NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Policy	**No:** NYS-P10-006
IT Policy: **Identity Assurance**	**Updated:** 2/16/2017
	Issued By: NYS Office of Information Technology Services **Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits

This policy establishes a State government-wide framework for issuing and managing trusted identity credentials to allow citizens, businesses, and government employees to conduct business online with New York State (NYS). A trusted identity credential is one in which a State Entity (SE) has confidence that the identity credential represents the person named in it and that the person engaged in the electronic transaction is the person to whom the identity credential was issued.

This policy benefits users of systems and e-Government services by providing a framework that creates and issues NYS electronic identity credentials that will be universally trusted by ensuring alignment with national identity assurance standards and guidelines. SEs will be able to participate in shared identity solutions and reduce the need to issue and manage their own electronic identity infrastructure for e-Government services; resulting in reduced costs of providing online services that require user authentication.

2.0 Authority

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

3.0 Scope

This policy is promulgated pursuant to New York State Information Technology Policy NYS-P03-002, Information Security, and applies to ITS, all State Entities (SE) that receive services from ITS, and affiliates of same (e.g., contractors, vendors, solution providers). It also serves as recommended practice for the State University of New York, the City University of New York, non-Executive branch agencies, authorities, NYS local governments and third parties acting on behalf of same.

This policy applies to online services provided by an SE which require user authentication. This includes all systems for which SEs have administrative responsibility including those managed or hosted by other entities.

4.0 Information Statement

This policy requires that all SEs complete an assessment to determine the appropriate identity assurance level for all NYS IT systems that require authentication. This assessment's only focus is on whether the person seeking to access the system is who they claim to be and the potential impact to the security and integrity of the system if that person is not who they claim to be. Completion of this assessment results in assignment of the system's identity assurance level.

All identity management processes and technologies used to access NYS IT systems must be managed according to the system's assigned identity assurance level, and aligned with federal guidelines and National Institute of Standards and Technology (NIST) guidance on e-authentication.

The system's identity assurance level defines the accepted assurance level a user must have to access the system. The level of certainty in the identity of a user is established through the strength or rigor of the:

- Identification and verification used to establish the identity of the individual to whom an identity credential was issued; and
- Confidence that the individual who uses the credential is the individual to whom it was issued, through the strength of the authentication method used and the rigor of the processes used to manage identity credentials.

NYS has adopted a four-level approach to identity assurance for authenticated access. Each level represents a different degree of certainty in the identity of the user. These four "assurance levels" are aligned with the four levels of assurance established by the U.S. Federal Government[1].

Table 1, Identity Assurance Levels, outlines the four identity assurance levels.

[1] Described in OMB M-04-04-E-Authentication Guidance for Federal Agencies, NIST Special Publication 800-63–Electronic Authentication Guideline, and Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance

Table 1. Identity Assurance Levels

Identity Assurance Level	*Description*
1	Low or no confidence in the asserted identity's validity
2	Confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

Improper authentication of users can result in direct and potentially dire consequences to the SE and users. **The SEs information owner is ultimately responsible for accepting the risk for assigning the appropriate identity assurance level for the system.**

The procedure outlined in Appendix A allows the SE to examine the data within its system and identify the risks of improperly validated access to or potential data exposure. By understanding these risks, the SE is better able to determine the required identity level of assurance and the corresponding authentication technology.

5.0 Compliance

Results of the identity assurance level assessment procedure shall be available for review by the EISO for every online service. All identity credential processes in NYS are managed using the Identity Assurance Standard for the assigned identity assurance level.

