# STATE OF NEW YORK

# IT Transformation

## Request For Information (RFI) Enterprise Identity and Access Management

The New York State Office for Information Technology Services (ITS) is coordinating responses to this RFI on behalf of the Division of Budget (DOB) and the IT Transformation Program. This RFI is posted on the ITS website:

http://www.cio.ny.gov
**Issued: May 25, 2012**

**Submission Deadline: June 27, 2012, 12:00 PM ET**

All contacts/inquiries shall be made by email to the following address:
ITTransformation.eiamservices@cio.ny.gov

# Table of Contents

Appendices:

# 1.0 Introduction

## 1.1 Purpose of this Request for Information

New York State (the “State” or “NYS”) is issuing this Request for Information (RFI) to gain a better understanding of the current industry best practices and vendor capabilities in the Identity and Access Management (IAM) environment. Specifically, NYS is seeking information from vendors on approaches and architectures for the implementation of an Enterprise IAM (EIAM) solution that meets the needs of the State, but also leverages IAM investments already made by the State, as well as the mature and robust solutions present at the agency level. NYS understands fully that when constructing such a system, the workflow, business processes and human-acceptance factor are just as important as the technical solution deployed. Because large EIAM solutions can be challenging to implement, NYS is also seeking vendor responses on their experiences and successes with similarly sized projects for other clients. The information received from this RFI could be used to issue a Request for Proposal (RFP) for the procurement of EIAM solutions or services and also contains preliminary information to serve as a platform for reaction and discussion with the vendor community. This issuance does not constitute a commitment to issue a bid, or award a contract, or to pay any costs incurred in preparation of a response to this request.

## 1.2 IT Transformation Program

Governor Andrew Cuomo announced in his Budget Address of 2011 that the State of New York (NYS) can no longer afford to perform business as usual. This announcement led to the initiation of a massive effort to transform the way NYS performs business and provides goods and services to its citizens. A major piece of this effort is to transform the delivery and consumption of information technology. To satisfy this, the IT Transformation Program was initiated last year. Since that time, the State has engaged Subject Matter Experts (SMEs) to benchmark New York’s IT environment and identify ways to deliver government services more efficiently and effectively to all its consumers. EIAM was identified as a high-priority opportunity. For the purposes of this document, EIAM is defined as a statewide IAM solution that includes, but is not limited to, the following areas described in fuller detail in Section 2.4.1:

- Identity Management
- Credential Management
- Access Management
- Federation
- Auditing and Reporting
- IAM Governance

# 2.0 Enterprise Identity and Access Management

## 2.1 EIAM Overview

Several NYS Agencies already use identity and access management processes and related tools to manage access to their information assets and services. Although there have been some successful NYS IAM initiatives, existing solutions are not robust enough to meet current or future enterprise-wide IAM needs. The State's approach, therefore, is to establish an EIAM shared services solution that satisfies its unique business, functional, and technical needs, without disrupting the daily operations of already established IAM applications and solutions that are deemed successful and will continue to run for the near future. Planning for a smooth transition, while considering integration and interoperability, is essential.

The NYS EIAM project is dedicated to improving identity and access management for citizens, government business partners and government employees in conducting online state business and to deliver automated, integrated, efficient, secure, and compliant services and tools that can be utilized to manage user's identity and access capabilities. Access decisions will be based in part on the relationship between the user and the State and trust in the identity relevant to the nature of information being accessed. To that end, NYS is seeking an innovative framework and approach for individuals and organizations to securely access government services. This includes the implementation of a federation model for authentication and authorization, the establishment of a robust statewide directory, enabling single-sign-on (SSO) capability for State employees, self-registration capabilities for internal and external users, developing strong authentication capabilities, enacting FIPS 201 (Federal Information Processing Standard Publication 201) compliant credentialing that will support future convergence of logical and physical access, and developing advanced auditing and reporting capabilities. The desired outcome is the ability for individuals to engage and transact with the State government online, and for business users to do business with the State through a robust set of secure administrative functions.

