



**New York State
Education Department**

Request for Information (RFI)

for an

Enterprise Identity and Access Management System

March 26, 2014

**New York State Education Department
89 Washington Avenue, Room
Albany, NY 12234**

TABLE OF CONTENTS

1. INTRODUCTION 1

 1.1 Organization Background 1

 1.2 PROJECT CONTEXT 2

 1.3 Proposed Functional Components for EIAM System: 4

 1.4 Education Environment Complexities 5

 1.5 RFI contact information 5

 1.6 administrative guidance for respondents 7

2. RESPONSE REQUIREMENTS 7

 2.1 RESPONSE OUTLINE and ORGANIZATION 7

 2.1.1 Cover Letter 7

 2.1.2 Company Information 7

 2.1.3 General Product Information 8

 2.1.4 Product Specifics 8

 2.1.5 Implementation and Support Services 9

 2.1.6 Pricing Model 10

 2.1.7 Pricing Estimates 10

Appendix A – Educational Organization (EdOrg) Strands 11

NEW YORK STATE EDUCATION DEPARTMENT

Enterprise Identity and Access Management (EIAM) System

Request for Information

The New York State Education Department (NYSED) hereby issues this “Request for Information” (RFI) to determine system capabilities with respect to NYSED’s EIAM System needs.

1. INTRODUCTION

1.1 ORGANIZATION BACKGROUND

The New York State Education Department (NYSED) is responsible for oversight of all educational institutions in the state, for operating certain educational and cultural institutions, for certifying teachers, and for registering and licensing practitioners of more than 40 professions. NYSED’s supervisory activities include chartering all educational institutions in the state, including schools, libraries, museums, and historical societies; accrediting college and university programs; allocating state and federal financial aid to schools; and providing and coordinating vocational rehabilitation services.

A Board of Regents, consisting of 17 members elected by the state legislature, governs NYSED. The Board oversees the University of the State of New York (USNY), consisting of all public and private schools, colleges and universities, chartered libraries, museums, historical societies, and other educational institutions in the state. NYSED’s chief executive officer is the Commissioner of Education and President of the University, who is appointed by the Board of Regents.

NYSED is composed of these major organizational areas:

- Office of P-12 Education
- Office of Higher Education
- Office of Cultural Education
- Office of Counsel
- Office of State Review
- Office of Professions
- Adult Career and Continuing Education Services
- Office of Operations and Management Services

The Office of P-12 Education has primary responsibility within NYSED for measuring student performance and implementing accountability measures in schools. This office plays a central role in the collection, management, and reporting of educational data. The P-12 website contains additional information on the programs, services, and organization of that office, including information about current educational data collection and reporting.

(<http://www.p12.nysed.gov/offices.html>).

Public school districts and charter schools are known as Local Educational Agencies (LEAs) in New York State. These LEAs are responsible for administering and operating the individual public schools within a district.

A complete description of the University of the State of New York and the State Education Department can be found at <http://usny.nysed.gov/about/>.

1.2 PROJECT CONTEXT

NYSED aims to implement a robust EIAM system, which would provide secure authentication (verifying identity) and authorization (approving and providing access to services) for several groups of stakeholders including:

1. NYSED employees and agents
2. Constituents of the P-12 public education system in NYS including:
 - a. Educators, school leaders, district administrators, etc.
 - b. Parents/Guardians and students
3. Vendors conducting business with NYSED
4. Other constituents (e.g. professionals doing business with NYSED's Office of the Professions)

Existing systems that either provide identity and access management capabilities or are protected by such capabilities include identity directories, authorization systems and end-user applications and include:

