November 3, 2023

National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: Public Draft: NIST Cybersecurity Framework 2.0

Greetings NIST,

Thank you for the opportunity to provide feedback on the draft NIST Cybersecurity Framework 2.0. Recommendations have been outlined in the subsequent pages.

Sincerely,

Nicole Rohloff

Recommended Changes - Draft NIST CSF 2.0				
ID	**Comment**	**Location of Change**	**Comment Type**	**Suggested Language *(bold italicized)***
1	While it is mentioned throughout the document, recommend a brief introduction on the CSF "core" in this section; this will be helpful for those new to the CSF.	Page 1, Executive Summary, Lines 77-78	Substantive	Those actions are intended to address cybersecurity outcomes described within the CSF Core, ***which provides a set of desired cybersecurity activities and outcomes using common language.***
2	Minor edit; suggest elaborating on the plethora of resources available on the CSF website.	Page 1, Executive Summary, Lines 94-95	Substantive	***Supplemental guidance, success stories, resources, and frequently asked questions*** will be developed, ***updated,*** and available on the NIST Cybersecurity Framework website.
3	Minor edit; this touches on human (i.e., people) risk which is worth mentioning as it's a common enterprise risk.	Page 1, Section 1, Line 119	Substantive	***Address human risk and inform*** decisions about cybersecurity-related workforce needs and capabilities.
4	Minor edit, recommend adding the word "governance" as there are several aspects included in this bullet.	Page 1, Section 1, Lines 111-113	Substantive	***Establish and align governance*** (e.g., policy, business, and technological approaches) to managing cybersecurity risks across an entire organization or in a more focused area, such as a portion of the 113 organization, a specific technology, or technology suppliers.
5	Recommend adding a bullet under "prioritize" that stresses the importance of understanding gaps or risks in meeting an organization's strategic plan goals/objectives. Furthermore, since it's reportable to an organization's board of directors, it's probably worth mentioning here. This is included in section 3; however, it would be prudent to mention early on within the CSF.	Page 2, Section 1, Lines 116-118	Substantive	Identify, organize, and prioritize actions for reducing cybersecurity risks that align with the organization's mission, ***strategic goals and objectives,*** legal and regulatory requirements, and risk management and governance expectations.
6	Minor edit.	Page 3, Section 1, Line 153	Substantive	Add the following role: ***performance management professionals***
7	Minor edit; recommend introducing ERM at the onset.	Page 4, Section 1, Lines 167-168	Substantive	Section 4 discusses using the Framework to help integrate cybersecurity risk management with other types of risk management, ***such as Enterprise Risk Management (ERM).***

ID	Comment	Location of Change	Comment Type	Suggested Language (bold italicized)
8	Add additional reference point for "informative resources."	Page 4, Section 2, Lines 176-177	Substantive	……..(Examples), and references to additional guidance on how to achieve those outcomes 177 (Informative References), as depicted in Fig. 1 ***and Section 2.2.***
9	Minor edit.	Page 5, Section 2, Line 202	Substantive	Understanding its i***nformation technology (IT) and operational technology (OT)*** assets (e.g., data, hardware, software, systems, facilities, services….).
10	Figure 1 is helpful; recommend providing a completed version (at a very high level) so the reader has a visual sample of how the CSF pieces fit together. Regardless, it might be helpful to include the CSF "getting started" link in this section. It will take readers directly to the appropriate page, which would be helpful for the layperson that is new to the Framework.	Page 5, Section 2	Substantive	This section explains the basics of the Framework Core. See Appendix C for the Framework Core's descriptions of the Functions, Categories, and Subcategories. ***A detailed overview is also available on the NIST 2.0 website (insert link: https://www.nist.gov/cyberframework/getting-started)***.
11	Elaborate on the value of ERM and alignment with cybersecurity risk and enterprise strategy.	Page 5, Section 2, Lines 196-197	Critical	Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management ***(ERM)*** strategy, ***which helps align cybersecurity risk with strategic efforts.***
12	Minor edit.	Page 5, Section 2, Line 200	Substantive	……..and procedures; ***and the development and*** oversight of cybersecurity strategy.
13	Minor edit.	Page 8, Section 2, Lines 292-293	Substantive	Improve cybersecurity communication ***and collaboration*** with internal and external stakeholders.
14	I realize the sample Profile page is a work in progress; however, it would be helpful for readers to reference existing sample Profiles in the interim. Suggest adding the link in this section as well.	Page 9, Section 2, Line 310	Substantive	……to internal and external stakeholders. Appendix A provides a notional Profile template. ***Additionally, CSF Profile samples are available at: https://www.nist.gov/cyberframework/examples-framework-profiles.***
15	Suggest the addition of a bullet under 3.1.1.	Page 10, Section 3, Line 328	Critical	***Address deviations from an enterprise's strategic plan goals and/or objectives.***