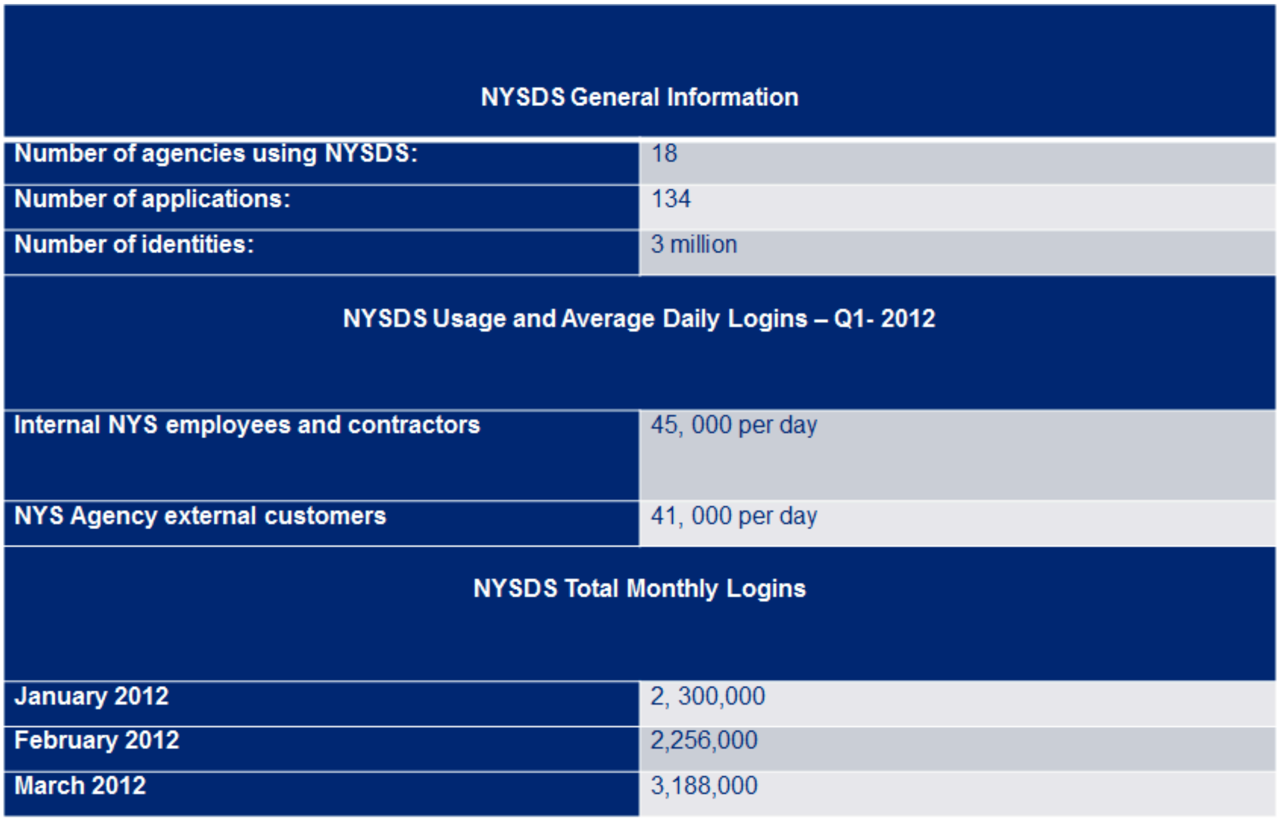
The proposed solution should be based on the Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0 (and other guidance listed in Appendix A) while meeting the strategic imperatives listed below:

- ✓ Improve ability to conduct business on-line and in a secure fashion;
- ✓ Provide a secure EIAM solution that reduces risks of data breaches and identity theft;
- ✓ Increase operating efficiency and reduce operating costs;
- ✓ Enhance auditing and regulatory compliance, and;
- ✓ Enhance ability to prevent fraud and reduce security risk.

