ENSIGN
INFOSECURITY

# National Institute of Standards and Technology (NIST)

## Ensign InfoSecurity Feedback to Request for Feedback for the Cybersecurity Framework (CSF) v2.0

26 April 2022

**CONFIDENTIAL**

This Page is deliberately left Blank

Ensign InfoSecurity (Singapore) Pte. Ltd.
30A Kallang Place
#08-01
Singapore 339213

**26 April 2022**

TO WHOM IT MAY CONCERN
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899

**FEEDBACK TO NIST CYBERSECURITY FRAMEWORK VERSION 2.0**

Thank you for the opportunity for Ensign InfoSecurity to provide feedback on the NIST Cybersecurity Framework (CSF) version 2.0.

We are pleased to share how we use the NIST CSF to deliver our Consulting services. The feedback and recommendations are based on the means in which we use the CSF for the cybersecurity maturity profiling services and threat analysis services.

The opinions contained herein are Ensign's only. The opinions are provided for consideration in the development of the next version of the CSF only.

This document is prepared for NIST. Ensign InfoSecurity will not be held responsible for parties beyond NIST. The circulation of this document to parties beyond NIST must be approved by Ensign InfoSecurity in writing.

We trust that you will find the contents of the document meeting your needs.

Please reach out to me at [redacted] for any further clarifications or collaborations.

Yours Sincerely
Mr. Teo Xiang Zheng
Head of Advisory, Consulting
Ensign InfoSecurity (Singapore) Pte. Ltd.
[This is an electronic document and requires no signature]

# Contents

# 1 About Ensign

Ensign InfoSecurity is the largest pure-play end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Ensign's core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is inhouse research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region. More information can be found at https://www.ensigninfosecurity.com/.

The following input is prepared by Ensign Consulting, who provides cybersecurity advisory and assurance services to our client.

# 2 Ensign Consulting's Context of Adopting NIST Cybersecurity Framework (CSF)

The Ensign Consulting Team leverages the NIST CSF to advise our clients on their cybersecurity program. The NIST CSF is the primary reference framework for Ensign Cybersecurity Maturity Framework (CSMF) and maturity assessments, where we determine our client's sophistication in understanding and implementation of cybersecurity and cybersecurity controls. The CSMF uses the definition of the Implementation Tiers to evaluate the level of maturity of each of the 23 Categories in the CSF. The results are then averaged to provide the Functional maturity scores.

Separate to the evaluation of the cybersecurity maturity across the 23 Categories and 5 Functions, we also leverage the MITRE ATT&CK Framework to perform a threat profile for the subject organisation we are evaluating to determine the target state maturity levels across the 23 Categories. This leverages the publicly available mapping files from NIST SP 800-53 to NIST CSF and MITRE ATT&CK to NIST SP 800-53. This approach is taken to avoid the leveraging of benchmarking data which does not provide a contextually relevant definition of the target maturity levels. Borrowing the context of MITRE's Threat-Informed Defense approach, we believe that using the threat context to derive the target maturity level is more beneficial to our clients.

After the cybersecurity maturity assessments, we devise improvement programs for clients referencing NIST CSF and the NIST SP 800-53. In addition to maturity programs, NIST CSF is a supplementary framework for other assessments, where other frameworks are dictated by client's scope of work.

While other similar frameworks such as the CMMC exists, we believe that the broader context and lack of rigid compliance objectives support a better alignment for advisory engagements.

# 3 Feedback to Improve NIST CSF in Version 2.0

## 3.1 Improved definitions in the framework

NIST CSF's brevity (compared to other cybersecurity standards such as ISO 27002) allows for flexibility in adoption across industries. However, there is also a lot of ambiguity in understanding where an organisation stands in terms of implementation. **We recommend more detailed explanations and definitions for implementation tiers including**:

1. Definition of necessary controls or demonstration of capability at each implementation tier for each (sub)category;
2. Definition of outcomes at each implementation tier for each (sub)category; and
3. Guidelines on how an organisation's leadership could recommend and approve a target implementation tier.

While our understanding of the subcategories in NIST CSF is informed by our knowledge of other frameworks such as specific controls in NIST SP 800-53, NIST CSF's subcategories can appear too vague for organisations who want to adopt the framework independently. As a result, **we recommend more descriptive explanations of (sub)categories** (may be covered in the controls and outcomes mentioned above).