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Enterprise Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
e-authentication	Also known as electronic authentication. The process of establishing confidence in user identities electronically presented to an information system.
e-Government	The use of computer technology to provide faster, more convenient, and better delivery of government services to customers by reducing paper processes and the need to go to government offices for the service. Customers in e-Government can include citizens, businesses, and other governments. Typically, these services are available over the Internet on a government agency's website or a government portal, like NY.GOV ID.
Online Service	A service accessed via the Internet or other networks which provides access to citizens, businesses, business partners, other State Entities, local government entities, and the State workforce.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Enterprise Information Security Office
Reference: NYS-P10-006
NYS Office of Information Technology Services
1220 Washignton Avenue, Building 5
Albany, NY 12242
Telephone: (518) 242-5200
Email: EISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
10/05/2010	Original Policy Release	
09/12/2012	Reformatted and updated to reflect current CIO, agency name, logo and style	
10/18/2013	Full revision	Thomas Smith, Chief Information Security Officer
09/19/2014	Removed references to EIAM service and EIAM Program Office; moved procedures to Appendix B; removed Mitigation Request and Proposal – replaced by exception request form	Deborah A. Snyder, Acting Chief Information Security Officer
02/16/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer

9.0 Related Documents

NYS Identity Assurance Standard

National Institute of Standards and Technology (NIST) Special Publication 800-63, Digital Identity Guidelines

APPENDIX A: IDENTITY ASSURANCE LEVEL ASSESSMENT PROCEDURES

Identity Assurance Level Assessment Procedures

Step 1 – Identify the Information Owner and Assemble the Assessment Team

Before the assessment can be conducted, the following two activities must be completed.

1. **Identify the Information Owner**

   The information owner is the person in the SE Division/Business Unit responsible and accountable for the information asset. The information owner is typically at the manager or executive level and is typically non-IT staff. The information owner is responsible for determining who has access to protected resources and what those access privileges are.

   The information owner is responsible for the identity assurance level assigned for authenticated user access. However, the information owner may delegate the actual determination of the identity assurance level required to the Team (described below). The information owner or his/her representative will identify personnel to serve on the Team.

2. **Identify the Assessment Team Members**

   Typically, a team of individuals (hereinafter referred to as the Team) will execute this identity assurance assessment on behalf of the information owner when onboarding an application.

   Though dependent on the type of project, it is recommended that the Team include the information owner or their delegate, legal staff knowledgeable about requirements related to this information, information security staff responsible for supporting the business and IT operations and/or development staff supporting the project. The selected staff should be knowledgeable of the system, data used, business processes it supports, transactions that occur, applicable laws or regulations, security requirements, various user roles or responsibilities when using the computer system, and consequences of unauthorized use.

Step 2 – Collect System Information

Using the IAL Assessment Worksheet (Appendix B), complete the section titled General Information. For the field, Government Interaction Supported, only one box will be checked in most cases. However, there may be systems that are meant to serve multiple audiences (e.g., citizens, business, or other government entities). In those instances check all that apply.

Step 3 – Identify User Roles

The best way to determine the identity assurance level for a user is to understand the types of users who use the system, their roles, what transactions they will be able to perform once authenticated, and what the consequences would be as a result of unauthorized access. For this reason, it is imperative that all user roles be identified.

Using the IAL Assessment Worksheet (Appendix B), complete the section titled ***Identify User Types***.

Step 4 – Determine Assurance Level for Each User

Using the IAL Assessment Worksheet (Appendix B), complete the section titled ***Determine Risk and Impact*** for each user role identified in Step 3, which includes how to:

Step 4.a Identify the transactions a user can perform

For example, the ability for a private citizen to inquire about benefit programs that fit their individual needs could be a primary objective of an online eligibility assistance system. The same system can also allow a user to fill out or create an application for benefits or services.

For some systems, a complete set of transactions for the system will be analyzed. For others, the transactions will be a representative set. When there are many transactions, the Team is to identify as many as possible, with emphasis on those transactions that carry the highest risk to the SE or to a user.