- Active Directory (AD). This is the directory behind the new EngageNY Portal.
- Oracle Internet Directory (OID)
- New York State Directory Services (NY.gov ID – see <https://my.ny.gov/>)
- SEDREF (State Education Department Reference File) - NYSED source system for core identifying information on institutions. Provides unique ID for all Institutions and all educational organization relationships, except NYC Network-to-School.
- TEACH - Source system for all NYS and NYC teachers who are certified (and typically fingerprinted) for work within New York State schools.
- TAA (Teacher Authentication and Authorization) - TAA PIN Process is used to associate a teacher to multiple locations and/or multiple LEAs and also to her OID account with association via the unique identifier, the TEACHID.
- EngageNY Portal Identity Provider- Authenticates and federates identity information to applications within the Portal.
- Engage NY Portal 2.0 and applications (new- see description below)
- American Recovery and Reinvestment Act (ARRA) Reporting System
- BEDS-IMF-School Safety (VADIR/DASA) Application
- Information and Reporting Services Portal (IRSP)

- Mandated Services Aid (MSA)
- Title One
- New York State Student Identification System (NYSSIS)
- Examination Request System
- OSA Report Generator
- State Aid Management System (SAMS)
- State Education Department Delegated Account System (SEDDAS)
- Monitoring and Vendor Performance System (MVPS)
- State Education Department Reference File (SEDREF)
- High School Equivalency Diploma (HSED)
- Impartial Hearing Reporting System (IHRS)
- Level 2 Reporting (L2RPT)
- L0 Historical View and Update
- Growth Reporting System (GRS)
- Teacher Certification (TEACH)
- Comprehensive Special Education Information System (CSEIS)
- Higher Education Data System (HEDS)
- Library Development Grants (LDGRANTS)

Initially, the implementation of an EIAM system at NYSED will focus on migrating technologies that support the EngageNY Portal program. The Portal offers a secure single sign-on (SSO) environment for role-based access to data dashboard and content management applications to educators, students, and their guardians.

This RFI seeks information regarding possible solutions that would replace the existing IAM supporting the Portal and will later provide a foundation for identity management, federation, authentication and authorization, and application on-boarding services needed to support business needs across the agency and with additional stakeholders and constituents.

The IAM solution is intended to support NYSED as well as locally (e.g. LEA, BOCES, RIC etc.) sourced or built applications and should be capable of integrating with emerging student record APIs and leveraging a statewide ID system (NY.gov ID – see <https://my.ny.gov/>)

NYSED is interested in the possibility of being able to support federation e.g. with NYC and/or multiple districts / BOCES-Regional Information Centers (RICs) who might in the future wish to integrate their own directories or IDPs.

To support the Portal the EIAM system must service approximately 2.9 million students, 5.8 million guardians (of NYS public school students), and 200,000 educators in various educational organizations spanning New York State. The EIAM solution must be fully developed (or configured), tested, and deployed to users by September 1, 2015.

1.3 PROPOSED FUNCTIONAL COMPONENTS FOR EIAM SYSTEM:

EIAM Category	Key Functional Components (high level)
Central User Repository (Directory) and Services	<ul style="list-style-type: none"> • Maintain integrated view of all statewide orgs, e.g., NYSED, BOCES, RIC, LEA, District, CMO, etc. See Appendix A • Central user repository and associated account information (directory); <u>note</u> - solutions should have the capability of leveraging the NY.gov ID services or synchronize/federate identity (password synchronization) data to NY.gov ID. • Act as an identity provider to SED service providers • Supports federated identity management
Authentication	<ul style="list-style-type: none"> • Single sign-on services and policies • Session management • Password services • Strong authentication
Authorization	<ul style="list-style-type: none"> • Collection, maintenance, and movement of authorization data sets between multiple data stores and a central data repository via open and standard protocols (e.g. SIF, web services, APIs) • Maintain role and relationship information for users provisioned in the system • Application of business logic to determine role-based access controls • Application of privileges at the application and data levels (e.g. which applications can be accessed by which users, what type of data can be viewed, entered, or modified by which users, etc.)
User and Access Management	<ul style="list-style-type: none"> • Delegated administration of role assignment • User and role management (e.g. associating a user with multiple roles and associated educational organizations) • Provisioning • Password management • Self Service
Application On-boarding to a SSO Environment	<ul style="list-style-type: none"> • Support SSO and provide role and access control data to service providers (e.g., application vendors) in real time • Development and management of relationships between applications, users, and their roles within each application • This catalog of relationships, combined with federation services, enables users to access a wide variety of applications through a single sign-on experience
Identifier Generation	<ul style="list-style-type: none"> • Support creating, assigning, and maintaining unique, statewide identifiers for students, their legal guardians, and school/district staff members within NYS. • Unique identifiers for each group must be unique, non-changing, and non-duplicative.
Middleware messaging and education-specific data storage.	<ul style="list-style-type: none"> • The current implementation will incorporate data synch using SIF 3.0 brokerage services. This broker will receive updates from external entities, update internal information and publish updates back to external entities. This includes traditional identity information, but also includes education-centric data such as educational organization (EdORg) that is used to make

