From: [redacted]
To: cyberframework
Cc: [redacted]
Subject: Comments////Re:Discussion Draft | NIST Cybersecurity Framework 2.0 Core
Date: Monday, September 4, 2023 11:29:19 PM
Attachments: CSF 2.0 Core with Examples Discussion Draft[74].pdf

---

Hi, the comments for CSF 2.0 draft are as follows:

1 GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood

Ex1: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees)

Suggestions: also adds the following statement "..., the business goals and business-specific risks of supervisors in business units,...

Additional comments: In actual CSF implementation, we find many suervisors of busines units refuse or are very reluctant to assist in cybersecurity implementation for fear of possible negative influence on businessc(e.g. delay business efficiency or similar). So, identifying the primary business concern of such persons and clearly demonstrate how cybersecurity can assist their business goals and mitigate business-specific risks are of great importance to win their favorable impression and support.

2 GV.SC-04: Suppliers are known and prioritized by criticality

Ex1: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission

Suggestions: also add the following statement "...the strategic level of suppliers for the organization... "

3 ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)

Ex1: Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use

Suggestions: also add the following statement "...or service/data...."

4 PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)

Ex1: Verify a person's claimed identity at enrollment time using government-issued identity credentials (e.g., passport, visa, driver's license)

Ex2: Issue credentials only to individuals (i.e., no credential sharing)

Suggestions: also add the following statement as an example: "verify the identities of service requests or data.... using digital signature or similar"

Additional comments: Identity proofing is not only for individuals, but also for services or applicaitons.

5 PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)

Ex1: Remove data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed

Suggestions: also add the following statements: "Remove data or the ciphers...."

6 PR.PS-01: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)

Ex1: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality)

Ex2: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software

Suggestions: also add the following statements as an example: "Before installing or updating software or setting parameters, review relevant solutions to assess the security impact. After installing or updating software or setting parameters, review security settings to verify there is non-negligible impact on cybersecurity."

Additional comments: According to our practice, during network change, some engineers may block firewalls or suspend anti-virus software temporarily for ease of operation and forget to enable the security feature again after change, and then sercurity defects are left until successful attacks occur...

7 PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)

Ex1: Avoid single points of failure in systems and infrastructure

Suggestions: it is difficult to avoid single points of failure for hypervisor in cloud computing, which is an inherent security.

8 DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (formerly PR.DS 06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)

Suggestions: also add the following statements as an example: "Monitor software or applications for tampering"

9 RS.MI-01: Incidents are contained

Suggestions: also add the following statements as an example: "Modify the passwords of the affected or attacked devices and block its all communication ports...., or disconnect the affected or attacked devices from the network "

10 RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed

Suggestions: also add the following statements as an example: "If necessary, perform recursive testing

on services to ensure that no services are lost or damaged "

全球服务
Global Services
极致服务 生态引领
Ultimate Service Leading Ecosystem

Cao Kunpeng
Cybersecurity
Quality Dept./ Engineering &
Service Operation Division
[redacted]
P.R.China
[redacted]

原始邮件

发件人：NISTCybersecurityandPrivacyProgram
收件人：曹鲲鹏00053796;
日 期：2023年04月25日 03:15
主 题：**Discussion Draft | NIST Cybersecurity Framework 2.0 Core**