"NCEdCloud IAM Service or the Service"** is defined as the sum of the components, elements, features, functionality, and aspects that constitute the North Carolina K-12 Identity and Access Management Service. This includes facilities, infrastructure, hardware, software, and network that are hosted, owned, and/or

managed by Identity Automation, contractors and/or sub-contractors of Identity Automation.

i. **"Outage"** is a failure of the NCEdCloud IAM Service to be Available for use by NCDPI, LEAs, teachers, students, and any other users via an internet connection. Excluded Events shall not be considered Outages. When calculating the duration of an Outage, the period begins upon the earlier of (a) the failure being reported by Contractor, (b) the failure being reported by NCDPI, or (c) the failure being reported to Contractor by an LEA, teacher, student, or any other user. The period ends when the Outage has been resolved.

j. **"Public School Unit or PSU"** is defined as North Carolina K-12 schools, school districts, charter schools, lab schools, or State-run schools.

k. **"Scheduled Downtime"** is defined as the period during which the NCEdCloud IAM Service is not Available because of scheduled maintenance, system updates and patches, and system upgrades, all of which must be planned and agreed upon in advance.

l. **"Term Months"** is defined as the number of calendar months in the term of the most current Agreement.

m. **"Total Account Credit"** is defined as the sum of all Account Credits not in dispute and not already applied as detailed below.

n. **"Total Potential Time"** shall be the total time, measured in minutes, in a calendar month minus the total time for Scheduled Downtime and for any Excluded Events.

o. **"Users"** any person who has an active account within the NCEdCloud IAM Service. This can include, but is not limited to, K-13 students, school district teachers and staff members, DPI staff, third-party vendors, and student guardians.

p. **"Uptime"** is defined as Total Potential Time minus the total time, measured in minutes, in a calendar month during which there is an Outage(s). Uptime shall be expressed as a percentage and is calculated in accordance with Section 1.3.

2. Hosting Services

This section refers to the hosting services to be provided by Identity Automation.

2.1 Hosting Site

Identity Automation will comply with all applicable state statutes, including N.C.G.S. 1438-1375 through 1379. Identity Automation must utilize a Third-Party Assessment Agency/Organization to perform the assessment of Identity Automation's security controls to determine the extent to which security controls are implemented correctly, operate as

intended, and comply with the Statewide Information Security Manual. Assessments must be conducted using industry best practice certification, e.g. SOC 2 Type 2 or NIST Risk Management Framework (RMF). Identity Automation shall provide the assessment reports required by this section within one (1) year of the assessment completion date. Contracts with vendors providing offsite hosting or cloud services must require the vendor to provide the State with an annual risk assessment report to establish compliance with N.C.G.S. 1436-1342. The State shall ensure that its security staff is available for consultation during these processes. Identified gaps between required Security Control Baselines and Identity Automation's implementation as documented in the Security Assessment Report shall be tracked by Identity Automation for mitigation in a Plan of Action and Milestones (POA&M) document. Identity Automation will remediate within an agreed-upon timeline any material weaknesses in IA's security controls identified in such report that are identified as a reason for the auditor to issue such report as "qualified" or "adverse", and Identity Automation will use commercially reasonable efforts to remediate any other material weaknesses identified in such report. The proposed production system must be securely hosted and accessed in a data center that meets and conforms to SSAE16 Type II certification. Identity Automation's hosted site shall remain operational 24 x 7 x 365 during the term of the Service contract, subject to the terms of this SLA. The data center may be located at Identity Automation's site(s) or may be subcontracted. The hosting site must include the use of auditable procedures for system operations, change control, capacity planning, performance management, problem management, backup (including off-site storage), and fail-safe and disaster recovery. The systems environment must be scalable to accommodate future systems expansion as specifically described in Section 2.6 below and must reside in the continental United States of America.

