الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Certification Scoping Standard

[NCSA-NISCF-CERT-NIA-SS]

Standard

National Cyber Security Agency (NCSA)

December 2023

V 3.2

C0 – Public / PS1 – Non-Personal Data (Non-PD)

Document Control

Document Details	
Document ID	NCSA-NISCF-CERT-NIA-SS
Version	V 3.2
Classification & Type	C0 – Public / PS1 – Non-Personal Data (Non-PD)
Abstract	This document details the requirements (information) that shall be provided during a National Information Assurance (NIA) Certification Application, under the National Information Security Compliance Framework (NISCF), in order to National Cyber Governance and Assurance Affairs (NCGAA) to approve the scope.

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Certification Scoping Standard" - V 3.2 - C0 – Public / PS1 – Non-Personal Data (Non-PD), in order to provide the requirements that shall be provided during a National Information Assurance (NIA) Certification Application, under the National Information Security Compliance Framework (NISCF), in order to National Cyber Governance and Assurance Affairs (NCGAA) to approve the scope.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Certification Scoping Standard".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

LEGAL MANDATE(S)

Based on Emiri Decree No 1 of year 2021, National Cyber Security Agency (NCSA) – National Cyber Governance and Cyber Assurance Affairs (NCGAA) is the entity responsible for issuing certificates for Technology and Information Security service providers and Certificates of Compliance with National Information Security standards and policies.

This Standard has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure conformance with the relevant applicable laws of the State of Qatar.

Table of Contents

1. Introduction

National Cyber Security Agency (NCSA) published in May 2023 the National Data Classification Policy V3.0 [IAP-NAT-DCLS] and National Information Assurance Standard V2.1 [IAS-NAT-INFA], in replacement of National Information Assurance Policy V2.0.

Based on the fact that:

- The approach to achieve organizational compliance was unchanged;
- The Data Classification Model was unchanged;
- The limited changes to National Information Assurance (NIA) controls statements with no additional requirements; and
- Negligible impact of the changes on existing National Information Assurance (NIA) Compliance achieved;

Cyber Assurance Department, National Cyber Governance and Assurance Affairs - National Cyber Security Agency (NCSA) decided to continue accepting applications for Certificate of Compliance against NIAP V2.0 until December 31, 2023.

Previously issued Certificates and/or Certificates issued during this period against NIAP V2.0 will continue to be valid for their defined period of validity mentioned in the Certificate. Certified organizations against NIAP V2.0 could only request Re-Certification against National Information Assurance (NIA) Standard V2.1.

Based on the facts stated above, the Cyber Assurance Department encourages and currently accept applications for its newly offered Certification against National Information Assurance (NIA) Standard V2.1.

To highlight the updated scoping requirements for Certification against National Information Assurance (NIA) Standard V2.1, NCSA developed this document, titled "National Information Security Compliance Framework (NISCF) – National Information Assurance (NIA) Certification Scoping Standard" - V 3.2 - C0 – Public / PS1 – Non-Personal Data (Non-PD), to provide the cyber space with clearer requirements for scoping of NIA Certification Service.

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to provide requirements for NISCF's NIA Certification Service scoping across the full lifecycle of NISCF's NIA Certification Service.

2.2. Scope

This document applies to all NISCF's NIA Certification Service for the purpose of obtaining, maintaining, updating or renewing NISCF's Certificate of Compliance for NIA against National Information Assurance (NIA) Standard V2.1.

3. Key Definitions

Implementation Services Helping in the operational implementation to help achieving conformity.

Information Assets A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilized effectively. Information Assets can be processed in a physical (i.e., paper), digital (i.e., IT / OT) or cognitive (i.e., human knowledge) format.

Information Assets Classification Register (IACR) Document or a set of documents that includes the classification (categorizing the data based on its security attributes (confidentiality, integrity, and availability), in order to handle it according to its security rating) of identified data and their Information Assets.

Processed Any operation or combination of activities that is performed over data, including collection, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, combining, restricting, erasing or destroying it.

The terminologies used in this policy are consistent with the definitions provided in the NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public).

4. Standard Requirements

4.1. Scoping Requirements for Certification Operation

4.1.1. Scoping for request for NISCF's NIA Certification (Application)

4.1.1.1. Certification Plan

4.1.1.1.1. The applicant to NISCF's NIA Certification Service shall submit, as part of the request to NISCF's NIA Certification, the Certification Plan documentation that is approved by the applicant's top management, with a clear version and date.

4.1.1.1.2. The Certification Plan document shall include the different phases of implementation and Certification of National Information Assurance (NIA) Standard V2.1 requirements, if any.

Note: The applicant, or NISCF's NIA Certification Service subject if different from the applicant, shall aim toward organizational compliance (i.e., apply National Information Assurance (NIA) Standard V2.1 requirements to all processes/functions). In certain situations, it is impractical to implement National Information Assurance (NIA) Standard V2.1 requirements and obtain the related Certification for all the processes/functions at once. It is possible to divide the organizational compliance into phases.