Actions a user can perform must be identified and documented in the section titled Transactions Supported. These include:

- ***Inquire*** - allows the user to access authorized data or information. The user makes a request for information and receives it. This information may be related to the user in some way (i.e., private) or can be general information (i.e., public).
- ***Create*** - allows the user to enter new data into a system. The user creates data that does not currently exist. However, if existing information is available in a system and new information is appended, the “create” transaction is essentially a modification of existing data, and is covered by the “modify” transaction.
- ***Modify*** - allows the user to change existing data or information in a system and save those changes. The original information may or may not be recoverable.
- ***Delete*** - allows the user to destroy or eliminate data or information so that it is no longer available for inquiry or modification. The elimination of data or information may be temporary (recoverable) or permanent (unrecoverable).
- ***Approve/Deny*** – allows the user to accept or deny a request or voucher. This is a type of “modify” transaction, as it appends additional data to the existing record.
- ***Cancel*** – allows the user to withdraw from a transaction with no changes made to the record; the record remains intact.

Step 4.b Determine and document the set of potential consequences associated with the transactions

In this activity, the Team develops and documents the consequences of unauthorized use for each transaction it is assessing. This is performed by answering six (6) questions[2] in the Worksheet that help the Team draw out consequence statements depending on the type of transaction being assessed.

Each of the consequence statements will play an important part in determining the impact levels (Step 4c) and, consequently, the identity assurance level required (Step 4d).

The type of transaction (i.e., inquire, modify, delete, create, etc.) is important for developing these consequence statements, because each type affects data in different ways.

Depending on the type of transaction, unauthorized use can result in many possible undesired outcomes and consequences to the SE or to the user. This is because of the inherent effect that each transaction has on related data and information.

The Team can consider these effects when determining the consequences of unauthorized use of a transaction. For example:

- ***Inquire***. Unauthorized use can result in disclosure of data to unauthorized individuals. Data that is to be kept confidential (e.g., subject to HIPAA, New York State Information Security Breach and Notification Act) or is considered to be Personal, Private or Sensitive Information (PPSI), can cause serious consequences for the SE or for the user if disclosed to unauthorized individuals. The Team should consider what consequences result from this unauthorized disclosure.
- ***Create***. Unauthorized use can result in the creation of data that is misleading, fraudulent, or used for unintended purposes; essentially, the integrity of existing data is put in question. The creation of unauthorized data can interfere with the use of existing data for authorized purposes. As with the unauthorized modification of data, the Team should consider what consequences result from the inability to use existing data for the purposes intended, or from the use of data that may not be accurate.
- ***Modify***. Unauthorized use can affect the integrity of the data and the ability to use the data for its intended purpose. Unauthorized modification of data may constitute disclosure (i.e., confidential data may be seen by an unauthorized individual before they modify it). The Team should consider what consequences result when the integrity of the data is affected.
- ***Delete***. Unauthorized use causes the data to be unavailable. If the loss of data is temporary, the Team should consider what consequences result from having to recover or restore the data, and from the temporary inability to use

[2] Adapted from OMB M-04-04 E-Authentication Guidance for Federal Agencies

it for the purposes intended. If the loss is permanent, the Team should consider what consequences result from the permanent inability to use the data for the purposes intended.

Using the IAL Assessment Worksheet (Appendix B), complete the section titled ***Determine Consequences.*** Examples of possible responses for each category of harm are listed below.

Category of Harm	Identity Assurance Impact Levels			
	1	2	3	4
1. What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?	Alternatives are readily available with no additional costs or degradation of service quality. Minor embarrassment.	Alternatives are readily available with additional costs and/or degradation of service quality. Loss of reputation or standing between the principals. Loss of trust or confidence between the principals.	Alternatives are **not readily** available. Loss of reputation or standing beyond the principals (including third parties). Loss of trust or confidence beyond the principals (including third parties).	Alternatives are **not** available. Wide-scale permanent loss of reputation or standing. Wide-scale permanent loss of trust or confidence.
2. What potential financial losses would be incurred by any involved party? (**Note:** The severity of the loss depends on the impact of the loss on the affected party)	No financial loss.	Financial loss that has no impact or only an insignificant material impact on the financial standing of an individual or organization. A budgetary impact that may require reallocation of funds but no additional financing.	Financial loss that has a significant material impact on the financial standing of an individual or organization. A budgetary impact that may require re-allocation of funds and additional financing.	Financial loss that severely jeopardizes the financial standing of an individual or organization. Financial restructuring may be required.