Related to the previous two points, NISTIR 8183 Rev. 1 Cybersecurity Framework Version 1.1 Manufacturing Profile is a good example of how concepts in NIST CSF could be elaborated further. Though it may not be feasible to build a Profile for every sector in the main NIST CSF, some examples and elaborations to help organisations better understand the framework would be welcomed.

Currently, protection against supply-chain-related attacks is not explicitly mentioned under Protect function (under Identify function, there is a category for Supply Chain Risk Management). Given the increased in supply-chain-related attacks, **we recommend a consideration for establishing another supply chain (sub)category under IDENTIFY, PROTECT, DETECT and / or RESPONSE functions which goes beyond Risk Management**. The response context could also make references to the CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks[1]. Topics which are relevant may include:

- Technology and Technology Services Procurement Cybersecurity (controls and practices)
- Vendor Risk Monitoring (including assessments)
- Digital Attack Surface Monitoring (including vendors)

Enterprise architecture refers to the design of an organisation's objectives, operating model and processes. Enterprise architecture encompasses business architecture, data architecture and technology architecture. At the moment, this concept of enterprise architecture is embedded / implied in several Identify function's categories and subcategories. Given the importance and usefulness of the concept for an organisation, **we recommend a consideration for establishing enterprise architecture and cybersecurity architecture as a (sub)category under IDENTIFY and PROTECT functions**. This could include maturing concepts such as Zero Trust Architecture principles (ZTA) and Secure Access Secure Edge (SASE) concepts. This could reference the NIST SP 800-207.

## 3.2 Improved coverage of the framework

Since the release of NIST CSF version 1.1, many cybersecurity concepts have been placed under the spotlight. NIST has developed a series of papers to guide the discussion for some of them, namely:

- Secure Software Development (SP 800-218)
- Zero Trust Architecture (SP 800-207)
- IoT Cybersecurity (NISTIR 8259 Series, SP 800-213)
- Cloud Security (SP 800-210)
- Cyber Supply Chain Risk Management (SP 800-161)
- Risk Management Framework (SP 800-37)
- Privacy Framework[2]

In addition, the following topic has not received additional guidelines since NIST CSF version 1.1, but merits an update:

- OT Cybersecurity (SP 800-82)
- Mobile Device Security[3]

Given that NIST CSF is to be the overarching framework for cybersecurity, organisations should be able to understand how to achieve specific cybersecurity objectives such as cloud security or IoT security vis-à-vis a broader cybersecurity program under a NIST CSF. As a result, **we recommend the inclusion of bidirectional guidance and references between these specific frameworks and NIST CSF**.

## 3.3 Improved relevance of the framework

In our work, we often leverage both NIST CSF and NIST 800-53 to guide our clients to their desired cybersecurity posture. The timely mapping between NIST CSF version 1.1 and NIST SP 800-53 revision 5 was helpful for us in our analysis. As such, **we recommend the continuation and timely update of linkage / mapping between NIST CSF and other cybersecurity framework**. The linkages should allow NIST CSF to stay relevant in between version updates, as it maps to newer frameworks or frameworks refreshed to update our understanding of cybersecurity.

[1] https://cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[3] https://www.nccoe.nist.gov/mobile-device-security

However, we also noticed that certain controls that are previously mapped to certain categories (for example, “Distributed Processing & Storage” and “Port & I/O Device Access” are no longer relevant to “PR.PT-4: Communications and control networks are protected” in the latest mapping despite being mapped in the previous revision of NIST SP 800-53). **We recommend transparency in such changes to ensure an accurate understanding of both NIST CSF and other relevant frameworks**.

We also note that in recent years, MITRE has developed useful cybersecurity tools, namely the ATT&CK and Engage Frameworks. While ATT&CK is more focused on adversaries and provides an initial relevant list of mitigation controls for each threat technique / sub-technique, Engage complements by providing proactive threat engagement actions to support organisations attempting to move from Risk-informed to Repeatable, and subsequently Adaptive Implementation Tiers. **We recommend exploration into how NIST CSF and MITRE Engage could be integrated**.

## About Ensign InfoSecurity

Ensign InfoSecurity is the largest pure play cybersecurity company in Asia Pacific with over 500 cybersecurity professionals.

Our clients trust and rely on us to bring our collective capabilities across Consulting, Systems Integration, Managed Services and Labs to deliver cyber excellence.

We work with our clients to transform them into cyber-resilient leaders, helping them **Conquer the Unknown**.