## 2.2 Current Environment

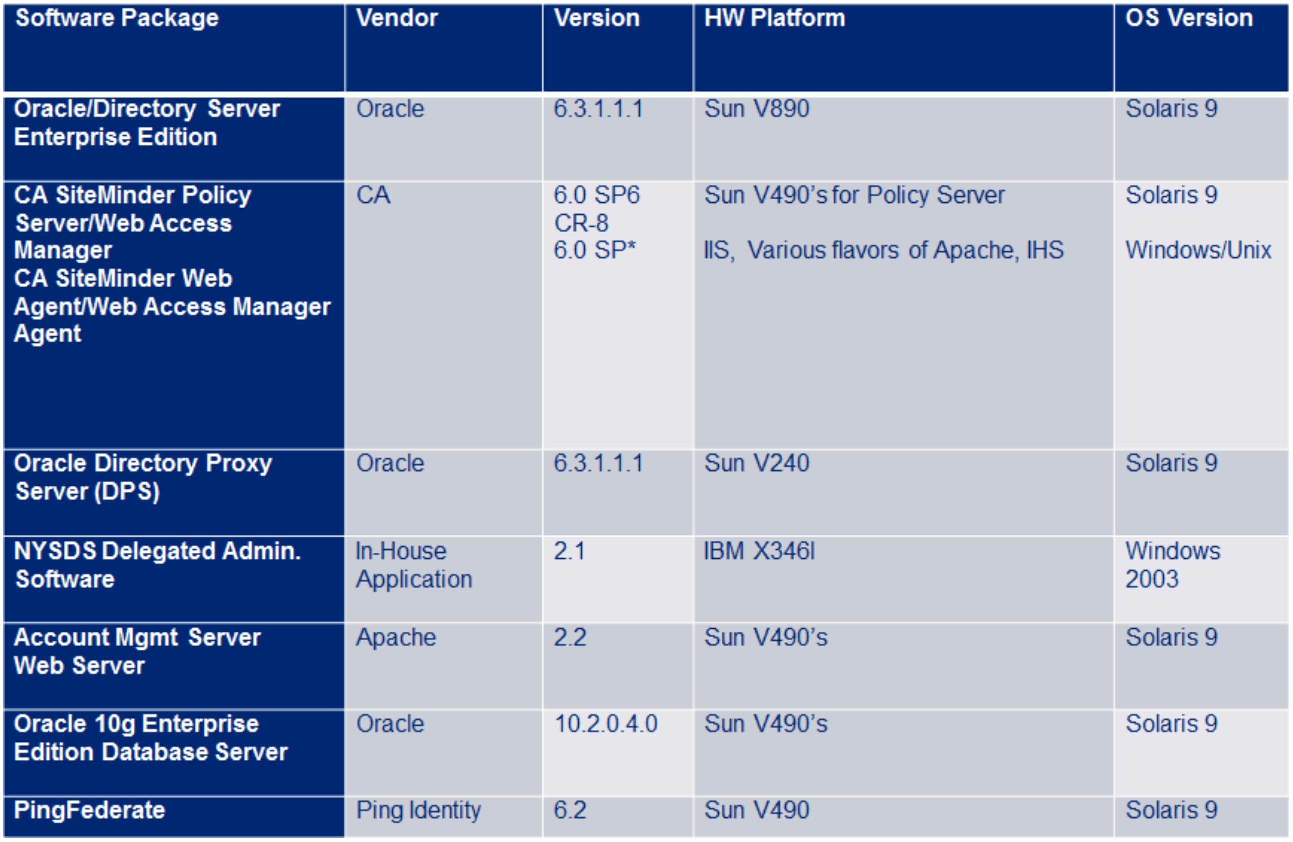
Today, the State manages and maintains the New York State Directory Services (NYSDS) system which is branded NY.gov (http://www.cio.ny.gov/directory_services). The identification is a loosely coupled shared service offering comprised of best of breed technologies such as LDAP (Lightweight Directory Access Protocol) directory services, web-based Single Sign On (SSO) access management, and standards-based federation. The NYSDS is currently supporting more than 3 million users and over 130 applications across many state agencies. It has the capability to assert NY.gov-branded online credentials to relying parties as well as consume credentials from trusted identity providers.

For over a decade, NYS has managed NYSDS as a central authentication infrastructure that employs a delegated administration capability for user provisioning and course-grained authorization control. Over the past several years, NYS has expanded the NY.gov ID system that allows for sharing of identities to enhance an application's ability to maintain fine-grained authorization information. These on-going enhancements continue to limit the need for agencies within NYS, which are performing identity and access management functions internally, to rely on these silo systems and to be able to open their systems to the broader NYS identity environment. Tables 1 and 2 below depict the recent statistics on NYSDS as well as an outline of the software and platforms associated with NYSDS, respectively.



| NYSDS General Information | |
|---|---|
| Number of agencies using NYSDS: | 18 |
| Number of applications: | 134 |
| Number of identities: | 3 million |
| NYSDS Usage and Average Daily Logins – Q1- 2012 | |
| Internal NYS employees and contractors | 45, 000 per day |
| NYS Agency external customers | 41, 000 per day |
| NYSDS Total Monthly Logins | |
| January 2012 | 2, 300,000 |
| February 2012 | 2,256,000 |
| March 2012 | 3,188,000 |

*Table 1 - Note: NYSDS usage and growth of customer base is directly related to NYS Agency customer application peak periods of use.*



| Software Package | Vendor | Version | HW Platform | OS Version |
|---|---|---|---|---|
| Oracle/Directory Server Enterprise Edition | Oracle | 6.3.1.1.1 | Sun V890 | Solaris 9 |
| CA SiteMinder Policy Server/Web Access Manager<br>CA SiteMinder Web Agent/Web Access Manager Agent | CA | 6.0 SP6 CR-8<br>6.0 SP* | Sun V490's for Policy Server<br>IIS, Various flavors of Apache, IHS | Solaris 9<br>Windows/Unix |
| Oracle Directory Proxy Server (DPS) | Oracle | 6.3.1.1.1 | Sun V240 | Solaris 9 |
| NYSDS Delegated Admin. Software | In-House Application | 2.1 | IBM X346I | Windows 2003 |
| Account Mgmt Server Web Server | Apache | 2.2 | Sun V490's | Solaris 9 |
| Oracle 10g Enterprise Edition Database Server | Oracle | 10.2.0.4.0 | Sun V490's | Solaris 9 |
| PingFederate | Ping Identity | 6.2 | Sun V490 | Solaris 9 |

