Federal Identity, Credential, and Access Management
Trust Framework Solutions

Determination of Identity Assurance Level Requirement
for
Agency Applications Accepting FICAM TFS Approved Third Party Credentials

Version 1.0.0

It is in the government's best interest to leverage industry resources whenever possible. To support E-Government activities, the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS) aims to leverage industry-based credentials that citizens already have for other purposes. A component of the TFS, the Trust Framework Adoption Process (TFPAP), defines a process whereby the government can assess the efficacy of the Trust Frameworks for federal purposes so that an Agency online application or service can trust an electronic identity credential provided to it at a known level of assurance comparable to one of the four OMB-04-04, "E-Authentication Guidance for Federal Agencies", Levels of Assurance.

This documents provides a worksheet, based on OMB-04-04 and Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems", to determine the appropriate Level of Assurance in a user's asserted identity that is required in order to address the risks associated with authentication errors.

As noted in OMB-04-04, the risk from an authentication error is a function of two factors:

1. potential harm or impact, and
2. the likelihood of such harm or impact

Categories of harm and impact include:

- Inconvenience, distress or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

FICAM Guidance

FICAM recommends the following in the application of this guidance:

1. This worksheet should be filled out by the business owner of the application or in partnership with the business owner and not solely by the technical team
2. OMB-04-04 allows for "tuning" the risk using a "likelihood of harm/impact" factor. But based on operational experience and the constantly evolving threat landscape of the Internet, it is HIGHLY recommended to set that factor equal to 1. i.e. DO NOT discount the likelihood of harm, and assume there is ALWAYS a likelihood of harm.
3. If feasible, partition your application into distinct areas based on the sensitivity of the data/transaction and associated required Level of Assurance e.g. Only Level 1 is needed for browsing the site but Level 2 may be required for conducting a sensitive transaction. Treating the entire application as Level 2, while theoretically easier, may increase overall credential and management costs.

Determination of Identity Assurance Level Requirement

Description of Application Activity, Service or Transaction:	
Date/Assessor/Approved:	

Assessment Question: *If the above described is compromised, could it result in… (complete each question using the table cells below)*

Category of Harm	Level 1 Assessment	Level 2 Assessment	Level 3 Assessment	Level 4 Assessment
☐ **1. Inconvenience, distress or damage to standing or reputation**	☐ *Any inconvenience, distress or damage to the standing or reputation of any party?*	☐ *A serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party?*	☐ *A serious long-term inconvenience, distress or damage to the standing or reputation of any party?*	☐ *A severe and permanent inconvenience, distress or damage to the standing or reputation of any party?*
☐ **2. Financial loss or agency liability**	☐ *Any financial loss or any agency liability?*	☐ *A minor financial loss to any party (Note: $ amount is dependant upon party involved)*	☐ *A major financial loss to any party. (Note: $ amount is dependant upon party involved)*	☐ *An extreme financial loss to any party. (Note: $ amount is dependant upon party involved)*
☐ **3. Harm to agency programs or public interests**	**Not Applicable**	☐ *A limited adverse effect on a government organization (i.e. can only perform primary function with noticeably reduced effectiveness), or minor damage to program, organizational asset, or public interest?*	☐ *A serious effect on a government organization (i.e. can only perform primary function with significantly reduced effectiveness), or serious damage to program, organizational asset, or public interest?*	☐ *A catastrophic effect on a government organization (i.e unable to perform primary function), program, organizational asset, or public interest?*
☐ **4. Unauthorized release of sensitive personal or commercial information.**	**Not Applicable**	☐ *A limited adverse effect on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information?*	☐ *A serious effect on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information?*	☐ *A catastrophic effect on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information?*
☐ **5. Unauthorized release of sensitive government information (non-personal information)**	**Not Applicable**	☐ *A limited adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties?*	☐ *A serious effect on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties?*	☐ *A catastrophic effect on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties?*
☐ **6. Personal Safety**	**Not Applicable**	**Not Applicable**	☐ *A personal injury requiring medical attention?*	☐ *A serious personal injury or death?*
☐ **7. Civil or criminal violations**	**Not Applicable**	☐ *A violation that may result in minor consequences?*	☐ *A violation that may result in serious consequences?*	☐ *A violation that may result in exceptionally grave consequences*
ASSURANCE LEVEL REQUIREMENT *Minimum level of assurance required to achieve an agency program outcome, deliver a service, or execute a transaction.*	☐ **Minimum Level 1 Required** *Level 1 is required if any assessment category (1-2) is checked in the column above.*	☐ **Minimum Level 2 Required** *Level 2 is required if any assessment category (1-7) is checked in the column above.*	☐ **Minimum Level 3 Required** *Level 3 is required if any assessment category (1-7) is checked in the column above.*	☐ **Minimum Level 4 Required** *Level 4 is required if any assessment category (1-7) is checked in the column above*

