NIST Team,

Thanks for publishing and maintaining the Cybersecurity Framework! It is well-written. Here is my response to your request for information:

High-level feedback:

- **There is opportunity to increase the number of controls**
- 108 controls are attainable for most organizations. However the InfoSec team is left to fill in the gaps
- Resources are limited, controls within risk prioritized tiers could aid with effective mitigation
- Would be helpful to have additional controls, a stop gap between 108 controls and 800-53
- Perhaps existing controls could be expanded to demonstrate levels of maturity
- **Categories could be enhanced for reporting purposes**
- The five categories are high level
- The 23 sub-categories result in skewed reporting
-- Some categories only have two controls
-- In that scenario, one control results in 50 percent compliance
- Would be helpful to organize by or switch to 10-12 domains
- **There is opportunity to add risk ratings**
- High, moderate and low
- Would help businesses prioritize remediation

Detailed feedback to enhance CSF v1.1:

1. Add a guidance field

The 'NIST CSF Control Description' field is concise, which leads to confusion and a need for interpretation. Consider adding a 'Guidance' field to the CSF PDF and spreadsheet. For example…

NIST CSF #	NIST CSF Control Description	Guidance
ID.GV-4	Governance and risk management processes address cybersecurity risks	Maintain a risk register process to provide senior leadership with transparency in the cybersecurity domain. Risk register entries should be reserved for cybersecurity issues that pose significant risk to the organization (risk mitigate or risk accept). Technical vulnerabilities should only be considered for register entries when extended remediation is proposed (e.g. 60 days or more beyond standard). Discuss register entries in risk governance meetings with cybersecurity and senior leaders present. Meet periodically to maintain risk governance routines (quarterly is recommended).

2. Add a documents and artifacts field

Consider adding a 'Documents and Artifacts' field to the CSF PDF and spreadsheet. That would provide guidance for how a given requirement can be validated. For example…

NIST CSF #	NIST CSF Control Description	Documents and Artifacts
ID.GV-4	Governance and risk management processes address cybersecurity risks	• Risk register • Risk governance meeting minutes

3. Enhance the CSF with common controls [Maturity Level One]

It is necessary to implement these foundational controls:

a. Add a requirement for patching. It is not explicitly mentioned within the CSF.

b. Flesh out the CSF to help ensure controls are in-place and effective. For example:

- ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
  - New: There is appropriate separation of duties in the Cybersecurity Leader's reporting structure, such as reporting to the CEO, Chief Risk Officer, Chief Legal Counsel or Board of Directors. When the cybersecurity reports to the IT executive, that is a conflict of interest
  - New: The Cybersecurity Leader provides updates to the Board of Directors or similar executive group
- ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
  - New: An intake process ensures each threat advisory is addressed. Options: (a) When an advisory is received, assign a team member to process it,
    (b) Have a periodic meeting to analyze threat intelligence or
    (c) Enter each advisory into a log to ensure it is processed
- ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
  - New: A cybersecurity professional provides guidance when a supplier wants to redline contract security language
- PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
  - New: Access reviews are conducted periodically (quarterly is recommended)
  - New: Access reviews are conducted when an employee or contractor changes roles. Legacy accesses are rescinded to preserve separation of duties
  - New: Compare a current list of employees and contractors to active system and application accounts. Immediately rescind accesses for departed personnel
  - New: Integrate Single Sign-On into web applications to facilitate systematic removal of accesses
- PR.AT-1: All users are informed and trained
  - New: Update this requirement to: "All users are informed, trained and tested to ensure comprehension"
  - New: Add a requirement for a phishing test program. Annual security awareness training alone is not sufficient

- PR.DS-5: Protections against data leaks are implemented
  - New: Restrict access to technology commonly used to exfiltrate data such as external storage, Internet storage and personal e-mail (e.g. USB drives, Dropbox and Gmail, respectively)
- PR.IP-4: Backups of information are conducted, maintained, and tested
  - New: Store backups offline to protect from ransomware encryption
- PR.IP-10: Response and recovery plans are tested
  - New: Incident response and business continuity exercises include senior executives, lines of business leaders, information technology, legal and public relations
- RC.CO-1: Public relations are managed
  - New: Establish a Crisis Communications Plan and a Holding Statement template to prepare for an emergency or unexpected event

c. Add a requirement for procedures within sub-programs such as vulnerability management, access control and third party risk management. Procedures provide a focus on process execution and help ensure controls are effective as you know.
- The closest control is 'ID.AM-3: Organizational communication and data flows are mapped'

4. Address threats and countermeasures since 2014 [Maturity Level One]

CSF v1.0 was published in 2014. Version 1.1 was made available in 2018 and is a minor release. It is necessary to add new requirements to adapt to changes in the threat landscape.

a. Consider updating the CSF with ransomware mitigation controls from this advisory:
- CISA Alert (AA21-131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks: https://www.cisa.gov/uscert/ncas/alerts/aa21-131a

b. It is also necessary to update the CSF with recent adversarial tactics. Consider these resources from CISA and NSA for controls to identify and mitigate risk.
- CISA Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology: https://www.cisa.gov/uscert/ncas/alerts/aa22-047a
- NSA Network Infrastructure Best Practices: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2949885/nsa-details-network-infrastructure-best-practices

5. Expand the data security section (PR.DS) [Maturity Level Two]

Separate the core framework into common controls that apply throughout the enterprise (e.g. security awareness) and data security controls that should be implemented where sensitive data is stored, processed or transmitted (e.g. encryption).

a. Add requirements for Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).

b. Add a penetration testing requirement. The use of vulnerability scanning alone may fail to detect significant vulnerabilities. Pen testing is used to address that gap and is commonly used in areas where sensitive data is present. Ethical Hackers leverage suites of security tools to identify vulnerabilities and use that information to gain access. They also use custom scripts, conduct manual tests and strive to exploit business logic. If an organization hosts sensitive information, it makes sense to test with hacking techniques.

c. Add a requirement for a Security Operations Center or active monitoring by cybersecurity personnel 24x7x365.

d. Add a requirement for the cybersecurity program to maintain controls specific to line of business products, services and assets.

