Canada Border Services Agency
Agence des services frontaliers du Canada

NIST CSF 2.0 Draft

Feedback and Comments

Tarek Ali MBA TOGAF ITIL

Senior Advisor / Enterprise Security Architecture [ESA]

Information, Science and Technology Branch

Canada Border Services Agency / Government of Canada

[redacted]

MS Teams: Voice or Chat

PROTECTION • SERVICE • INTEGRITY

Canada

Version reviewed -

Draft of *The NIST Cybersecurity Framework 2.0*

https://doi.org/10.6028/NIST.CSWP.29.ipd

Suggestions provided per line number -

97

describes general strategies that lead to outcomes that reduce cyber risk.

112

in a more focused area **based on priorities**, …

115

Analyze and discover priorities …

117

Mission, **mandate**, …

114

Framework should also be intended for cyber security practitioners and operational professionals to guide their front line activities, especially to identify organizational gaps and strategic shortcomings in their functions.

197

Govern should also align with the organizational goals and mandates, business objectives, etc.

202

Inventory, analyze, categorize and understand its assets …….

214

Adoption of zero trust?

223

Disaster recovery and Business continuity planning?

226

Suggest renaming wheel to cybersecurity framework cycle

234

Would suggest changes in one component of the cycle should force updates to all other components, to maintain dynamic coordination. Governance will coordinate changes.

247

Suggest references to critical standards be categorized by domain and interest in the appendix, to provide rapid lookup based on area of concern / interest. Perhaps NIST already has such a central index site.

256

Perhaps some boiler plate reference and solution architectures can be provided based on standard industry examples. This is similar to certain standard models from TOGAF.

282

To oversee **partner organizations** and third parties.

294

Suggest expanding to **development** and supply chains to non tangible and internal sourcing of resources.

322

Wholesale change might not be possible, therefore for complex scenarios and organizations there might be a need for **transition profiles**.

327

Community profiles should also be indexed and available as examples in the appendix.

329

Should add that **profiles are governance delivery and execution mechanisms**, allowing for centralized coordination between the different components of the CSF cycle.

355

Should include organization and enterprise requirements analysis, associated with specific use cases.

Should also capture business and operational critical functions and use cases.

364

Should include creation of a roles and responsibilities matrix for all stakeholders.

370

Since this area is new to many, some example of supporting information or elements should be added to appendix, for example as templates.

383

Analysis methods and strategies should be suggested in the appendix, based on common use cases and scenarios.

397

The repetition of steps reinforces the notion that the CSF 2 is a cycle of continuous improvement and not a static wheel.

399

Suggest establishment of CSF cross functional and cross departmental working groups to facilitate communications. The CSF plan should be integrated into the organizational strategic plans and funded accordingly.

408

Different instances of the CSF should not be encouraged. Rather a central CSF governance cycle with multiple categories and sub categories across all use cases and scenarios.

425

Suggest establishment of CSF office or group to create and update profiles on a dedicated, regular basis.

433

Example of metrics for different profiles could be suggested in the appendix.

445

Suggest relabelling tiers as maturity levels or maturity tiers. This reflects existing nomenclature - What Is CMMC? - Cybersecurity Maturity Model Certification - Cisco

453

In diagram would relabel third party risk as external risk.

462

Certainly mission critical organizational components can be at a higher maturity tier than others, out of necessity and priority.

500

The development of the overall strategy should be an organic grassroots process with information flowing up from the implementation / operational layer, otherwise details and nuance will be lost. In fact the blue large arrow is the govern part of the cycle.

521

As mentioned info should flow up from ops level before creation of a strategic executive plan, not just after controls implementation.

528

There is once again the need to define metrics at all levels of the CSF implementation, from strategic plan down to ops.

549

Internal supply chains should also be secured, such as software development pipelines.

567

Assessment of supply chains should be evidence based against established controls. Independent certification and audit also play a role. Application of zero trust to suppliers is key, within limits.

599

Include networks

603

Critical to have supplier disaster recovery and business continuity plans.

609

Profiles with attached verifiable evidence are more reliable for validation.

611

A quantitative and qualitative assessment method is required to leverage profiles for assessment. Perhaps a scoring matrix similar to IT Vendor Assessment Scorecard Builder (gartner.com)

644

A privacy impact assessment can help inform the target maturity tier for the organization.

665

Another critical step would be application of privacy specific controls based on assessment and target.

Pr.aa-02

Zero trust is applied to internal and external identities.

Pr.at

Specialized working groups and knowledge sharing bodies are created to share cyber sec knowledge throughout the organization.

Pr.ds-11

Data should be real time protected and restorable with up to date disaster recovery and business continuity plans.

Pr.ps

A configuration management database should be maintained to backup and restore config state of all resources and assets on demand.

A devsecops approach should be considered to integrate security into the development cycles.

Pr.ir

Advanced zero trust and multi-factor authentication measures should be considered.

General disaster recovery and business continuity plans should be maintained.

De.cm

Formal Security information and event management (SIEM) capabilities should be deployed for real time threat detection and response.

Security by design and engineering should integrate security monitoring capabilities into all assets and resources.

Rc.rp

General disaster recovery and business continuity plans should be maintained.