Examples of Harm/Impact: The following table provides generic assessment examples for each category of harm/impact and assurance level. These examples may be used as part of the assessment process and in addition to the assessment criteria specified in the table on the preceding page

Category of Harm	Examples of Harm for each Assurance Level			
	Level 1 Examples	**Level 2 Examples**	**Level 3 Examples**	**Level 4 Examples**
☐ **1. Inconvenience, distress or damage to standing or reputation**	☐ *Alternatives are available with little or no delay having no additional costs or degradation of quality of service.* ☐ *Minor embarrassment only*	☐ *Alternatives are readily available* ☐ *Loss of reputation or standing between the principals* ☐ *Loss of trust or confidence between 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. Financial loss or agency liability**	☐ *No financial loss amount*	☐ *Financial loss amount that has no or insignificant material impact on the financial standing of an individual or organization* ☐ *A budgetary impact that may require re-allocation of funds but with no additional financing.*	☐ *Loss of a financial amount 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*	☐ *Loss of a financial amount that severely jeopardizes the financial standing of an individual or organization* ☐ *Financial re-structuring may be required.*
☐ **3. Harm to agency programs or public interests**	☐ *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.* ☐ *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*
☐ **4. Unauthorized release of sensitive personal or commercial information.**	☐ *No loss of privacy.* ☐ *No increase of 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 or decreased competitive standing.* ☐ *Loss of competitive advantage*	☐ *Potential inability to fulfill legal or contractual obligations* ☐ *Damage to business relationships requiring legal remedies*	☐ *Disruption of social order or civil unrest* ☐ *Loss of business continuity* ☐ *Cessation of business relationships* ☐ *Market volatility* ☐ *Loss of authority (e.g. due to intervention external party)*
☐ **5. Unauthorized release of sensitive government information (non-personal information)**	☐ *No increase of public scrutiny or media attention*	☐ *Loss of public confidence* ☐ *Increase of public scrutiny or media attention* ☐ *Diminished program integrity*	☐ *Increased oversight (e.g. increased audits, more stringent approval processes, etc.)* ☐ *Temporary revocation of departmental authorities* ☐ *Compromise to critical asset*	☐ *Loss of continuity of critical government services* ☐ *Erosion or loss of departmental authorities* ☐ *Major damage to or potential loss of a critical asset* ☐ *Irreversible damage to public trust*
☐ **6. Personal Safety**	☐ *No physical injury or psychological distress*	☐ *No physical injury or psychological distress that requires treatment by first-aid personnel or health care professional.*	☐ *A physical injury or psychological distress that requires treatment by first-aid personnel or health care professional.*	☐ *A physical injury or psychological distress that requires an emergency response*

Category of Harm	Examples of Harm for each Assurance Level			
	Level 1 Examples	**Level 2 Examples**	**Level 3 Examples**	**Level 4 Examples**
☐ **7. Civil or criminal violations**	☐ *False claims or wrongful actions having no financial or legal implications pertain to the individual only.*	☐ *False claims or wrongful actions having minor financial or legal implications and which pertain to the individual only.* ☐ *The violation does not ordinarily require disciplinary, investigative or enforcement action* ☐ *The violation may result in a summary offence*	☐ *False claims or wrongful actions significant financial or legal implications and which may also pertain to third parties (e.g. trustees acting on behalf of the individual)* ☐ *Violation could require disciplinary, investigative or enforcement action* ☐ *The violation may result in an indictable offence (e.g. criminal offence)*	☐ *False claims or inaccurate representations in relation to services or transactions where the safety and well-being of the individual or other affected parties may be jeopardized.* ☐ *The violation requires disciplinary, investigative or enforcement action* ☐ *The violation may result in an indictable offence of a serious nature (e.g. terrorism)*