2.2 Hosting Services

Hosting Services shall consist of the following:

a) Provision and housing of the NCEdCloud IAM Service computer hardware within a designated physical facility including conditioned electrical power and multiple access paths to the Internet;

b) Provision of secure access via the Internet, using a web browser and web services, to the NCEdCloud IAM Service by its Users; shall support all major web browsers, including but not limited to, IE, Chrome, Safari, Firefox, at current version and two versions prior; shall support all major mobile web browsers at current version and two versions prior;

c) Installation, configuration, system administration, and maintenance services for the facilities, equipment, and software required to operate and ensure access to the NCEdCloud IAM Service in a manner consistent with this SLA. Identity Automation or its approved subcontractor also shall perform standard database administration functions to maintain efficient and secure operation of the hosted databases;

d) Provision and support of a minimum of two system instances - production and a testable (QA) non-production instance.

Identify Automation may use third parties to provide physical infrastructure for its data centers, Internet connectivity, energy utilities, security services, fire prevention services, environmental services such as HVAC, and third parties for maintenance and support on hardware, all of which may be part of Hosting Services. Where Identity Automation is intending to make a change to the Hosting Services that will have a direct and material impact on the State, or, where the change would allow a third party direct access to the State's Confidential Information or the State Data, Identity Automation will provide prior written notice to the State. Identity Automation may be required to demonstrate the third party is duly authorized, licensed and or capable of performing the task or service requested. In either case, Identity Automation shall remain solely responsible for providing the Hosting Services described herein, according to the Service Levels described in this SLA.

2.3 Service Levels

Identity Automation, or its approved subcontractor(s), shall provide Hosting Services to enable the State, and its Users, to use the NCEdCloud IAM Service as described in the Agreement. The Service Levels that Identity Automation, or its approved subcontractor(s), shall meet are set forth below, together with remedies for the failure to meet them. A failure caused by a hosting entity chosen by Identity Automation shall be treated as a failure caused by Identity Automation.

a) The following terms shall be used in defining and measuring compliance with Service Levels:

   i) **"Availability"** or **"Available"** means the total time in a calendar month when the NCEdCloud IAM Service is accessible via an Internet connection and performing the major and critical functions, including the Identity Provider (IDP) and the IAM Service portal, as specified in the Agreement. The hosted environment shall be deemed available, even if it is not accessible by the Users, if the inaccessibility is due to the State's network infrastructure or its connection to the Internet, when a user's computer or network infrastructure impairs or prevents access, an Internet failure outside the control of Identity Automation or its approved subcontractor(s), or a force majeure event.

   ii) **"Downtime"** shall mean Scheduled Downtime and Unscheduled Downtime, collectively.

   iii) **"Scheduled Downtime"** is defined as time planned and agreed upon in advance for reasons including scheduled maintenance, system updates and patches, planned system outages and system upgrades with notification.

   iv) **"System Response Time"** means the amount of time elapsed between the point at which an http/https request reaches the Hosting Site and the beginning of the transmission of a response back to the originating station. Identity Automation *or* its approved subcontractor(s) shall continually monitor the performance of the hosted environment and will use commercially reasonable efforts to maintain the agreed upon Response Times. Response Time is a metric exclusive to Identity Automation's Hosting Site.

v) **"Uptime"** means the percentage of total time in a calendar month that the hosted environment is either Available or in Scheduled Downtime. Uptime is calculated as the sum of Available time plus Scheduled Downtime divided by total time, expressed as a percentage.

vi) **"Unscheduled Downtime"** is 100% minus Uptime, both expressed as percentages. For example, if the Service Uptime was 98% for a given month, the Unscheduled Downtime is 2% (100% - 98%). Unscheduled Downtime shall be determined to start as of the time when Identity Automation becomes aware of the outage, through internal system monitoring, notification by the State, or notification by a User, whichever occurs first.

2.4 Availability Service Credits

The table below lists credit tiers based on monthly application Uptime. If the NCEdCloud IAM Service monthly Uptime is less than 99.9%, NCDPI shall be entitled to receive automatic credits as indicated below.