*Table 2*

NYS' existing IAM environment consists of many agency specific solutions as well. In general, these are silo business processes designed to accomplish similar goals and objectives. Currently there are at least 7 separate user authentication repositories and over 20 user provisioning tools in use within 14 different NYS agencies. There is limited integration with agency applications for user provisioning and there are many "Commercial off the Shelf" (COTS) and homegrown tools providing functionality to manage user access across the various state entities. However, despite this, there are agencies that have more mature IAM functionality in their applications which the State in interested in leveraging. For example:

**Department of Motor Vehicles' (DMV) MyDMV** - provides individuals with on-line services such as:

- Change My Address
- Get My Driving Record Now
- Paperless Reminders for Inspections and Registration Renewals
- Request Restoration After a Revocation

This application currently has approximately 525,000 individuals registered and approximately 2000 registrations are expected per day, resulting in a growth of over 3 million in a 5 year period. Characteristics of the IAM components within this application are:

- It is hosted by DMV but leverages the ITS mainframe

- NYSDS is the authentication repository
- CA eDirectory is used as the authorization repository
- Users get created with a single role stored in the CA eDirectory.
- NYS trust level 2 is used for vetting individuals for the first time
- ITS password rules are enforced
- NYSDS Global Unique Identifier (GUID) is used for the registered users
- There is a 2 year dormant account policy for individuals in NYSDS
- CA Identity Manager is used to provision to NYSDS using web services (TEWS, DAWS)

**Department of Tax and Finance (DTF) OLS (OnLine Services)** - provides individuals with on-line services such as:

- Change My Tax Address
- File my Tax Return (Sales tax, MTA, Withholding Tax, etc)
- Protest my filing
- Administer my account
- Secure emails for bills and notifications
- Make payments
- 80 transactions in all

This application is the cornerstone to NYS Tax web filings. Over 80% of all businesses filed electronically last quarter through this solution (over 75,000 in just one day). There are currently 1.2 M registered taxpayers in the system ( 570,000 Individuals, 614, 000 business, 10,000 Tax professional) and upwards of 160,000 have signed on and done work in a single day. This year alone 3.1 million web transactions have been processed online and taken in $9B in payments. The growth of taxpayers supported could be dramatic adding around 5M individuals in the next two years through integration with software providers. Characteristics of the IAM components within this application are:

- NYSDS is the authentication repository
- It is hosted by DTF
- Commerce is the fine grained delegation and authorization repository
- Attribute based security no role based
- Currently a NYS trust level 1
- ITS password rules are enforced
- OLS systems are userid, not GUID based
- There is a 2 year dormant account policy for individuals in NYSDS
- OLS integrated with NYSDS through secured web services to create and maintain accounts.

Embarking on an enterprise project of this magnitude, however, requires a baseline of current statewide investments in EIAM. As a result, an asset inventory of EIAM products was conducted late last year. Table 3 below depicts a high level summary of the State's current EIAM investments as well as areas in which the State does not own any products. Solutions that leverage these investments and proposals that integrate these various components are encouraged and welcomed.

