Potential impact categories and values

Impact Categories	Impact Values of Authentication Failure		
	Low	Moderate	High
1. Inconvenience, distress, or damage to standing or reputation	Limited and short-term inconvenience, distress or embarrassment to any party	Serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party
2. Financial loss or agency liability	Insignificant or inconsequential unrecoverable financial loss or agency liability to any party	Serious unrecoverable financial loss or agency liability to any party	Severe or catastrophic unrecoverable financial loss or agency liability to any party
3. Harm to agency programs or public interests	Limited adverse effect on organizational operations or assets, or public interests. Examples: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness (ii) minor damage to organizational assets or public interests	Serious adverse effect on organizational operations or assets, or public interests. Examples: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness (ii) significant damage to organizational assets or public interests	Severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions (ii) major damage to organizational assets or public interests
4. Unauthorized release of sensitive information	Limited release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199	Release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199	Release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199
5. Personal safety	Minor injury not requiring medical treatment	Moderate risk of minor injury or limited risk of injury requiring medical treatment	Risk of serious injury or death
6. Civil or criminal violations	Risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts	Risk of civil or criminal violations that may be subject to enforcement efforts	Risk of civil or criminal violations that are of special importance to enforcement programs

Table 3: Potential impact categories and values

Source: *OMB M-04-04 Section 2.2. Risks, Potential Impacts, and Assurance Levels*

ANNEX – CCIRC IMPACT SEVERITY MATRIX

This matrix is provided for reference purposes only; each organization is encouraged to establish their own impact severity matrix, using thresholds appropriate for the size, complexity, and nature of the organization.

Impact Severity Matrix

Impact	Info Disclosure	Life or Injury	Economic	Health and Safety	Essential Services	Public Confidence / Media
Very low *negligible effect*	Publicly available info = Unclassified	Minor discomfort for some	Small impact on SME / medium effect for individual Damages < $1K	F/P/T/M and CI able to provide for Canadians' welfare	Small group = temp loss(< 24 hrs.)	Negligible effect
Low *Minor effect*	Low sensitivity info = Protected A	Moderate to serious discomfort for some	Small effect on Canada's economic sector Large impact for SME $1K < Damages < $100K	Lead response agency requires surge resources to contain a problem / Other H+S services are not significantly impacted	Small group / small city = medium (between 24 and 72 hrs.) / temp loss	Letters to the editor / Phone complaints / Local news coverage
Medium *Major effect*	Medium sensitivity info or injury to the national Interest = Protected B / Confidential	Serious discomfort / injury / illness for many	Medium effect on Canada's economic sector Very large impact for SME $100K < Damages < $10M	Lead response agency requires surge resources to contain a problem / Other H+S services are adversely impacted	Small group / small city / large city = Long (>72 hrs.) / medium / temp loss	Media editorials / National media coverage / Focussed debate in Parliament
High *Significant effect*	High sensitivity info or serious injury to the national interest = Protected C or Secret	Potential loss of life / permanent disability	Canada's economy / strategic economic objectives damaged $10M < Damages < $1B	Lead response agency approaching capacity to contain a problem / Other H+S services becomes ineffective	Large group / large city / P/T = Long / medium / temp loss	Gov. policy challenged / Extensive international media coverage / Acts of civil disobedience
Very High *Catastrophic effect*	Exceptionally grave injury to the national interest = Top Secret	Potential for widespread loss of life	Extensive damage to Canada's economy / strategic economic objectives Damages > $1B	Lead response agency's capacity to contain a problem is exceeded / Other H+S services are halted	Large City / P/T = long / medium loss	Disruption of Gov. Services / Violent demonstrations / Focused international media coverage / Canadians severely impacted

Assurance level identity proofing objectives

Assurance Level	Objectives	Control	Method of processing
LoA1	Identity is unique within a context	Self-claimed or self-asserted	In-person or remote
LoA2	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	In-person or remote
LoA3	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through 1. use of identity information from an authoritative source 2. identity information verification	In-person or remote
LoA4	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other context	Proof of identity through 1. use of identity information from multiple authoritative sources 2. identity information verification 3. entity witnessed in-person	In-person only

Table 5: Assurance level identity proofing objectives

Source: *ISO/IEC 29115: 2013, Table 8-1 page 13*

Identity proofing and verification approach

Assurance Level	Registration Requirement	
	In-Person	**Remote**
LoA1	Not Required	Proof of Identity • Email address Verification Method • Confirm the validity of email address and ensure that it uniquely identifies an individual.
LoA2	Not Required	Proof of Identity • Email address • Mobile telephone number Verification Method • Confirm the validity of email address and ensure that it uniquely identifies an individual. • Verify that the identity exists objectively, for example, by sending account activation link to the registered email and a verification code as SMS message to mobile telephone number. To completely activate the credential, both the activation link and the correct verification code are required.
LoA3	Proof of Identity • Government ID Card • Email address (if applicable) • Mobile telephone number • Another identification that contains current corroborating information such as House Registration Document or Resident Book, driving license, and passport Verification Method • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Record a photograph or other form of	Proof of Identity • Government ID Card (Color copy) • Email address • Mobile telephone number • A copy of House Registration Document or driving license or passport. Verification Method • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Verify that the identity exists

Assurance Level	Registration Requirement	
	In-Person	**Remote**
	biometric i.e. fingerprint to ensure that applicant cannot repudiate application • Confirm possession of mobile telephone number by sending activation code required for completing the registration process as SMS message to that particular number.	objectively, truly lives in the registered address and owns the email address by, for example, sending activation link via email and username and password via registered mail to the address.
LoA4	<u>Proof of Identity</u> • Government ID Card • Certificate of Employment • Email address • Mobile telephone number • Other identifications that contain current corroborating information such as House Registration Document or Resident Book, driving license, and passport <u>Verification Method</u> • Inspect photo-ID and verify via the issuing government agency or through trusted third party e.g. organization that in charge of national ID • Confirm authenticity and validity of all supplementary documents. Verify them against the issuing authority. • Record a photograph • Record a current biometric i.e. fingerprint, palm print, and hand geometry to ensure that applicant cannot repudiate application • Verify that the identity exists objectively, truly lives in the registered address and owns the mobile telephone number and email address by sending elements required for completing the registration process via out-of-band channels. Example of scenario is - sending activation link via email - sending username and password via registered mail to the address - when login with the above elements, OTP will be generated and sent via SMS message to the mobile telephone number	Not Applicable

Table 6: Identity proofing and verification approach