4.1.1.1.3. Each phase of implementation and Certification stated in the Certification Plan document, as specified in requirement **4.1.1.1.2**, shall include:

- A target date for completing the implementation; and
- A target date for applying to NISCF's NIA Certification Service.

4.1.1.2. Scope Document

4.1.1.2.1. The applicant to NISCF's NIA Certification Service shall submit, as part of the request to NISCF's NIA Certification, a Scope Document that is approved by the applicant's top management, with a clear version and date.

4.1.1.2.2. The Scope Document shall include the scope statement that defines clearly and explicitly the scope of the NISCF's NIA Certification Service request, that will be mentioned on the potential NISCF's NIA Certificate of Compliance.

4.1.1.2.3. The scope statement shall reference the relevant phase of the Compliance Plan, as defined in requirement **4.1.1.1.2**, constituting the scope of NIA Certification request.

4.1.1.2.4. The scope statement, referred to in requirement **4.1.1.2.2**, shall be factual, clear, concise and shall not reflect an inspiration, a goal or a mission.

4.1.1.2.5. The Scope Document shall include boundaries of the NISCF's NIA Certification Service request, by providing:

- The organizational boundaries: Identification of the departments, functions, or any other organizational units that are accountable for the scope within the NISCF's NIA Certification Service Subject;
- The physical boundaries: Identification of the physical and geographical location in which the scope is governed, managed and operated, including third-parties; and
- The logical boundaries: Identification of the non-tangible limits of the scope, in which Information Assets are processed and / or full or partial applicable controls are managed or operated, including third-parties.

4.1.1.2.6. The Scope Document shall include a clear indication which phase, from the Certification Plan, if any, it covers (please refer to requirements **4.1.1.1.2** and **4.1.1.1.3**).

4.1.1.3. Information Assets Classification Register (IACR)

4.1.1.3.1. The applicant to NISCF's NIA Certification Service shall submit, as part of the request to NISCF's NIA Certification, the Information Assets Classification Register (IACR) identifying all the Information Assets in the scope, that is approved by the applicant's top management, with a clear version and date.

4.1.1.3.2. The IACR shall include the necessary details about the Information Assets that shall include at least:

- The categorization of each Information Asset based on the three criteria of Confidentiality, Integrity and Availability in conformance with the classification scheme provided in the National Data Classification Policy [IAP-NAT-DCLS] V3.0;

- The classification level of each Information Asset based on the three classification levels of Low, Medium and High in conformance with the classification scheme provided in the National Data Classification Policy [IAP-NAT-DCLS] V3.0;

- The format in which each Information Asset is processed (e.g., physical records, Information Technology, Operational technology, Human Resource Knowledge…);

- The location where each Information Asset is processed;

- The type of each Information Asset (e.g., Financial, Government, Personal…) with a clear identification of Personal Data[1]; and

- The status of use of each Information Asset based on its location and format of processing.

4.1.1.3.3. The IACR shall include the responsibilities over the Information Assets in terms of Data owner and Data custodian.

4.1.1.4. Statement of Applicability (SoA)

4.1.1.4.1. The applicant to NISCF's NIA Certification Service shall submit, as part of the request to NISCF's NIA Certification, the Statement of Applicability (SoA) that is approved by the applicant's top management, with a clear version and date.

4.1.1.4.2. The SoA shall list all the controls as stated in National Information Assurance (NIA) Standard V2.1 and shall identify which controls have been selected as applicable.

4.1.1.4.3. The SoA shall include status of implementation (i.e., planned, on-going, completed) of each applicable control.

4.1.1.4.4. The SoA shall include a statement of exclusion for each of the non-applicable baseline controls.

4.1.1.4.5. The SoA shall include a justification of the choice of each Additional control.

[1] As defined in Law 13-2016

4.1.1.5. Pre-Certification Assessment Evidence

4.1.1.5.1. The applicant to NISCF's NIA Certification Service shall submit, as part of the request to NISCF's NIA Certification, the assessment results and conclusions of the compliance for each applicable control for the scope.

4.1.1.5.2. The assessment referred to in requirement **4.1.1.5.1**, shall be performed by an organization unit and individuals that are independent from the implementation and operation of NIA controls for the scope.

4.1.2. Scoping for request for NISCF's NIA Certification Scope Expansion

4.1.2.1. Confirmation of Relevancy

4.1.2.1.1. The Certified Organization requesting for scope expansion of an active NISCF's NIA Certificate of Compliance shall provide a revised Certification Plan (see section **4.1.1.1**) taking into consideration the changes in the implementation and Certification phases, if any, due to request for the scope expansion.

4.1.2.2. Scope Expansion Document (SED)

4.1.2.2.1. The Certified Organization requesting for scope expansion of an active NISCF's NIA Certificate of Compliance shall submit a Scope Expansion Document (SED).