	authorization decisions. See https://www.sifassociation.org/Resources/Developer-Resources/SIF-3-0/Pages/SIF-3.0-Infrastructure.aspx .
--	--

Table 1: EIAM System Functional Components

1.4 EDUCATION ENVIRONMENT COMPLEXITIES

Criteria used to make access decisions in the EngageNY Portal are complex. User Roles, Educational Organization membership and Context define the scope and type of data that a user can access:

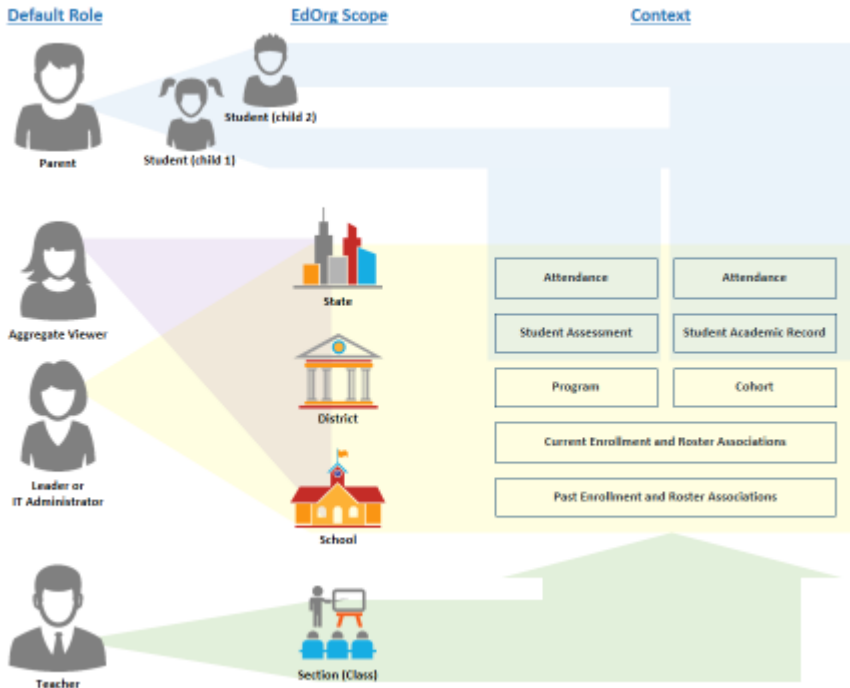


Figure 1- Basis of Effective Permissions

NYSED defines User Roles and associated permissions for student record access management. The IAM solution is expected to manage these roles within the context of the EdOrg hierarchy (see Appendix A for more information on EdOrg hierarchies).

1.5 RFI CONTACT INFORMATION

Interested Entities are encouraged to submit a written “Letter of Interest,” including a cover letter on company letterhead, characterizing their interest and background. Information pertaining to ideas, concepts, design issues, and practical knowledge gained from relevant experiences implementing EIAM solutions is being sought. Additionally, responses to the questions and inquiries listed in Section 2 are requested. NYSED may, at its discretion, invite interested entities to visit its offices at 89 Washington Avenue, Room, Albany, New York, for further discussions.

Note: This IS NOT a Request for Proposals. It is an invitation to provide the NYSED with information regarding current technologies and viable approaches to implementing an Enterprise Identity and Access Management System. Additionally, responses will be used to gauge the level of interest in the EIAM Project. Information obtained may be used to develop a needs requirement upon which a future procurement might be based. If further discussion is required, or should questions arise, please contact the NYSED contact person listed below.