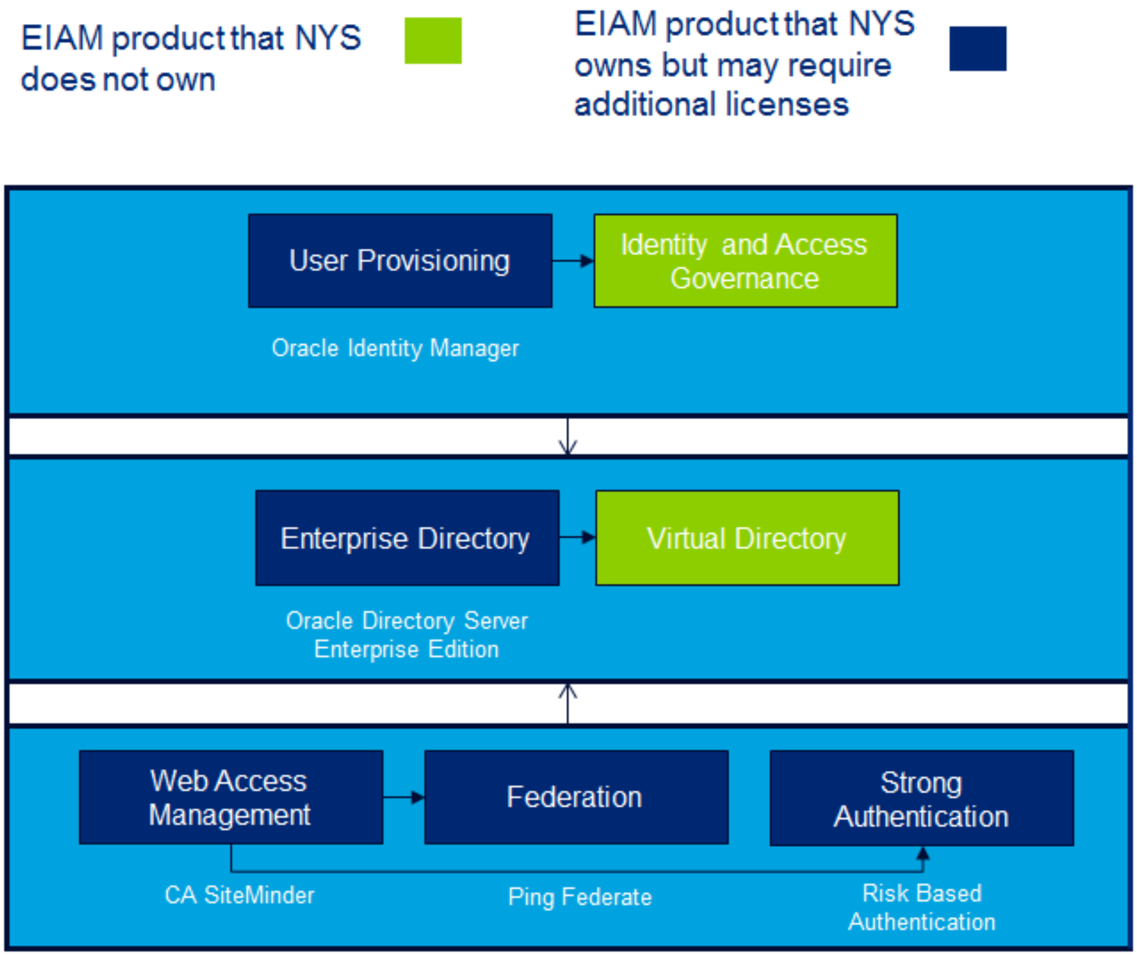
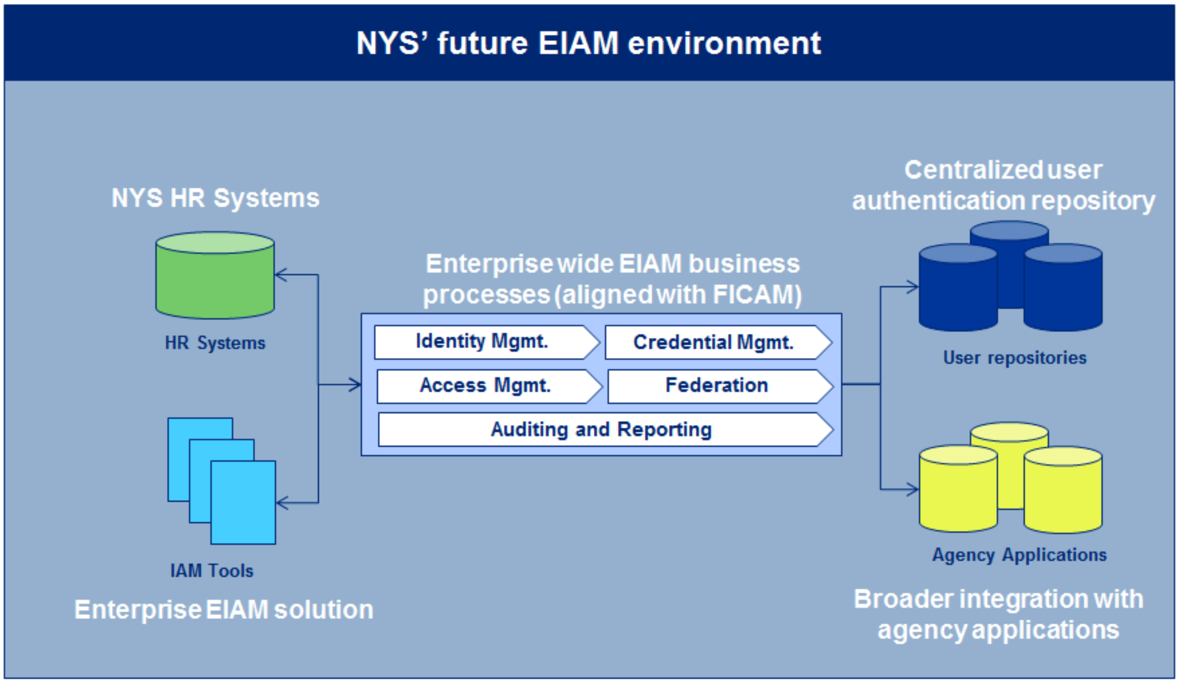

EIAM product that NYS does not own 🟩
EIAM product that NYS owns but may require additional licenses 🟦
User Provisioning
Identity and Access Governance
Oracle Identity Manager
Enterprise Directory
Virtual Directory
Oracle Directory Server Enterprise Edition
Web Access Management
Federation
Strong Authentication
CA SiteMinder
Ping Federate
Risk Based Authentication