APPENDIX A: IDENTITY ASSURANCE LEVEL ASSESSMENT PROCEDURES

Category of Harm	Identity Assurance Impact Levels			
	1	2	3	4
3. What effect(s) would result from an unauthorized release of sensitive information (e.g., PPSI, HIPAA)?	No loss of privacy. No increase in public scrutiny or media attention.	Loss of privacy, unwanted surveillance, tracking, monitoring, data profiling or data matching. Loss of confidence in the organization, compromised business relationships. Loss of public confidence. Increase of public scrutiny or media attention. Diminished program integrity.	Potential inability to fulfill legal or contractual obligations. Damage to business relationships requiring legal remedies. Increased oversight (e.g., increased audits, more stringent approval processes). Significant financial penalties to the SE. Compromise to critical asset.	Disruption of social order or civil unrest. Loss of business continuity. Cessation of business relationships. Loss of authority (e.g., due to intervention by an external party). Loss of continuity of critical government services. Major damage to or potential loss of a critical asset. Irreversible damage to public trust.
4. To what civil or criminal violations would the agency be subject (e.g., out of compliance with regulatory rules)?	No civil or criminal violations possible.	False claims or wrongful actions having minor financial or legal implications pertaining to the individual only. Violation does not ordinarily require disciplinary, investigative or enforcement action.	False claims or wrongful actions having significant financial or legal implications which may also pertain to third parties (e.g., trustees acting on behalf of the individual). Violation could require disciplinary, investigative or enforcement action.	False claims or wrongful actions having severe financial or legal implications where the safety and well-being of the individual or other affected parties may be jeopardized. Violation requires disciplinary, investigative or enforcement action.

Category of Harm	Identity Assurance Impact Levels			
	1	2	3	4
5. What harm to agency programs or public interest would be realized?	No noticeable reduction in effectiveness of a primary function of an organization. No compromise to a critical asset. No loss of public confidence.	Noticeably reduced effectiveness of a primary function of an organization. Little or no compromise to a critical asset. Temporary loss of public confidence.	Significantly reduced effectiveness of a primary function of an organization. Compromise to a critical asset. Long-term loss of public confidence.	Unable to perform primary function of an organization. Major damage to or potential loss of a critical asset. Permanent loss of public confidence.
6. How would personal safety be impacted?	No possible impact on personal safety.	No physical injury or psychological distress that requires treatment by first-aid personnel or health care professional.	Physical injury or psychological distress that requires treatment by first-aid personnel or health care professional.	Physical injury or psychological distress that requires an emergency response.

Step 4.c Assign impact levels based on consequences to the SE or to the authorized user

Not all consequences are created equal. In this step the Team will evaluate the impact to the organization using the consequence statements from above. Using the potential impacts will assist in determining (in the next step) the assurance level.

Using the IAL Assessment Worksheet (Appendix B), complete the section titled ***Determine Impact Levels.***

Step 4.d Use the impact levels to determine the identity assurance level for each user

The purpose of this step is to determine the required assurance level based on the impact levels determined in the previous step. The higher the impact to the organization, the higher the assurance level required.

Using the IAL Assessment Worksheet (Appendix B), complete the section titled ***Identity Assurance Level Required***. The identity assurance level is determined by the highest impact categorization of all six (6) questions.

Step 5 – Identity Assurance Level Sign-off

If the Team seeks to reduce the identity assurance level, an exception request form must be filed with the Enterprise Information Security Office (EISO). The information owner is ultimately responsible for accepting the risk for the approved identity assurance level for this system. To assure policy compliance, the completed IAL Worksheet must be submitted to the EISO office for review.

Once implemented, if system requirements have changed, an SE must reassess the assurance level to ensure it still meets the identity assurance level that was assigned and verify that the system is properly protected.