Participation in this RFI is voluntary, and NYSED will not pay for the preparation of any information submitted by a respondent or for NYSED's use of that information.

Vendors are advised that if any part of their response to this RFI contains trade secrets or is submitted to NYSED by a commercial enterprise or derived from information obtained from a commercial enterprise and which, if disclosed, would cause substantial injury to the competitive position of the subject enterprise, then vendors should identify such in their response.

Mail or E-mail Letters of Interest To:

US Mail:

New York State Education Department
Contract Administration Unit
Room 501 W EB
89 Washington Avenue
Albany, NY 12234
Attention: Enterprise Identity and Access Management System RFI

E-mail:

iamrfi@mail.nysed.gov

Respondents who mail their "Letter of Interest" are requested to provide an electronic copy in MS Word or PDF Format. These formats are also required for E-mail submissions.

NYSED Contact Person:

All questions regarding the Enterprise Identity and Access Management System RFI must be submitted in writing, via E-mail, to:

Adeline Jebaraj
E-mail: iamrfi@mail.nysed.gov

Questions pertaining to this RFI are due by April 7, 2014. Answers to questions will be posted by April 14, 2014 to the following web address:
<http://www.p12.nysed.gov/comprcontracts/comprcontracts.html>

NYSED may issue announcements amending this RFI in response to vendor questions. In addition, after reviewing RFI responses, NYSED may request clarifying information from vendors who offer information of specific interest to NYSED.

1.6 ADMINISTRATIVE GUIDANCE FOR RESPONDENTS

RFI schedule:

March 26, 2014	RFI published
April 7, 2014	Deadline for questions
April 14, 2014	Response to questions issued
April 28, 2014	Deadline for receipt of responses

2. RESPONSE REQUIREMENTS

2.1 RESPONSE OUTLINE AND ORGANIZATION

Responses should be organized as follows:

2.1.1 Cover Letter

The respondent should provide a cover letter (limited to no more than two pages in length) that includes the following corporate information:

- Company Name
- Contact Name
- Title
- Phone #
- E-mail address
- Mailing address
- Fax #

Note: Provide additional contact persons as needed.

Respondents should also provide the following information:

- Whether the company is publicly or privately held (if public, provide company symbol)
- Number of full-time employees

2.1.2 Company Information

The vendor shall summarize its experience in the Enterprise Identity and Access Management systems field. An indication of the extent and scope of the experience should be provided, including:

- Length of time your company been providing Enterprise Identity and Access Management systems
- Prior Enterprise Identity and Access Management systems design or implementation work you have performed with other educational entities, including the dates of this work
- Contacts in educational entities that you have worked with
- The role of your company in these engagements (e.g., primary or sub-contractor)
- The project phases in which your company participated
- The environments in which the systems were implemented

- Any partnerships or alliances your company has that would provide benefits to the project

Based on the experience outlined above, vendors should identify the following:

- Lessons learned from past implementations regarding analysis, design, development, testing, deployment, and training tasks
- General implementation time frames from previous efforts
- What your company believes is its competitive advantage

2.1.3 General Product Information

Company literature and brochures describing Enterprise Identity and Access Management products may be included as part of the response. While additional information links are not disallowed, NYSED prefers not to receive links wherein pertinent information is available but requires extensive searching.

Product information should include:

- Overview of how the product works (including a system overview diagram). Transparency is desirable. The system needs to be explainable rather than a “black box.”
- What are the hardware and software requirements for using the product?
- What is the current version of the product? Are any major releases currently planned?
- Is the product proprietary or open source?
- Is the product typically hosted by the vendor (or a third party) or installed in-house?