*Table 3 - Note: Arrows indicate known dependent integration points*

## 2.3 Future Environment

New York State is interested in identifying how to improve the existing IAM environment. Ideally, NYS would like to build on and leverage investment already made in a variety of IAM products. Past IAM expansion efforts such as establishing the NYS Identity Trust Model (http://www.cio.ny.gov/policy/NYS-P10-006.pdf) developing the technical architecture, and building federation capabilities has provided the State with the necessary foundation to move forward, and enhance, integrate and implement new technology solutions. NYS' future vision is depicted below:

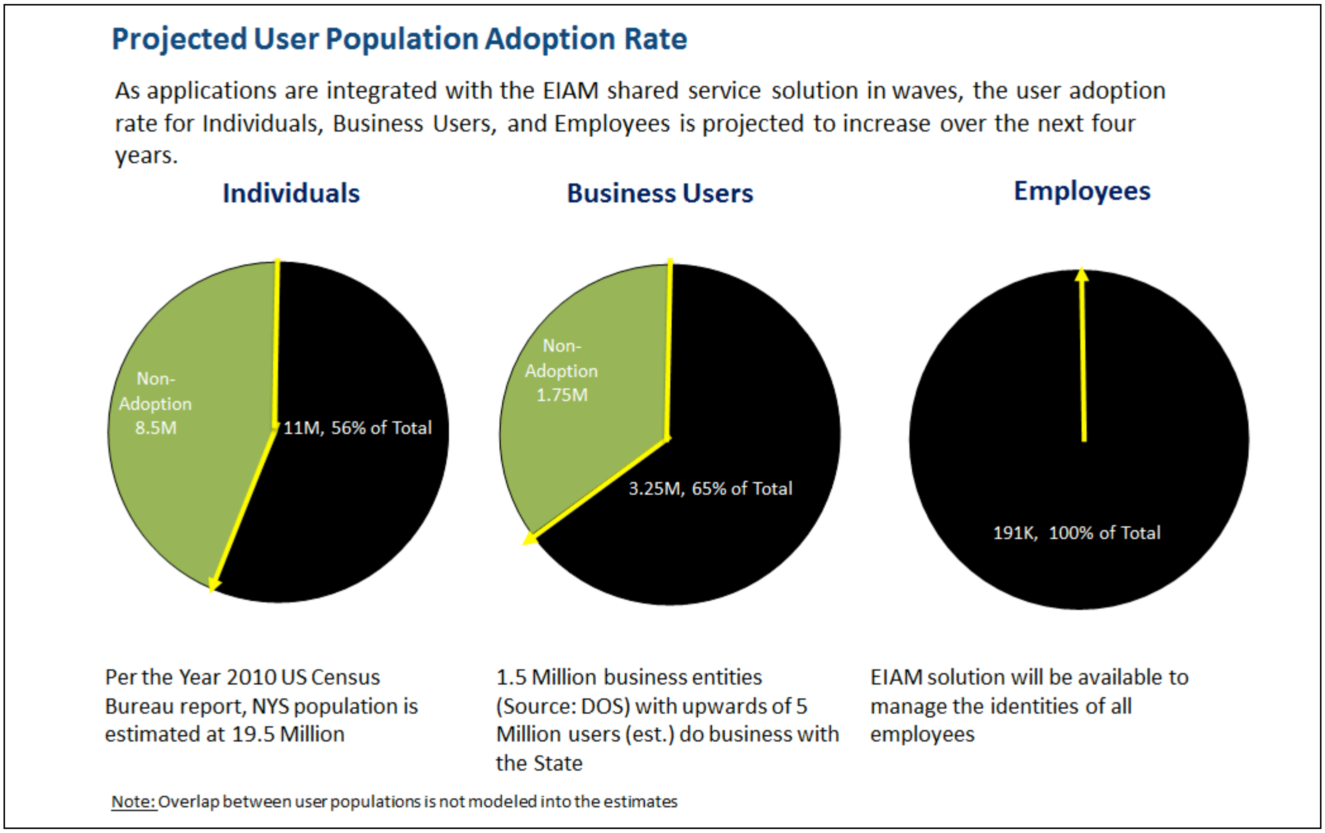
NYS' future state EIAM shared services environment is based upon standardized business processes that align with the ICAM model and national standards, and a NYS approved reference architecture.


