PUBLIC SUBMISSION

As of: 4/27/22 7:21 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-l3m3-f7hw
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0070
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Joint Accreditation System of Australia and New Zealand (JAS-ANZ)

General Comment

Dear NIST, please find a submission from the Australian & New Zealand Accreditation Body for management system certification (including ISO/IEC 27001) attached. Note also that the Australian Government Department of Education, Skills & Employment (DESE) contributed input to this submission.

Attachments

2022_JAS-ANZ_Submission_to_NIST_April_25_letter

JOINT ACCREDITATION
SYSTEM OF AUSTRALIA
AND NEW ZEALAND
HELPING MARKETS
WORK BETTER

JAS-ANZ.ORG

AUSTRALIA

FECCA House
4 Phipps Close
Deakin ACT 2600

PO Box 304
Deakin West ACT 2600

P: +61 (0)2 6232 2000

NEW ZEALAND

Level 4 Berl House
108 The Terrace
Wellington 6143

PO Box 10476
Wellington 6143

P: +64 (0)4 473 4426

25 April 2022

Alicia Chambers
alicia.chambers@nist.gov
NIST Executive Secretariat
National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899, USA

Dear Alicia Chambers

Thankyou for the opportunity to provide comments on the use, adequacy, and timeliness of the Cybersecurity Framework and the degree to which other NIST resources are used in conjunction with or instead of the Framework.

JAS-ANZ is limiting its comments to items 8 (*Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework*) and 9 (*Adaptions of the Cybersecurity Framework*) on the list in Docket Number 220210-0045.

Who are JAS-ANZ and DESE?

The Joint Accreditation System of Australia and New Zealand (JAS-ANZ) was established in 1991 by the Australian and New Zealand governments as their nationally recognised accreditation body for the accreditation of 'third-party' certification bodies (or other forms of conformity assessment bodies) to issue accredited certifications (or other attestations) to standards or other requirements. JAS-ANZ provides accreditation services to around 130 public and proprietary schemes globally, and complies with relevant requirements for accreditation bodies that are members of the International Accreditation Forum and the International Laboratory Accreditation Cooperation. JAS-ANZ personnel are active members of Australian and New Zealand standards committees, which in turn contribute to the development and use of International Organization for Standardization (ISO) and IEC (International Electrotechnical Commission) standards globally.

The Australian Government Department of Education, Skills and Employment (DESE) contributes to economic prosperity and social wellbeing by creating opportunities and driving better outcomes for people, through education, skills and employment pathways.

As part of assistance measures for persons looking for work, DESE engages private service providers under contractual arrangements that include compliance with information security requirements for both participant and Australian Government information.

.

The DESE ISMS Scheme – an example of a national government adaption of non-NIST frameworks in conjunction with the NIST Cybersecurity Framework

In early 2021, JAS-ANZ published Issue 1 of the 'DESE ISMS' Scheme, owned by DESE as the Scheme Owner. The '*object of conformity*' for the third-party certification scheme is the information security management systems (ISMS) and environment of contracted service providers, of which DESE engages to assist persons prepare for and look for work. More specifically, the scope of this certification scheme is compliance with the Department's contractual requirements (Statement of Applicability, SoA) for providers' ISMS under the Right Fit for Risk (RFFR) accreditation approach. The latter approach is a component of the Department's External Systems Assurance Framework (ESAF) by which the department gains assurance over providers' ISMS.

The approach in the DESE ISMS Scheme has four key features that afford adaptability and proportionality:

1. Incorporation of the Australian Government Information Security Manual, published by the Australian Cyber Security Centre within the Australian Signals Directorate, as the 'source' of information controls for the Statement of Applicability in ISO/IEC 27001 based certification ('Annex A' controls). The Manual 'outlines a cyber security framework that an organization can apply, using their risk management framework' that '*draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.' The range of NIST controls that are applicable to organizations are categorised into four systems, which from most to less sensitive are: TOP SECRET (requiring auditing by government personnel or delegates), SECRET (*requiring auditing by Government approved third-party auditors, 'Infosec Registered Assessors Program Assessors' - 'IRAP Assessors'*), PROTECTED, and OFFICIAL. The information being protected in the DESE ISMS Scheme is confirmed by DESE to be classified as OFFICIAL;