2.1.4 Product Specifics

1. Is the solution internal or cloud based? If internal, what additional software and hardware would SED require if your proposed EIAM solution was adopted?
2. How does your proposed solution provide the following services?
 - Provisioning and de-provisioning of user accounts
 - Provisioning and de-provisioning of credentials
 - Provisioning and de-provisioning of access rights
3. What is the EIAM architecture of your proposed solution? Provide a complete description of each major component, its purpose and role in the overall solution.
4. How does your proposed EIAM solution ensure that any identity-management model can be expandable to include new forms of identity verification and assertions?
5. How would your product migrate the current EngageNY Portal catalog/authorization data into your solution?
6. How would you migrate IAM business rules into your product? How does your proposed solution implement the administration of accounts and access rights? Does the solution allow for centralized and delegated approaches?
7. Which web SSO systems does your proposed EIAM solutions support and interoperate with?
8. Describe how your proposed solution enables decisions about access to information resources to be made and administered by the owner of the resource. This includes

determinations of levels of access to be granted to specific users, to specific roles to which users may be assigned, or both.

9. What audit, logging and reporting capabilities does the EIAM solution support?
10. Describe how your proposed EIAM solution can support and is compliant with the NYS Identity Trust Model (<http://www.cio.ny.gov/policy/NYS-P10-006.pdf>).
11. What organizational structure / roles / responsibilities are recommended for managing the proposed EIAM solution after implementation?
12. Has your EIAM solution been used for other K-12 Educational applications or portals?
13. Do you have a recommended Reference Architecture for your EIAM solution and could you provide NY SED with a copy?
14. Describe how your EIAM solution supports creating, assigning, and maintaining unique, statewide identifiers for students, their legal guardians, and school/district staff members.
15. How does your product enable management of organization data including:
 16. Creation, reads, updates, and deletion of organizational entities and attributes
 17. Management of relationships between organizations (e.g., schools to networks, districts to BOCES, Course Section to School, etc.)?
 18. What interfaces does your product include for managing these data (e.g., UI, APIs, messaging services, standards, and protocols, etc.)?
- 19.
20. How does your product enable management of relationships between people and organizations (e.g., staff to LEA, teacher to course section, student to course section)? What interfaces does your product include for managing these relationship data (e.g., UI, APIs, messaging services, standards, and protocols, etc.)?
21. How does your product enable management of relationships between people (e.g., parent or guardian to student)? What interfaces does your product include for managing these data (e.g., UI, APIs, messaging services, standards, and protocols, etc.)?
22. Does your product support SIF 3.0 as a data transport and data format mechanism, or would you recommend different standards for data messaging and/or for the standardized format of education-specific data for use with your product(s)?

2.1.5 Implementation and Support Services

Include information about how you would typically provide support both during and after implementation. Include information on the following:

- Implementation Services
 - Project Management
 - Detailed Requirements Gathering and Analysis
 - System Design
 - System Construction or Configuration
 - Integration and Testing
 - Documentation
 - Application Warranty Services
 - Training

- Recurring (Annual) Services
 - Hosting
 - Application Maintenance, Technical Support and Help Desk Services

Describe options on how independent a customer is after implementation:

- What aspects of support of the product are expected to be covered by NYSED's functional and IT staff versus what is expected to be handled by your company?
- What are the business and IT resources required in our organization to support the product after implementation?

2.1.6 Pricing Model

Include information about your pricing model for the product:

- Do you charge a software licensing fee?
- Do you charge by user, by server, by district?
- Do you negotiate state-wide agreements with state educational authorities?
- Do you offer a perpetual license agreement?
- How are ongoing maintenance charges assessed?

2.1.7 Pricing Estimates

Include ballpark estimates for the following scenarios:

- Fixed price estimate for a one-time implementation
- Pricing estimates for 5-year, 10-year, and perpetual licensing
- Pricing estimates for maintenance, technical support, and Help Desk Services to operate the solution
- Any discounts that would be applicable

Appendix A – Educational Organization (EdOrg) Strands

The following illustrates the current NYSED representation of the various education organizational hierarchies within New York State and New York City. Note that Course and Section objects on the diagram are part of the hierarchy.

An EdOrg “Strand” represents hierarchical relationships among educational organizations. A Strand is a collection of organizational types (“EdOrg Type”) that have some thematic, political, pedagogical, financial, or geographic association recognized by the state education system. EdOrg Types share common identifiers and classification as well as the same attributes used to track them or used to describe them.