AVAILABILITY CREDIT TIERS	
UPTIME	**CREDIT PERCENTAGE**
≥ 99.9%	0%
< 99.9% and ≥ 99.8%	5%
< 99.8% and ≥ 99.6%	10%
< 99.6% and ≥ 99.2%	15%
< 99.2%	20%

Pursuant to Attachment A of Amendment 5, the Statement of Work (SOW), Identity Automation shall provide NCDPI with key availability metrics on a monthly basis, to include Uptime percentage. NCDPI agrees to notify Contractor if the NCEdCloud IAM Services provided under this Amendment are not in good working order or are not available during the term of this Amendment. Uptime % will be calculated as follows:

$$Uptime\ \% = \left(\frac{Total\ Potential\ Time - Outage\ Time}{Total\ Potential\ Time}\right) x\ 100$$

Identity Automation will calculate, using the equation below, the Credit Amount by dividing the total Annual Not-To-Exceed Amount by the Term Months, and then multiplying that value by the Credit Percentage corresponding with the applicable monthly Uptime percentage listed in the table above.

$$Credit\ Amount = \frac{Annual\ Not-To-Exceed-Amount}{Term\ Months}\ x\ Credit\ Percentage$$

2.5 System Response Time

a) Identity Automation agrees that the NCEdCloud IAM Service System Response Time, for the IDP and the IAM Service portal, shall be within 3.5 seconds for the maximum number of concurrent Users within the production environment ("Response Time Metric"). **Average System Response Time** is calculated by a third-party vendor who will monitor the Service Response Time and provide an average system response time. Requests for administrative reconfiguration, system exports, imports, uploads and reporting are excluded from the Response Time Metric requirement due to the intensive nature of such large-scale operations.

b) If the Service fails to meet the Average System Response Time of 3.5 seconds on a quarterly basis, the State shall be entitled to remedies in the form of an account credit, which Identity Automation shall provide in accordance with the applicable Credit Percentage set forth in the table below. For the State, this will amount to the Current Invoice Amount multiplied by the Credit Percentage that corresponds with the Average Response Time as set forth below.

c) If the system is not responding due to the lack of availability, then only the credits set forth in Section 2.3 related to system Uptime shall be applicable. This section is only applicable to this SLA.

AVERAGE RESPONSE TIME	**CREDIT PERCENTAGE**
< 3.5 seconds	0%
3.50001 seconds - 5 seconds	10%
> 5 seconds	15%

d) Average System Response Time statistics within the production environment will be reported in the SLA Performance Report. System Response Time is measured from the server when responding to an http/https request for various NCEdCloud IAM Service transactions.

The table below lists credit tiers based on monthly application Uptime. If the NCEdCloud IAM Service monthly Uptime is less than 99.9%, NCDPI shall be entitled to receive automatic credits as indicated below.

AVAILABILITY CREDIT TIERS	
UPTIME	**CREDIT PERCENTAGE**
≥ 99.9%	0%
< 99.9% and ≥ 99.8%	5%
< 99.8% and ≥ 99.6%	10%
< 99.6% and ≥ 99.2%	15%
< 99.2%	20%

2.6 Maximum Account Credit

The State acknowledges and agrees that: (a) the account credits contemplated by Sections 2.3, 2.4, 2.5, and 4.4 of this SLA are remedies and represent the State's sole remedy for Identity Automation's failure to meet the service levels set forth herein; and (b) the aggregate amount of account credits, for all instances where Identity Automation in any given quarter does not meet the services levels set forth in Sections 2.3 or 2.4 or 2.5 or 4.4 of this SLA, shall not exceed 30% of the total annual contracted amount agreement to in Amendment 5. For example, if the Unscheduled Downtime in quarter "X" is 140 minutes and the Average System Response Time is > 5 seconds, the State would receive an aggregate account credit equal to 30% of the next scheduled invoice amount for quarter X and not receive a credit of 35%.

3. System Maintenance and Support Services

This section describes the maintenance and support Identity Automation will provide the State related to The NCEdCloud IAM Service.

3.1 System Support Service Objectives

The following are general System Support Services for which Identity Automation shall be responsible:

a) Identity Automation shall process, categorize and assess all changes to the NCEdCloud IAM Service environment, validating that changes to the Service are tested and controlled, and unplanned services disruptions are avoided.

b) Identity Automation shall notify the State of all necessary security patches that require a system outage.

c) Identity Automation shall oversee and maintain the Service so that all software and hardware are supported technology, as deemed appropriate for the State business functions.

d) Identity Automation is providing Tier 1, 2, and 3 Support Services via the Identity Automation Support Portal, 7:30 AM - 5:30 PM Eastern Time. Any Critical and Urgent (Severity 1 & 2) incidents will be handled on a 24 x 7 x 365 until resolved as indicated in Table 4.4.1 "Severity Levels" below.

e) Identity Automation personnel providing the Support Services pursuant to this document shall have expertise and be fully trained in problem identification and resolution relating to NCEdCloud IAM Service. Identity Automation personnel shall provide access to their software engineering and technical resources for quick resolution, feedback, troubleshooting, and support.

f) All incidents shall be logged in designated on-line support management software. The reported incidents shall be viewable in detail and summary format online by designated State Representatives.

g) Identity Automation shall provide to the State a monthly support incident analysis report, in a mutually agreed upon format.