NYS' future EIAM environment
NYS HR Systems
HR Systems
IAM Tools
Enterprise EIAM solution
Enterprise wide EIAM business processes (aligned with FICAM)
Identity Mgmt.
Credential Mgmt.
Access Mgmt.
Federation
Auditing and Reporting
Centralized user authentication repository
User repositories
Agency Applications
Broader integration with agency applications

NYS EIAM solution is expected to deliver key business outcomes that align with the strategic imperatives. There are ten driving business objectives that are the cornerstone of the EIAM transformation project. They are:

1. Provide agencies with a standards based approach to support key identity and access management functions (e.g. identity proofing) and cross-agency identity data sharing, without disrupting daily business operations.
2. Provide central user interface that provides a self-service, streamlined approach in which end-users (internal and external) register and connect with agency services.
3. Improved user experience by having a single place to register and access state services online for citizens.
4. Enhance user experience and reduced risk by reducing number of user ID's and passwords for users to access EIAM integrated applications.
5. Reduced risk by enabling real-time alerting and reporting of identity and access related security events via a Security Information and Event Management (SIEM) solution.
6. Timely granting of access to basic agency services and revocation of access privileges upon termination for employees.
7. Increased operating efficiency and reduced risk by standardizing physical access credentials and the process to manage them.
8. Lower help desk and human resource costs by reducing the number of accounts for a user, enabling single sign-on, and providing self-service options.
9. Reduced risk of fraud by deploying fraud prevention/detection and strong authentication solutions
10. Reduced support costs by starting to retire legacy IAM solutions where effort is duplicated with shared service solution.

The projected adoption rate and the ability to meet these objectives are crucial when considering a practical, feasible, and viable EIAM solution. Please see the diagram below which depicts the goals of NYS' EIAM solution in terms of potential adoption rates.



**Projected User Population Adoption Rate**

As applications are integrated with the EIAM shared service solution in waves, the user adoption rate for Individuals, Business Users, and Employees is projected to increase over the next four years.

Per the Year 2010 US Census Bureau report, NYS population is estimated at 19.5 Million

1.5 Million business entities (Source: DOS) with upwards of 5 Million users (est.) do business with the State

EIAM solution will be available to manage the identities of all employees

Note: Overlap between user populations is not modeled into the estimates

## 2.4 RFI Scope Statement

In this RFI, NYS is seeking information regarding available EIAM solutions designed to address identity management including directory, web-access management, credential management, federation, user authentication, authorization, auditing and reporting, user provisioning and governance. Responses to this RFI should address the core functionality and features of specific EIAM solutions, architectural design concepts, licensing and maintenance requirements, hardware requirements and an estimate of support resources required. The EIAM solution should also facilitate NYS individuals and the general public to access appropriate applications through the internet by providing the capability to establish user-ids and passwords, and to self-provision certain services and information resources. The EIAM solution should also provide self-care facilities such as user account administration forgot my password and forgot my username facilities.

The following sections describe this initiative in terms of what functionality is being considered at this time and how the State anticipates implementing the new shared service.

### 2.4.1 Functional & Technical Scope

The NYS Enterprise Identity and Access Management (EIAM) solution's objective is to provide an enterprise wide solution for identity and access management. The solution will include support for key functionality identified in the table below.

| Component | Desired Services |
|---|---|
| **Users** | User self-services such as forgotten user ID and password, self-registration, identity vetting etc. |
| **Identity Management** | Identity Provisioning, Workflow, Identity Proofing Services, Account Management, Delegated Administration, Self-registration, Registration Authority Services, |
| **Credential Management** | Single-factor authentication and multi-factor authentication controls, NIST 800-63-1 and FIPS 201 support, account self-services |
| **Access Management** | Authentication Services, Authorization Services, Provisioning Policy Administration, Web Access Management Solution, Risk Based Authentication controls, Audit Services, Reporting |
| **Federation** | Identity Mapping, Authorization, Audit, Provisioning |
| **Auditing and Reporting** | Security Incident and Event Monitoring (all EIAM solution components) |
| **IAM Governance** | Regulation compliance, policies and procedures, Trust agreements, |
| **Agency Resources** | Integrated NYS HR System, Agency Applications, User Directories |

## 2.5 RFI Response

The respondents should address the following issues, at a minimum, as they prepare a response to this RFI. Respondents should include some industry 'best practice' solution features that may not be expressly mentioned in this section. Given the complexity of these solutions, NYS is asking vendors to reference, unless otherwise prohibited by law or contract, actual implementation in either large commercial or government organizations that can demonstrate the actual use of the proposed solution in their responses.

To reduce cost, risk and migration efforts NYS requests respondents consider re-use of current IAM investments, where possible, as described in Section 2.2 Current Environment. Additionally respondents are asked to address how the proposed EIAM solution would maintain the current business operations while moving towards a single EIAM solution.

This RFI covers the entire scope of information that the State seeks to evaluate its current options, though some questions do not apply to all potential suppliers. Respondents should answer all questions in Appendix A that apply to their own services and qualifications.

## 2.6 General Information

### 2.6.1 Registration of Vendors and Individuals

Vendors and individuals interested in responding to, or receiving updated information related to this RFI must register through the Office of Information Technology Services (ITS) Procurement Registration System (PRS), www.cio.ny.gov/apps/prs. All pertinent information will be provided only to those registered in the PRS. ITS is not responsible for failing to inform any parties that are not registered in the PRS.