ID	Comment	Location of Change	Comment Type	Suggested Language (bold italicized)
16	The Community Profile call-out-box at the bottom of page 9 is not clear. If Community Profiles are synonymous with sample Framework Profiles, suggest renaming accordingly in this section (e.g., "Sample CSF Framework Profiles") and also include a link to the page. If these differ from Sample CSF Framework Profiles, recommend differentiating between the two (i.e., community vs. Profile samples). Also recommend that the sample Framework Profile page be updated to mention that 2.0 updates will be forthcoming: https://www.nist.gov/cyberframework/examples-framework-profiles	Page 10, Section 3, Line 328	Substantive	https://www.nist.gov/cyberframework/examples-framework-profiles
17	Minor edit.	Page 10, Section 3, Line 339	Substantive	Prioritize cybersecurity outcomes ***and identify appropriate personnel to address them.***
18	Minor edit.	Page 11, Section 3, Lines 364-365	Substantive	Gather the information needed to prepare the Profiles. An organization can gather relevant resources prior to preparing the Profiles, such as ***strategic plan goals and objectives,*** organizational policies……
19	Provide a link to sample Profiles at the end of #3 as it would be helpful for readers to reference existing sample Profiles.	Page 11, Section 3, Lines 382	Substantive	…….lexicon for describing cybersecurity work. ***Additionally, organizations may reference CSF Profile samples at https://www.nist.gov/cyberframework/examples-framework-profiles.***
20	Minor edit.	Page 11, Section 3, Lines 387-388	Substantive	…….resources (e.g., staffing, funding). Using Profiles in this manner aids in ***cybersecurity strategic planning*** and decision-making; including, ***cybersecurity risk strategy,*** and improvements to cybersecurity risk management in…).
20	Minor edit.	Page 14, Section 3, Lines 484-485	Substantive	One of the most common benefits of using the Framework is improving communication ***and/or collaboration*** regarding cybersecurity risks and posture with those inside and outside of an organization.

ID	Comment	Location of Change	Comment Type	Suggested Language (bold italicized)
21	Minor edit.	Page 14, Section 3, Lines 489-491	Substantive	The Framework provides a basis for improved communication ***and/or collaboration*** regarding cybersecurity expectations, planning, and resources among executives, business process managers, and implementation and operations practitioners across an organization.
22	While this section focuses on communication, recommend stressing the importance of collaboration as this is a critical component of addressing cybersecurity risk and improving cyber posture.	Page 14, Section 3, Line 297	Substantive	***The Framework can also foster collaboration across the organization, which can result in an overall improvement in the enterprise's security posture.***
23	Expand on importance of ERM/cyber risk alignment in the beginning (helps streamline, ensures consistency, etc.)	Page 20, Section 4, Lines 684-685	Substantive	……risk considerations, including cybersecurity. ***Aligning ERM with cybersecurity risk management helps standardize how cyber risks are identified, assessed, managed, monitored and reported on. Organizations can also*** benefit from using the Framework to better harmonize cybersecurity risk management activities with other risk management domains.
24	Minor edit.	Page 21, Section 4, Lines 703-704	Substantive	Including ERM-related input (e.g., enterprise risk categories, ***risk tolerance and risk appetite levels***, priorities, integrated risk 704 registers) when gathering information needed to prepare the Profiles (step 2).