3.2 System Maintenance and Updates

Subject to the terms and conditions of the Agreement and this SLA, Identity Automation shall provide Maintenance Services for the NCEdCloud IAM Service ("System Maintenance Services"). System Maintenance Services shall consist of the following:

a) The State has three environments that will be hosted by Identity Automation.

   i) The Production Environment contains the "live" software, hardware. and data (databases) for the Service and any other application or application component in use by the Service platform. Production covered on the disaster recovery procedures.

   ii) The QA environment is used for functional testing of the current release software to ensure that all scheduled releases pass testing before being promoted to production. These tests focus on documented test cases and test results and are not intended to do overall data validation. The QA environment shall be made available to the State.

a) Identity Automation shall periodically deploy releases of the Service into the QA and Production environments as defined above.

b) Identity Automation shall refresh data from production into QA on the same frequency that the Production environment is refreshed; notwithstanding the foregoing, the State acknowledges and agrees that there may be times when Identity Automation, in its discretion, delays such a request contingent on and subject to then-current Identity Automation software release testing cycles.

c) Except in cases of emergency, Identity Automation shall notify the State at least ten (10) days prior to activating each update unless a shorter time is mutually agreed upon. Notification shall include the following, at a minimum:

   i) Date of Update activation;

   ii) Notes describing the Update content;

   iii) Date, time, and duration of time required to deploy the Update; and

3.3 Monitoring and Reporting Services

Identity Automation shall provide 24 X 7 X 365 monitoring services that include the activities associated with the ongoing surveillance, tracking, problem escalation, resolution and reporting of application development problems. This monitoring shall include, but is not limited to:

a) Monitoring the status of the Service and notifying the State operations team of potential issues;

b) Monitoring the connections between the different layers of the Service;

c) Monitoring the IDP layer of the Service;

d) Monitoring for critical exceptions within the Service;

e) Monitoring the transaction and login rates for capacity and security; and

f) Monitoring the connections between the different layers of the system and the public internet.

4. NCEdCloud IAM Service Support Services

Subject to the terms and conditions of the Agreement and this SLA, Identity Automation shall provide the Support Services described herein for all components of NCEdCloud IAM Service, including hardware and third party supplied system software chosen by Identity Automation. Unless otherwise specified herein, Identity Automation will provide the Support Services from 7:30 AM to 5:30 PM EST, Monday through Friday, except during designated North Carolina State holidays.

4.1 Support Services Scope

Identity Automation shall provide the following Support Services in accordance with this SLA.

a) Receipt and review of issues submitted via any of the following methods:

   i) Phone, Email, Chat and Web Support Portal

b) Assignment and revision of the severity level of tickets

c) Response to tickets submitted via the Identity Automation Web Support Portal or phone

d) Resolution or escalation of tickets

4.2 Support Services Tier Levels

a) Tier/Level 1 (T1/L1) - This is the initial support level responsible for basic customer issues. It is synonymous with first-line support. The first job of a Tier I specialist is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem. This level should gather as much information as possible from the end user. Once identification of the underlying problem is established, the specialist can begin sorting through the possible solutions available.

b) Tier/Level 2 (T2/L2) - This is a more in-depth technical support level than Tier I and the techs are more experienced and knowledgeable on a particular product or service. It is synonymous with level 2 support.

c) Tier/Level 3 (T3/L3) - This is the highest level of support within the organization responsible for handling the most difficult or advanced problems. It is synonymous with level 3 support. These individuals are experts in their fields and are responsible for not only assisting both Tier I and Tier II personnel, but with the research and development of solutions to new or unknown issues.

d) Tier/Level 4 (T4/L1) - A fourth level of support often representing an escalation point beyond the organization. This is generally a hardware or software vendor