6. Add a risk management section [Maturity Level Three]

a. One of the most significant categories is Risk Assessment (ID.RA). I've interpreted that as:

"Threat Landscape and Controls Analysis: Conduct risk analysis, resulting in a formal report. Start by considering the inherent risk of the organization. Provide an overview of potential adversaries, techniques for compromising data and the cybercrime ecosystem. Describe the potential for impact, while citing reliable sources. Reference the organization's risk tolerance. Describe the organizations assets. Pivot into cybersecurity with protection boundaries, control framework and risk assessments. Provide fair and balanced analysis by documenting risk mitigation and recent accomplishments in that domain. Detail residual risk with recommendations for new processes and controls. Conclude with a summary statement that praises the organization's risk culture, with recognition for conducting risk analysis." (Reference: Program Maturity - Cybersecurity and Operational Risk Management)

Hoping the CSF can be updated with a similar statement with mid-level detail.

b. Add a Risk Mitigation Controls Menu within an appendix. Provide a listing of optional controls, with a description of risk mitigation properties. Reference my zero trust controls menu as an example. www.gideonrasmussen.com/zero-trust.html

Using an appendix with a list of options helps ensure the entire listing of controls is not mandated by policy or within a contractual requirement.

c. Add a requirement for cybersecurity metrics, KPIs and KRIs to be communicated to management.

7. Add a strong risk management section [Maturity Level Four]

The concept of strong risk management is typically adopted by those with a low risk tolerance such as financial institutions, government entities and pharmaceutical companies. Some organizations may decide to opt-out of this level of maturity due to their business model or cost. Therefore, the following topics are recommendations.

a. Add a recommendation for a Quality Assurance function separate from operations to validate whether critical cybersecurity controls are in place and effective.

b. Add a recommendation for operational functions and lines of business to declare self-identified audit issues, with a metric to measure to what extent the control environment is improving over time.

c. Add a recommendation to adopt the zero trust security model within security architecture and change management. Include mid-level detail for clarity, such as core components, data sources and variations of zero trust architecture approaches:

- Policy engine, administrator and enforcement point
- Continuous diagnostics and mitigation (CDM) system
- Industry compliance system
- Threat intelligence feeds
- Network and system activity logs
- Data access policies
- Enterprise public key infrastructure (PKI)
- ID management system
- Security information and event management (SIEM) system
- Enhanced identity governance
- Micro-segmentation
- Network infrastructure and software defined perimeters

Refer readers to NIST 800-207 for additional details. No need to reinvent the wheel.

d. Add a recommendation to maintain an insider threat program. Reference reputable practices such as Carnegie Mellon's Common Sense Guide to Mitigating Insider Threats.

e. Add a recommendation to conduct threat hunting. Endpoint protection and SIEM security monitoring alone are not sufficient. Cybersecurity professionals should actively search for threat actors within the IT environment. It is necessary to detect adversaries quickly (dwell time and mean time to detect). Early detection can mean the difference between an incident and a data breach.

8. Implement maturity level labeling within the CSF

Map each requirement to a maturity level within the CSF PDF and spreadsheet.

Maturity Level		
M1	Core cybersecurity framework	A framework communicates the minimum controls required to protect an organization.
M2	Common Controls	Controls in this category are viewed by many as necessary and common sense in a cybersecurity context. Some may view this maturity level as filling gaps in the control framework, basic due diligence.
M3	Risk management	Communicate control framework requirements for risk assessment and risk management. It is necessary to tailor controls to the organization and to adapt to changes in the threat landscape.
M4	Strong risk management	At this level the organization begins to demonstrate ownership of the

		cybersecurity program from an operational risk perspective. When management communicates low risk tolerance, that is synonymous with a commitment to strong risk management.

This approach would provide a middle ground between NIST CSF and 800-53. Keep in mind that most civilian organizations do not have massive funding like the federal government.

I've always loved that the CSF gives businesses options based on their risk appetite. This approach preserves that flexibility, with options to increase maturity and mitigate risk.

9. Risk prioritize controls

Implement risk-prioritized mapping of controls within the CSF PDF and spreadsheet. Reference this research, MITRE ATT&CK versus NIST 800-53. This table displays which controls mitigate the largest number of adversary tactics and techniques.

NIST 800-53 Rev 5 Control	# MITRE ATT&CK Mappings
System Monitoring	332
Configuration Settings	311
Baseline Configuration	253
Access Enforcement	240
Least Privilege	229
Malicious Code Protection	198
Least Functionality	196
Continuous Monitoring	194

This is just a sampling of the highest occurrences. There are many more rows.

10. Publish more quick start guides

The NIST Quick Start Guide for Ransomware is a good resource. Here are recommendations for additional guides.

• Network segmentation	• Preventing data exfiltration
• Threat hunting	• Program architecture
• Metrics, KPIs and KRIs	• Security operations center
• Risk assessments	• Risk register process
• Incident response	• Strategic planning
• Business continuity	• Disaster recovery
• Vulnerability management	• Identity and access management
• Third party risk management	• Cyber threat intelligence

NIST Team: Thanks so much for your efforts to protect our country! Feel free to reach out to me with questions or comments.

Gideon

The opinions expressed here are my own and not necessarily those of my current or past employers.