Recommended Changes - Draft NIST CSF 2.0

Comment Number	Comment	Location of Change (Page number, Section, Header, Paragraph, Line #)	Critical, Substantive, or Administrative Comment	Suggested Language *(bold italicized)*
1	While it is mentioned throughout the document, recommend a brief introduction on the CSF "core" in this section; this will be helpful for those new to the CSF.	Page 1, Executive Summary, Lines 77-78	Substantive	Those actions are intended to address cybersecurity outcomes described within the CSF Core, ***which provides a set of desired cybersecurity activities and outcomes using common language.***
2	Minor edit; suggest elaborating on the plethora of resources available on the CSF website.	Page 1, Executive Summary, Lines 94-95	Substantive	***Supplemental guidance, success stories, resources, and frequently asked questions*** will be developed, ***updated,*** and available on the NIST Cybersecurity Framework website.
3	Minor edit; this touches on human (i.e., people) risk which is worth mentioning as it's a common enterprise risk.	Page 1, Section 1, Line 119	Substantive	***Address human risk and inform*** decisions about cybersecurity-related workforce needs and capabilities.
4	Minor edit, recommend adding the word "governance" as there are several aspects included in this bullet.	Page 1, Section 1, Lines 111-113	Substantive	***Establish and align governance*** (e.g., policy, business, and technological approaches) to managing cybersecurity risks across an entire organization or in a more focused area, such as a portion of the 113 organization, a specific technology, or technology suppliers.
5	Recommend adding a bullet under "prioritize" that stresses the importance of understanding gaps or risks in meeting an organization's strategic plan goals/objectives. Furthermore, since it's reportable to an organization's board of directors, it's probably worth mentioning here. This is included in section 3; however, it would be prudent to mention early on within the CSF.	Page 2, Section 1, Lines 116-118	Substantive	Identify, organize, and prioritize actions for reducing cybersecurity risks that align with the organization's mission, ***strategic goals and objectives,*** legal and regulatory requirements, and risk management and governance expectations.
6	Minor edit.	Page 3, Section 1, Line 153	Substantive	Add the following role: ***performance management professionals***
7	Minor edit; recommend introducing ERM at the onset.	Page 4, Section 1, Lines 167-168	Substantive	Section 4 discusses using the Framework to help integrate cybersecurity risk management with other types of risk management, ***such as Enterprise Risk Management (ERM).***
8	Add additional reference point for "informative resources."	Page 4, Section 2, Lines 176-177	Substantive	.....(Examples), and references to additional guidance on how to achieve those outcomes 177 (Informative References), as depicted in Fig. 1 ***and Section 2.2.***
9	Minor edit.	Page 5, Section 2, Line 202	Substantive	Understanding its i***nformation technology (IT) and operational technology (OT)*** assets (e.g., data, hardware, software, systems, facilities, services....).
10	Figure 1 is helpful; recommend providing a completed version (at a very high level) so the reader has a visual sample of how the CSF pieces fit together. Regardless, it might be helpful to include the CSF "getting started" link in this section. It will take readers directly to the appropriate page, which would be helpful for the layperson that is new to the Framework.	Page 5, Section 2	Substantive	This section explains the basics of the Framework Core. See Appendix C for the Framework Core's descriptions of the Functions, Categories, and Subcategories. ***A detailed overview is also available on the NIST 2.0 website (insert link: https://www.nist.gov/cyberframework/getting-started)*** .
11	Elaborate on the value of ERM and alignment with cybersecurity risk and enterprise strategy.	Page 5, Section 2, Lines 196-197	Critical	Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management ***(ERM)*** strategy, ***which helps align cybersecurity risk with strategic efforts.***
12	Minor edit.	Page 5, Section 2, Line 200	Substantive	.....and procedures; ***and the development and*** oversight of cybersecurity strategy.