APPENDIX B: IDENTITY ASSURANCE LEVEL (IAL) ASSESSMENT WORKSHEET

Identity Assurance Level (IAL) Assessment Worksheet

General Information	
System Name: *Enter the name of the system for which the IAL Assessment is being completed.*	
System Description: *Enter a brief but adequate description of the system. The description should provide a summary of what the system is, its purpose, whom it serves, etc.*	
Government Interaction Supported: *Check the appropriate box(es) that best indicate(s) the type of government interaction the system supports:* • *Government-to-Citizen – Interaction between state government and its citizens.* • *Government-to-Business – Interaction between state government and the private business sector.* • *Government-to Government – Interaction across all levels of government (federal, state, local, tribal).*	☐ Government-to-Citizen ☐ Government-to-Business ☐ Government-to-Government
Date Assessment Completed: *Enter the date on which the IAL Assessment was completed.*	Click here to enter a date.
Information Owner: *Enter the name and the functional title of the Information Owner for the information associated with this system, along with his or her contact information. The Information Owner is the person in the State Entity responsible and accountable for the security of the information. Information owners are typically at the manager or executive level.* ***Note:*** *Information owners are typically not IT personnel. IT personnel only implement the security controls set forth by the information owner to protect the confidentiality, integrity, and availability of the information asset.*	Name: Functional Title / Job Title: Phone #: Email:

APPENDIX A: IDENTITY ASSURANCE LEVEL ASSESSMENT PROCEDURES

IAL Assessment Team Members: *Enter the names of the IAL Assessment Team, their functional job title, and their contact information, starting with the IAL Assessment Team chair or leader.*	**IAL Assessment Team Chair/Team Leader** Name: Functional Title: Phone #: Email: **IAL Assessment Team Members** Name: Functional Title: Phone #: Email: Name: Functional Title: Phone #: Email: Name: Functional Title: Phone #: Email: Name: Functional Title: Phone #: Email:

IDENTIFY USER TYPES *In this section, identify the set of users that will have authenticated access to the system.*			
User Role: *Identify the user types (e.g., citizen, vendor, NYS employee) that will be accessing the system.* **User Role Description:** *Provide a brief description of the user role.*		**User Role**	**User Role Description**
	1		
	2		
	3		
	4		
	5		

APPENDIX B: IDENTITY ASSURANCE LEVEL (IAL) ASSESSMENT WORKSHEET

Determine Risk and Impact

User Role:

User Role Description:

Enter one user role, and its associated description listed above, for which this table will be completed.

DETERMINE CONSEQUENCES

Consequence Statements: *For each identified transaction, write a consequence statement for each of the six (6) questions, indicating the potential consequences to the State Entity or to the user (enter N/A for a question if not applicable) in the event (of an authentication error) a non-authorized individual were to conduct the transaction.*

There is no need to provide a consequence statement if a question does not apply. Conversely, it is possible to identify many consequences in response to a single question that is particularly relevant to the transaction.

TRANSACTIONS SUPPORTED								
Transaction Name *Provide the transaction's name.*	**Transaction Description** *Provide a description of the transaction. Describe the actions the user can perform using the following action words: inquire, create, modify, delete, approve, or cancel.*	**Data Sensitivity** *Identify the data used in the transaction/system, and specifically note whether the data is restricted to certain actors or groups of actors as it contains sensitive information. Indicate the law or regulation governing the data.*	1. What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?	2. What potential financial losses would be incurred by any involved party?	3. What effect(s) would result from an unauthorized release of sensitive information?	4. To what civil or criminal violations would the agency be subject? (Out of compliance with regulatory rules.)	5. What harm to agency programs or public interest would be realized?	6. How would personal safety be impacted?
DETERMINE IMPACT LEVELS *Using the Table titled Identity Assurance Level Required for guidance, assign an impact value (1, 2, 3, 4) to each of the six (6) questions, based on the consequence statements associated with each. If there is more than one transaction for the user, then consider the consequence statement that poses the greatest risk and thus the greatest potential impact to the agency.*			☐ 1 None ☐ 2 Little ☐ 3 Serious/limited ☐ 4 Serious/severe	☐ 1 None/ insignificant ☐ 2 Minor ☐ 3 Serious ☐ 4 Severe/catastrophic	☐ 1 None ☐ 2 Limited ☐ 3 Serious ☐ 4 Catastrophic	☐ 1 None ☐ 2 No enforcement ☐ 3 Possible enforcement ☐ 4 Enforcement	☐ 1 None ☐ 2 Limited ☐ 3 Serious ☐ 4 Severe or higher	☐ 1 None ☐ 2 Minor ☐ 3 Non-serious ☐ 4 Serious/Death