2. 'IRAP Assessors' and the competency criteria for them (*which notably includes regard to ISO/IEC 27001 Lead Auditor status, as well as NIST information security controls*) are explicitly recognised as an option for use in the DESE ISMS Scheme, but are not mandatory to use;

3. Providers with caseloads of less than 2000 users per year (*persons seeking employment*) are exempt from the requirement to attain certification, but may voluntarily elect to do so. Instead, such providers are obligated to undertake periodic self-assessments against the DESE information security requirements and hold records of these; *And*

4. Organizations holding accredited ISO/IEC 27001 certification under the globally operated ISMS Scheme are afforded reduced audit time, providing they undertake a self-assessment and mapping of the 'gap' between ISO/IEC 27001 and ISMS requirements under the DESE ISMS Scheme and extent of reductions are justified by the certification body. **Furthermore, such organization may hold two separate certifications provided the scope of certification clearly demarcates the two.**

Additional risk-based features of the DESE ISMS Scheme further facilitate its proportionality and reasonable discretion (and responsibility) for organizations:

- Certain NIST information security controls (*incorporated via the Australian Government the Information Security Manual*) are prescribed as a minimum set of Core Expectations for organizations developing an ISMS and seeking certification to the scheme. These can be (*and must be for organizations with higher ISMS risks*) supplemented by additional controls, but cannot be omitted (*unless being met through equivalent controls, with a rationale provided*); *And*
- While audit time is primarily derived as per ISO/IEC 27006 (*personnel under the organization's control in scope of the ISMS),* risk loadings are applied based on caseloads (*job seekers whose private information is required to be obtained and held*).

In the view of an auditor with experience as an IRAP Assessor, an ISO/IEC 27001 Lead Auditor, and JAS-ANZ Assessor in the internationally harmonised ISMS Scheme for accredited ISO/IEC 27001 certification with CISSP and CISM credentials that was asked for comment on Issue 1, the DESE ISMS Scheme is a useful attempt at striking the balance of the 'best of both worlds' from NIST / Australian Signals Directorate, and ISO/IEC information security techniques.

DESE and JAS-ANZ would welcome any input from NIST in an Issue 2 update to the DESE ISMS Scheme

The Australian Signals Directorate was invited to be on the scheme technical committee for developing the DESE ISMS Scheme Issue 1 but advised its official position was that first-party use of the Information Security Manual supplemented with third party auditing by its approved IRAP Assessors is preferable to accredited third party certification to schemes. It nonetheless asked to remain notified of updates and developments in the DESE ISMS Scheme, and will be invited again for the Issue 2 update this year as the relevant Australian Government authority and publisher of the Australian Government Information Security Manual.

JAS-ANZ and DESE are of the view that the DESE ISMS scheme is an example of how technically complex information security techniques can be made more approachable for business owners, and thus facilitate development of cybersecurity organizational maturity. That is, how to maintain an appropriate balance between information security expectations of external parties (*government in this case*) with the rightful discretion of organization's top management operating increasingly diverse business models (*including operations entirely unrelated to the scheme)*.

With time and refinement, the two organizations are confident that the DESE ISMS Scheme will prove to be a useful mechanism for the security of government information, including for organizations involved in critical and/or highly sensitive business areas. The scheme has due regard to both the regulatory requirements for higher-risk government information and the principle that organizations maintain discretion on how to control their information as relevant to their context and preferred technical solutions. Additional Australian Government and Australian state/territory government partners for co-ownership and/or recognition of the scheme are being actively sought in the upcoming Issue 2 update of the scheme.

JAS-ANZ and DESE are interested in discussing the DESE ISMS Scheme (including a proposed Issue 2 update) and comments above in further detail with NIST at a mutually convenient time.

In any case, JAS-ANZ looks forward to the development of the revised Framework and guidance regarding supply chains, and would be interested in exploring the application of the Framework in New Zealand and Australia with government and industry partners.

Thank you again for the opportunity to provide comment on the Cybersecurity Framework.

Yours Sincerely

Matthew Pitt (*electronically signed*)
Technical Manager, JAS-ANZ
(e) [redacted]
cell phone: [redacted]