4.3 Service Levels, Severity, and Escalation Procedures

a) Identity Automation shall assign an appropriate severity level based on the severity level descriptions contained in Table 4.3.1 below and shall convey such designation to the State when reporting the issue. The severity level will be the basis for the prioritization of work to resolve tickets. Support personnel shall revise the severity level designation for a ticket as needed, based on emerging information. Such change will be made or approved by the assigned supervisor of the support personnel and will be reported to the ticket submitter

b) If the State or the PSU does not agree with Identity Automation's designation of the severity level for any issue, it shall indicate the severity level the State's attributes to the issue as soon as possible, but in any event by the end of the Initial Response time for the severity level originally designated by the State.

c) The Parties shall work in good faith to agree upon the appropriate severity level provided that such determination shall not unreasonably delay the implementation of a solution to the issue.

d) Problem Resolution time begins when Identity Automation becomes aware of the issue, whether through notification by the State, a user, Identity Automation's own internal monitoring or otherwise, whichever occurs first.

e) Complaints: For any incident reported with unsatisfactory results not in compliance

with Service Levels, the State shall escalate to the Identity Automation Contract Administrator.

f) Clocking of Tickets: Severity 3, 4, and 5 tickets submitted after hours will be "clocked" as of the start of the next working shift. For avoidance of doubt, a ticket submitted at 5:31 pm on Tuesday, will be clocked as arriving at 7:30 am on Wednesday – assuming no holidays. Similarly, a ticket submitted at 5:31 pm on Friday will be clocked as arriving 7:30 am on Monday, assuming no holidays.

g) Initial Response Time is the amount of elapsed time between a ticket being submitted (clocked in accordance with "clocking of tickets" outlined above) and Identity Automation's Response, which consists of Identity Automation's communication to the user that the ticket was received, registered, assigned a severity level, and the identity of support personnel to whom the ticket is assigned.

h) Information and Deferral: The NCDPI and PSUs are required to provide sufficient available information relevant to the circumstances of tickets they submit. If the provided information is insufficient, Identity Automation will request reasonable additional information from the ticket submitter. Upon such a request by Identity Automation, the ticket will be considered deferred for the purposes of SLAs, until such time as the ticket submitter provides the reasonable additional information. If the ticket submitter does not provide sufficient information to Identity Automation's request within ten (10) business days, the deferred ticket may be closed.

i) Resolution refers to correction, a satisfactory interim workaround, the closure of a deferred ticket due to lack of response by the ticket submitter, the closure of tickets because of ticket duplication, or the determination that the ticket is unrelated to the operation of the NCEdCloud IAM Service. Upon Resolution, Identity Automation will notify the ticket submitter of such Resolution via email with reference to the ticket number, a brief description of the Resolution, and a notification that the ticket will be closed.

Table 4.3.1 Severity Levels

Severity Level	Title	Description	Notes	Initial Response[1]	Problem Resolution[2]
1	Critical	The system is unavailable to a large portion of the product's users or a major and vital feature of the system is unavailable to a large portion of the product's users adversely affecting the ability to use the core product. There is no work- around.	This pertains to the software working or not working for all – or a vast majority of users attempting to access the system. For instance, printing could be considered a vital feature, however if one user has a problem printing a report, this would not constitute a Sev-1 incident – it is likely a printer configuration issue for that one user.	Prime Time: M-F[1] 7:30 am – 5:30 pm EST Response to defect within 45 minutes Non-Prime Time: M-F[4] 5:31 pm – 7:29 am EST Response to defect within 90 minutes Weekends/Holidays[4] 7:30 am – 5:30 pm EST Response to defect within 120 minutes Weekends/Holidays[4] 5:31 pm – 7:29 am EST Response to defect within 180 minutes	24 hours
2	Urgent	The system is unavailable or a major feature of the system is unavailable to one or more users. There will be a workaround although it may not be as efficient as the application should be.	The critical difference between a Sev-1 and a Sev-2 hinges on whether the user is un-able to do work, or is able to do work	Prime Time: M-F[3] 7:30 am – 5:30 pm EST Response to defect within 90 minutes Non-Prime Time: M-F[4] 5:31 pm – 7:29 am Response to defect within 120 minutes Weekends/Holidays[4] 7:30 am – 5:30 pm EST Response to defect within 120 minutes Weekends/Holidays[4] 5:31 pm – 7:29 am EST Response to defect within 180 minutes	Anticipated within 3 Business Days, not to exceed 5 Business Days