APPENDIX B: IDENTITY ASSURANCE LEVEL (IAL) ASSESSMENT WORKSHEET

Identity Assurance Level Required

For each of the six (6) category questions, check the corresponding impact level in the matrix below, using the highest impacted user role per each consequence statement as identified in the Determine Risk and Impact table above. (Note: A box can be checked by double-clicking on the appropriate box and selecting "Checked" and "OK" from the pop-up.)

Category of Harm	Identity Assurance Impact Levels			
1. What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?	☐ **1** **No** inconvenience, distress or damage to the standing or reputation of any party	☐ **2** **Little** inconvenience, distress or damage to the standing or reputation of any party	☐ **3** A **serious short-term or a limited long-term** inconvenience, distress or damage to the standing or reputation of any party	☐ **4** A **serious or severe long-term** inconvenience, distress or damage to the standing or reputation of any party
2. What potential financial losses would be incurred by any involved party? **Note:** The severity of the loss depends on the impact of the loss on the affected party	☐ **1** **No or insignificant/in-consequential** unrecoverable financial loss to any party or an insignificant/incons equential agency liability	☐ **2** A **minor** unrecoverable financial loss to any party or a minor agency liability	☐ **3** A **serious** unrecoverable financial loss to any party or a serious agency liability	☐ **4** A **severe or catastrophic** unrecoverable financial loss to any party or a server or catastrophic agency liability
3. What effect(s) would result from an unauthorized release of sensitive information? **NOTE:** The severity of the effect is due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal, government or commercial information	☐ **1** **No loss or adverse effect** on an individual or agency	☐ **2** A **limited adverse effect** on an individual or agency	☐ **3** A **serious adverse effect** on an individual or agency	☐ **4** A **catastrophic effect** on an individual or agency

Category of Harm	Identity Assurance Impact Levels			
4. To what civil or criminal violations would the agency be subject (e.g., out of compliance with regulatory rules)?	☐ **1** **No** risk of civil or criminal violations	☐ **2** Risk of civil or criminal **violations** that **would not** ordinarily be subject to enforcement efforts	☐ **3** Risk of civil or criminal **violations** that **may be** subject to enforcement efforts	☐ **4** Risk of civil or criminal **violations** that is of special importance to enforcement programs and may have **exceptionally grave consequences**
5. What harm to agency programs or public interest would be realized?	☐ **1** **No adverse effect** on any agency program, asset or the public interest	☐ **2** A **limited adverse effect** on any agency program, asset or the public interest	☐ **3** A **serious adverse effect** on any agency program, asset or the public interest	☐ **4** A **severe or catastrophic effect** on any agency program, asset or the public interest
6. How would personal safety be impacted?	☐ **1** **No** risk of injury	☐ **2** A risk of injury **not requiring medical attention**	☐ **3** A risk of non-serious injury **requiring medical attention**	☐ **4** A risk of **serious** injury or **death**

The system's identity assurance level will be based on the selections in the table above. The right-most checked impact level should be the overall identity assurance level assigned to the system.				
Identity Assurance Level Required	☐ **1** Low or no confidence in the asserted ***identity***'s validity	☐ **2** Confidence in the asserted ***identity's*** validity	☐ **3** High confidence in the asserted ***identity***'s validity	☐ **4** Very high confidence in the asserted ***identity***'s validity

_____ _____

Information Owner Date

_____ _____

EISO Representative Date