4.1.2.2.2. The SED shall include a justification for the scope expansion and rationale for not applying for an isolated NISCF's NIA Certification Service request for the additional scope, taking into consideration the implementation and Certification phases described in the Certification Plan (referred to in requirements **4.1.1.1.2** and **4.1.1.1.3**).

4.1.2.2.3. The SED shall include the Expansion Scope Statement (ESS) that defines clearly and explicitly the scope subject of the request for scope expansion.

4.1.2.2.4. The SED shall include an Updated Scope Statement (USS) that defines clearly and explicitly the updated scope, taking into consideration the request for scope expansion referred to in requirement **4.1.2.2.3** and the scope of the active NISCF's NIA Certificate of Compliance referred to in requirement **4.1.1.2.2**, that will be mentioned on the potentially updated NISCF's NIA Certificate of Compliance.

4.1.2.2.5. The Expansion Scope Statement (ESS), referred to in requirement 4.1.2.2.3 and the Updated Scope Statement (USS), referred to in requirement 4.1.2.2.4, provided in the SED shall be in conformance with requirements 4.1.1.2.4 and 4.1.1.2.5.

4.1.2.3. Other Documents

4.1.2.3.1. The Certified Organization requesting for scope expansion of an active NISCF's Certificate of Compliance shall submit the Information Assets Classification Register (IACR), Statement of Applicability (SoA) and Pre-Certification Assessment Evidence in conformance with requirements respectively detailed in sections 4.1.1.3, 4.1.1.4, and 4.1.1.5.

4.1.3. Scoping for request for NISCF's NIA Re-Certification

4.1.3.1. Confirmation of Relevancy

4.1.3.1.1. The Certified Organization requesting for extending the period of validity of a NISCF's NIA Certificate of Compliance through Re-Certification shall provide a written confirmation that the:

- Certification Plan (see section 4.1.1.1);
- Scope Document (see section 4.1.1.2);
- Information Assets Classification Register (see section 4.1.1.3);
- Statement of Applicability (see section 4.1.1.4); and
- Pre-Certification Assessment Evidence (see section 4.1.1.5);

results and details, provided during the NISCF's NIA Certification Service request or updated during a previous scope expansion (see section 4.1.2), continue to be valid and relevant to the context of the Certified Organization or the NISCF's NIA Certification Service Subject at the time of the request for Re-Certification.

4.1.3.1.2. When confirmation mention in requirement cannot be provided, the Certified Organization shall provide an updated version of the above-listed documents to assess impact of the changes on the scope.

5. Compliance and Enforcement

5.1. Compliance Process

All applicants to the NISCF's NIA Certification Service and Certified Organizations holder of an NISCF's NIA Certificate of Compliance shall conform with the requirements defined in this standard.

5.2. Roles and Responsibilities

National Cyber Governance and Assurance Affairs (NCGAA) is responsible for enforcing and monitoring conformance to this standard.

5.3. Transitioning and effective date

5.3.1. Effective date

This standard is effective from January 1, 2024.

5.3.2. Transition period

NISCF's NIA Certification Services requests made and NISCF's NIA Certificates of Compliance issued before the effective date of this standard are not subject to this standard until the Re-Certification stage.

5.4. Exceptions and deviations

5.4.1. Exceptions to Standard Requirements

Exceptions to this standard shall only be defined by the National Cyber Security Agency (NCSA) through another policy or standard and / or any NCSA's organizational structure that has been given the authority over the NISCF or the NIA Certification Service.

5.4.2. Deviation process from Standard Requirements

Deviation from standard requirement shall be formally authorized in writing by the National Cyber Security Agency (NCSA).

5.4.3. Sanctions

National Cyber Security Agency (NCSA) reserves the right to not accept NISCF's NIA Certification Service requests and / or suspend or withdraw NISCF's NIA Certificates of Compliance provided by NCSA from Applicants and holders of NISCF's NIA Certification Service requests and NISCF's NIA Certificates of Compliance that do not conform with the requirements defined in this Standard.

National Cyber Security Agency (NCSA) reserves the right to impose any monetary or procedural sanctions in virtue of the authority that has been granted to NCSA, though laws and regulations, on Applicants and holders of NISCF's NIA Certification Service requests and NISCF's NIA Certificates of Compliance that do not conform with the requirements defined in this Standard.

6. Annexes

6.1. Acronyms

ESS	Expansion Scope Statement.
IACR	Information Assets Classification Register.
NCGAA	National Cyber Governance and Assurance Affairs.
NCSA	National Cyber Security Agency.
NIA	National Information Assurance.
NISCF	National Information Security Compliance Framework.
SED	Scope Expansion Document.
SoA	Statement of Applicability.
USS	Updated Scope Statement.

6.2. Reference

Emiri Decree No 1 of year 2021

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022

NCSA-NISCF-CERT-GTXD (General Taxonomy Document for National Certification - Public)

NCSA-NISCF-CERT-GPNC (General Policy for National Certification - Public)

NCSA-NISCF-CERT-SMSC (Standard for Management Systems Certification - Public)

End of Document