3	Essential	A minor feature of the system is unavailable or not functioning properly for one or more users. There is no work-around although the feature is not critical.	This is used for a problem that needs to be fixed, is essential to system operation however does not impede the client from working and making meaningful progress in accomplishing primary tasks. The difference between Sev-2 and Sev-3 is the relative importance of the feature impacted.	Prime Time: M-F[3] 7:30 am – 5:30 pm EST Within 12 business hours Non-Prime Time: M-F[4] 5:31 pm – 7:29 am EST Response to defect within 2 business days Weekends/Holidays[4] Response to defect within 2 business days	Next Release Cycle or later date if approved by the State or by the LEA initiating the ticket
4	Important	A minor feature of the system is unavailable or not functioning for one or more users. There is a workaround although it may not be as efficient as the application should be.	This is used for a problem that needs to be fixed, is essential to system operation however does not impede the client from working and making meaningful progress in accomplishing primary tasks. The difference between Sev-3 and Sev-4 is the existence of a workaround solution.	Prime Time: M-F[3] 7:30 am – 5:30 pm EST Response to defect within 4 business days Non-Prime Time: M-F[4] 5:31 pm – 7:29 am EST Response to defect within 5 business days Weekends/Holidays[4] Response to defect within 5 business days	Next Release Cycle or later date if approved by the State or by the LEA initiating the ticket
5	Inquiry	Generally, a noncritical issue or a question about functionality.	This is used for questions or noncritical issues.	Prime Time: M-F[3] 7:30 am – 5:30 pm EST Within 4 business days	N/A

[1] Initial ticket or phone response from Identity Automation acknowledging incident and severity level to Designated State Representatives.

[2] Identity Automation shall provide correction or a satisfactory interim workaround to the State.

[3] Incident reported during Normal Support Hours.

[4] Incident reported outside Normal Support Hours.

Any incident arising out of or caused by an Excluded Event (as defined in Section 2.3(a)(iv)) is not subject to the requirements set forth in Table 4.3.1.

5. Reporting and Access

Identity Automation will grant NCDPI access to an electronic dashboard for the purpose of viewing data and reports on demand and entering or commenting on tickets. The metrics to be provided are described in the following section. NCDPI shall have access to review all tickets related to the NCEdCloud IAM Service.

5.1 On-Demand Dashboard

Metrics will be summarized in an electronic dashboard provided by Identity Automation, which is accessible via the Identity Automation Support Portal. This dashboard will include at a minimum the following:

- Real time view, i.e. current state of open tickets and aging analysis
- The ability to navigate through the data to review metrics and groupings of metrics
- The ability to print the current view or standard report(s) in a distributable format
- The ability to download data to offline-viewable format

5.2 Period-Based Standard Reports

The Identity Automation Support Portal will provide the State and designated PSU administrators with the ability to:

- navigate through period-based data to review metrics and groupings of metrics, including, but not limited to:
    - Time slice: first half of day, second half of day, hour, half-hour
    - Fixed: day, week, month, quarter, annual calendar, annual fiscal
- Print the report(s) in a distributable format
- Download data to offline-viewable format

5.3 Discrete Metrics to be Tracked

The following metrics will be tracked by the Identity Automation Support Portal for the purposes of reporting. All metrics, regardless of periodicity, shall be distinguishable by multiple context.

- Total ticket counts and ticket counts by Severity levels;
- Ticket summary Status: open (unresolved-working and resolved-not yet closed), closed (will not resolve and resolved), abandoned;
- By tier;
- Response time and resolution time reporting in mass and by severity.

Metric	Average	Percentage	Number
Resolution time	X		X
Response time	X		X
Ticket			X
Ticket resolution by severity level		X	X

5.4 NCDPI Access to Support Portal

Identity Automation acknowledges that the NCDPI designated users may also submit tickets on behalf of a PSU or PSUs and will have the ability to monitor the status of existing cases, submitted via all channels by the NCDPI or PSUs. Identity Automation will grant four NCDPI team members with access to all tickets/cases regardless of status. These NCPDI users will have the ability to provide comments on specific tickets in a comment field but will not have the ability to change the status or other fields in the ticket.