The following Strands are illustrated below:

- Strand 1: Standard New York State Big 4
- Strand 2: Standard New York State BOCES
- Strand 3: New York City
- Strand 4: Charter Schools
- Strand 5: Virtual BOCES
- Strand 6: Schools for the Deaf & Blind

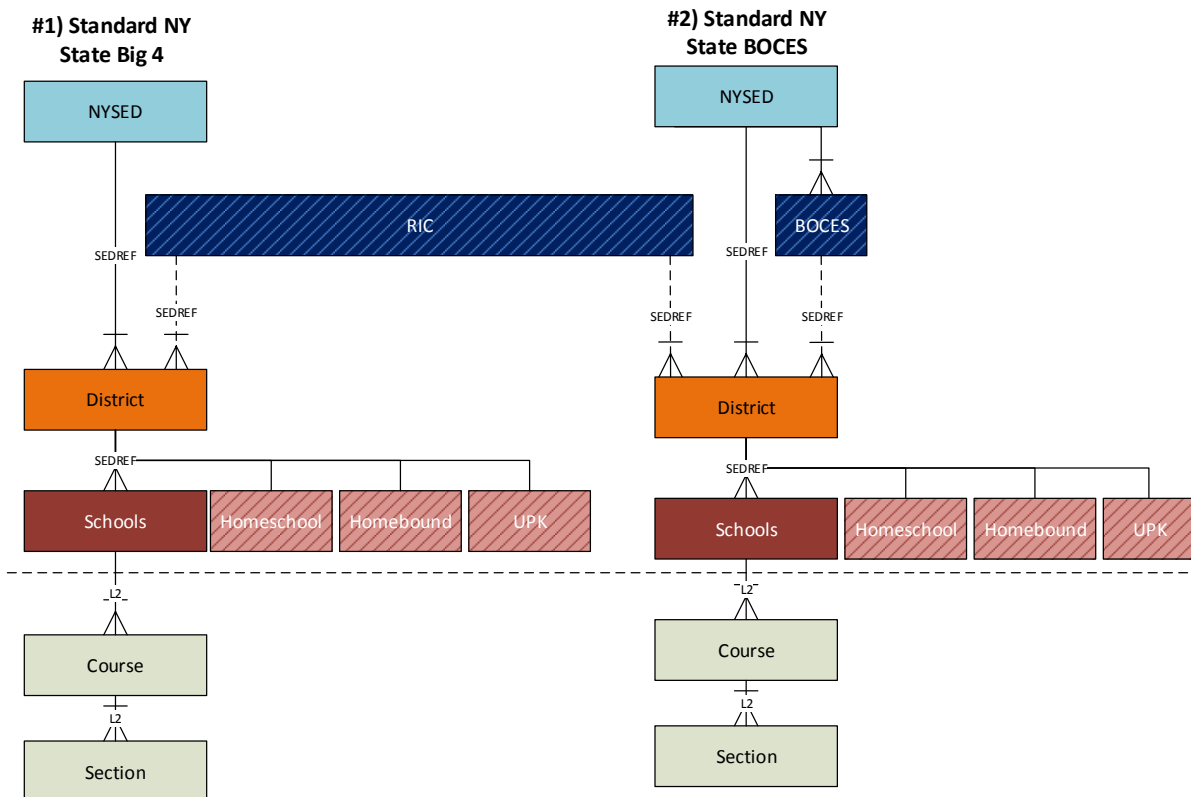


Figure 1 - NY Big 4 and BOCES Hierarchies

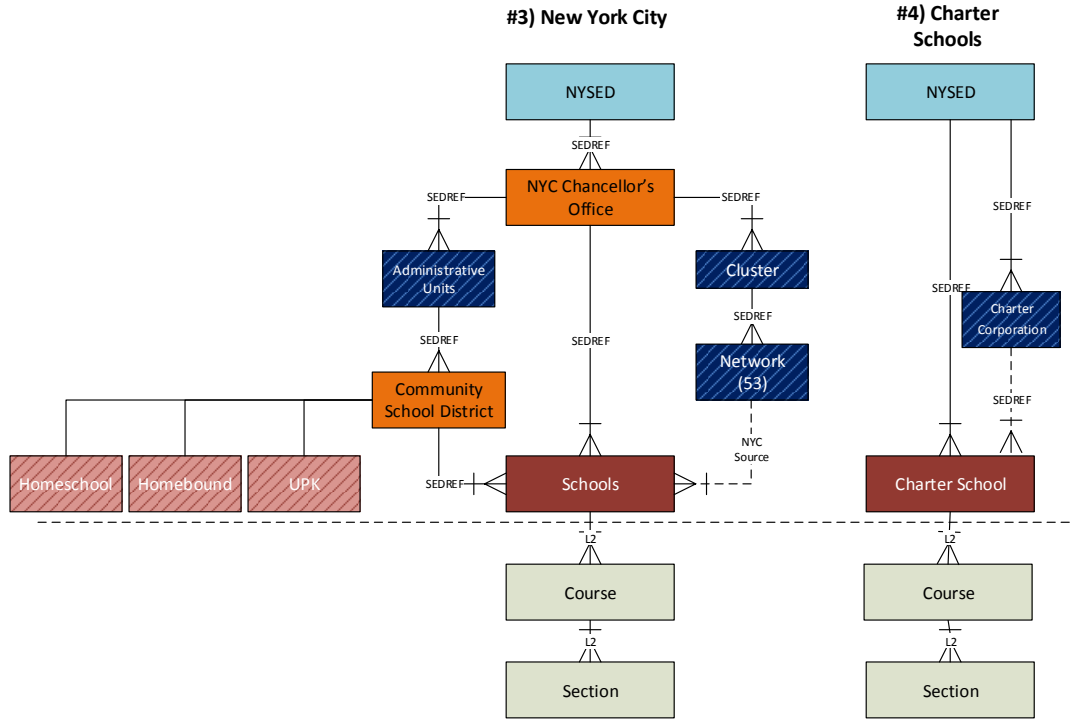


Figure 2 - NY City and Charter School Hierarchies

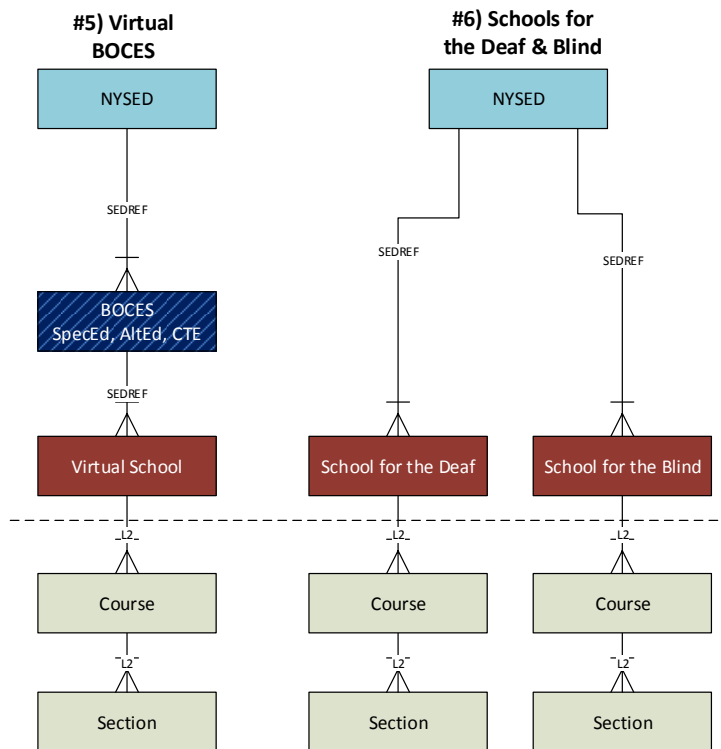


Figure 3 - Virtual BOCES and Schools for the Deaf and Blind