13	Minor edit.	Page 8, Section 2, Lines 292-293	Substantive	Improve cybersecurity communication ***and collaboration*** with internal and external stakeholders.
14	I realize the sample Profile page is a work in progress; however, it would be helpful for readers to reference existing sample Profiles in the interim. Suggest adding the link in this section as well.	Page 9, Section 2, Line 310	Substantive	.....to internal and external stakeholders. Appendix A provides a notional Profile template. ***Additionally, CSF Profile samples are available at: https://www.nist.gov/cyberframework/examples-framework-profiles.***
15	Suggest the addition of a bullet under 3.1.1.	Page 10, Section 3, Line 328	Critical	***Address deviations from an enterprise's strategic plan goals and/or objectives.***
16	The Community Profile call-out-box at the bottom of page 9 is not clear. If Community Profiles are synonymous with sample Framework Profiles, suggest renaming accordingly in this section (e.g., "Sample CSF Framework Profiles") and also include a link to the page. If these differ from Sample CSF Framework Profiles, recommend differentiating between the two (i.e., community vs. Profile samples). Also recommend that the sample Framework Profile page be updated to mention that 2.0 updates will be forthcoming: https://www.nist.gov/cyberframework/examples-framework-profiles	Page 10, Section 3, Line 328	Substantive	https://www.nist.gov/cyberframework/examples-framework-profiles
17	Minor edit.	Page 10, Section 3, Line 339	Substantive	Prioritize cybersecurity outcomes ***and identify appropriate personnel to address them.***
18	Minor edit.	Page 11, Section 3, Lines 364-365	Substantive	Gather the information needed to prepare the Profiles. An organization can gather relevant resources prior to preparing the Profiles, such as ***strategic plan goals and objectives,*** organizational policies.....
19	Provide a link to sample Profiles at the end of #3 as it would be helpful for readers to reference existing sample Profiles.	Page 11, Section 3, Lines 382	Substantive	.....lexicon for describing cybersecurity work. ***Additionally, organizations may reference CSF Profile samples at https://www.nist.gov/cyberframework/examples-framework-profiles.***
20	Minor edit.	Page 11, Section 3, Lines 387-388	Substantive	.....resources (e.g., staffing, funding). Using Profiles in this manner aids in ***cybersecurity strategic planning*** and decision-making; including, ***cybersecurity risk strategy,*** and improvements to cybersecurity risk management in...).
20	Minor edit.	Page 14, Section 3, Lines 484-485	Substantive	One of the most common benefits of using the Framework is improving communication ***and/or collaboration*** regarding cybersecurity risks and posture with those inside and outside of an organization.
21	Minor edit.	Page 14, Section 3, Lines 489-491	Substantive	The Framework provides a basis for improved communication ***and/or collaboration*** regarding cybersecurity expectations, planning, and resources among executives, business process managers, and implementation and operations practitioners across an organization.
22	While this section focuses on communication, recommend stressing the importance of collaboration as this is a critical component of addressing cybersecurity risk and improving cyber posture.	Page 14, Section 3, Line 297	Substantive	***The Framework can also foster collaboration across the organization, which can result in an overall improvement in the enterprise's security posture.***
23	Expand on importance of ERM/cyber risk alignment in the beginning (helps streamline, ensures consistency, etc.)	Page 20, Section 4, Lines 684-685	Substantive	.....risk considerations, including cybersecurity. ***Aligning ERM with cybersecurity risk management helps standardize how cyber risks are identified, assessed, managed, monitored and reported on. Organizations can also*** benefit from using the Framework to better harmonize cybersecurity risk management activities with other risk management domains.
24	Minor edit.	Page 21, Section 4, Lines 703-704	Substantive	Including ERM-related input (e.g., enterprise risk categories, ***risk tolerance and risk appetite levels*** , priorities, integrated risk 704 registers) when gathering information needed to prepare the Profiles (step 2).