6. Service Level Agreements

6.1 Severity 1-3 Resolution and Account Credit

In the event that the foregoing Problem Resolution timeframes set forth in in the Severity Level Table in Section 4 for any Severity 1, Severity 2, or Severity 3 incidents are not met, due to actions or inactions reasonably within Identity Automation 's control, the NCDPI shall be entitled to remedies in the form of an account credit. This credit shall be calculated using the Current Invoice Amount, as specified in Attachment A to Amendment 5 to the Contract, and in accordance with the following:

a) Failure to meet Problem Resolution time as listed above for Severity 1, Severity 2, or Severity 3 issues shall result in per incident account credit equal to 0.5% of the applicable Current Invoice Amount.
b) Failure to provide Problem Resolution for any incident within 180 days, unless agreed to by both Parties, shall result in an account credit equal to 0.3% of the applicable Current Invoice Amount per applicable incident on a quarterly basis until such issue is resolved.

Account Credit for IA's failure to meet Severity 1, 2, and 3 Resolution timeframes is limited to 15% of the Current Invoice Amount for the applicable month.

6.2 Severity 4 and 5 Account Credit

In the event that the foregoing Problem Resolution timeframes set forth in in the Severity Level Table in Section 4 for any Severity 4 or Severity 5 incidents are not met, due to actions or inactions reasonably within Identity Automation's control, NCDPI shall be entitled to remedies in the form of an account credit. If the percentage of Severity 4 and 5 incidents is below 95%, a 2% credit will be applied to the current total scheduled contract payment amount.

6.3 Severity Level Credits

It is noted that the NCDPI is entitled to the maximum credit for each incident in accordance with the service credit calculations as noted in the SLA. However, it is also noted that a single incident, can result in only one form of credit; if warranted in accordance with service credit calculations. For avoidance of doubt, if an incident results in an outage that justifies NC receiving a credit for that outage, that same incident cannot also receive a resolution time credit as this would reflect two separate credits for a single incident.

If Identity Automation fails to meet any one of the service levels described in this SLA for two consecutive months, the total credit amount limit described in Section 2.6 shall increase to 4% for any invoice consecutively following Identity Automation's failure to meet service levels for the two preceding months.

6.4 Account Credit Reporting and Reconciliation

Identity Automation shall submit to a Designated Representative of the NCDPI a Service Level Report to accompany each invoice detailing Identity Automation's performance metrics and calculating any related applicable credits. The Service Level Report shall contain the information listed in Appendix A – SAL Performance Reporting, at a minimum.

After the current invoice and Service Level Report have been submitted to the NCDPI, the Parties shall adhere to the following procedure:

a) The NCDPI shall have ten (10) business days from receipt of Identity Automation's Service Level Report to dispute the Account Credit as reported by Identity Automation or any of the calculations or data upon which the Account Credit was based. The NCDPI shall provide reasonable details as to the reason for any dispute. Identity Automation shall have thirty (30) days to respond to such dispute.
b) Regardless of any dispute, the NCDPI shall immediately be entitled to the Account Credit as reported in the Service Level Report. This amount shall not be deemed as Disputed Account Credit.
c) Identity Automation shall apply the Total Account Credit at the time of the next payment due to Contractor under this Amendment, to include payment for any transition assistance.

Total Account Credit shall expire at the termination of the Contract or the cessation of any transition assistance provided under the Contract, whichever occurs later. Notwithstanding the foregoing, Disputed Account Credit shall not expire and must be resolved with a good faith effort by the Parties.

APPENDIX A – SLA PERFORMANCE REPORTING

Below is an example of the SLA Performance Report. Identity Automation will create an SLA Performance Report that will be provided to the State along with the next invoice indicating system performance against agreed upon Service Level Agreements.

COMMITMENT	STANDARD	ACTUAL	ACTIONS
System Availability			
System Response Time			
System Logins			
User Logins by Location			
Average Severity 1-3 Response Time			
Total Severity 1-3 Incidents			
Average Severity 4-5 Response Times			
Total Severity 4-5 Incidents			