### 2.6.2 Submission Guidelines

ITS is coordinating responses to this RFI on behalf of the IT Transformation Program.

In order to facilitate the review of the responses, please provide the information in the exact order as presented in Appendix A. The answer field will expand to include entered text as it is filled. Please rename your completed Appendix A with the following naming convention:

**NYS IT Transformation EIAM Services RFI_VENDOR NAME.doc** (.docx format is also acceptable). Please include in the subject of the email: **NYS ITT Request for Information (RFI) – Enterprise Identity and Access Management (EIAM) – VENDOR NAME**

***Respondents that can prove the breadth of experience necessary to successfully implement an Enterprise Identity and Access Management project of this magnitude and that can provide solutions that will satisfy the needs of NYS employees, citizens and business should respond to this RFI by answering all questions provided in Appendix A. If a question cannot be answered, provide a brief explanation as to why the question cannot be answered (e.g., "N/A - function is outside the scope of offering").***

### 2.6.3 Questions concerning this RFI

Vendors must submit any and all questions in the format provided in Appendix B titled **"NYSITT_ConsolidatedEIAMServices_Appendix_B_Vendor_Questions_Template.doc". Please insert the vendor name in the appropriate space. The subject line on the email should state "*EIAM RFI Vendor Questions – VENDOR NAME"*** Each question must cite the particular RFI section and page number it refers to. The closing date for the submission of questions is **12PM ET, June 6, 2012.** Electronic mail is the required method for the submission of questions.

All questions must be submitted to the following mailbox **ITTransformation.eiamservices@cio.ny.gov** with the subject line "EIAM RFI Vendor Questions". No telephone inquiries will be accepted. It is the State's discretion whether to answer some or all questions concerning this RFI. However, consistent and pertinent questions across vendors will be answered and published for all vendors in a timely manner..

### 2.6.4 Requests for Additional Information

At its own discretion, ITS and DOB reserve the right to request additional oral or written information from some or all respondents about the information provided in their responses to this RFI.

### 2.6.5 Response Process and Timeline

**Response Due Date:** Responses to this RFI must be received no later than **12PM ET June 27, 2012.** Responses or amendments to responses received after the due date and time may not be considered in the process.

**Response Timeline:**

| Milestone | Date and Time |
|---|---|
| RFI Release Date | May 25, 2012 |
| Deadline Date for Questions | June 6, 2012 12PM ET |
| RFI Response Due Date | June 27, 2012 12PM ET |

### 2.6.6 General Terms

1. The State will not be liable for any costs of work performed in the preparation and production of any RFI response. By submitting a response, the respondent agrees not to make any claims for, or have any right to, damages because of any misunderstanding or misrepresentation of the specifications, or because of any misinformation or lack of information. The responses shall become the property of the State of New York.

2. This RFI is being issued for data gathering purposes only. As a result, neither the issuance of this RFI nor the State's receipt of a response or several responses to it binds or otherwise obligates New York State to procure any products or services referenced. Similarly, because this RFI is being issued for data gathering purposes only, a responder's response to this RFI does not bind or obligate the responder to provide or offer to the State any of the products or services referenced. No contract can or will be awarded based on submissions to this RFI.

3. ***This RFI does not fall under the requirements of State Finance Law §§139-j and 139-k (the Procurement Lobbying Law) and there is no restricted period***. However, we ask that you direct your questions and responses in writing to designated email address referenced above in section 3.1.3.

4. Freedom of Information Law and RFI Responses

   a) The purpose of New York State's Freedom of Information Law (FOIL), which is contained in Public Officers Law Sections 84-90, is to promote the public's right to know the process of governmental decision making and to grant maximum public access to governmental records.
   b) Thus, a member of the public may submit a FOIL request for disclosure of the contents of the responses submitted to the State in response to this RFI. The responses of respondents may be subject to disclosure under FOIL. However, pursuant to Section 87(2)(d) of FOIL, a State agency may deny access to those portions of responses which "are trade secrets or submitted to an agency 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."  Please note that FOIL has specific instructions for identifying material that an entity claims is exempt from disclosure under FOIL because the information is “trade secrets . . . which if disclosed would cause substantial injury to the competitive position.” Please also note that information which you may claim as proprietary, copyrighted or rights reserved is not necessarily protected from disclosure under FOIL.

c) If there is information in your response which you claim meets the definition set forth in Section 87(2)(d), please inform us in a letter accompanying your response.

5. The State reserves the right to:

a) Postpone or cancel this RFI upon notification to all RFI respondents.
b) Amend the specifications after their release with appropriate notice to all RFI respondents.
c) Request RFI respondents to present supplemental information clarifying their responses, either in writing or in formal presentation.