# Commentary on the NIST Cybersecurity Framework 2.0

The following pages contain comments on the draft copy of Cybersecurity Framework 2.0 written and assembled by the participants in the Georgetown University course "Cybersecurity Communications" (UNXD 4370). This class is part of the CyberCorps Scholarship for Service program. The only enrollees in the course are those selected as Georgetown CyberCorps Scholarship recipients (often called "CyberFellows"). Consequently, the comments that follow come from students who have a deep interest in the Cybersecurity Framework; they have committed to working in an executive branch agency in a cybersecurity position and thus will be primary users of Cybersecurity Framework 2.0 in the years ahead.

In the course, we review best practices from technical communications, including the guidelines for the 2010 Plain Writing Act (plainlanguage.gov). We also apply those best practices to challenges relevant to CyberFellows' future cybersecurity positions. So when I saw that NIST had released a new draft of its Cybersecurity Framework and was requesting public feedback, I challenged class members to provide their own feedback. They jumped at the opportunity.

Two qualifications:

- I instructed the students on best practices in technical communications, so any errors or omissions in that instruction are mine alone.
- I instructed the students that the Plain Writing Act covers the Cybersecurity Framework. That instruction was informed by my years as lead for the Federal Plain Language Report Card (2018-2021), and my years on the Board of the Center for Plain Language (2018-present).

Finally, I want to say that I'm proud of my students' work in the pages that follow. These students represent the best of their generation, and I'm heartened that they will be contributing to our nation's information security in the coming years. Indeed, as the following pages demonstrate, they have already begun to contribute.

I hope you find the following comments useful.

Sincerely,

David Lipscomb
Associate Teaching Professor
Georgetown University
[redacted]

**Comments on the Executive Summary**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 70-72 | Potential impacts to organizations from cybersecurity risks include higher costs, lower revenue, reputational damage, and impairment of innovation. | Cybersecurity risks can disrupt organizations through higher costs, lower revenue, reputational damage, and innovation impairment. | Remove unnecessary words and shorten sentence, per Sections III.a.3.ii and III.b.1 of the Plain Language Guidelines. |
| 74-76 | The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them. | The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate those risks and the actions that will reduce them. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 81-83 | These outcomes can be used to focus on and implement strategic decisions that improve cybersecurity postures (or state) while also considering organizational priorities and available resources. | These outcomes can help implement strategic decisions that improve cybersecurity postures (or state) while also considering organizational priorities and available resources. | Unnecessary use of the passive voice. See Section 3.a.1.i of the Plain Writing Guidelines. |
| 86-88 | The CSF also describes the concepts of Profiles and Tiers, which are tools to help organizations put the CSF into practice and set priorities for where they need or want to be in terms of reducing cybersecurity risks. | The CSF also describes the concepts of Profiles and Tiers, which are tools to help organizations put the CSF into practice and set priorities for reducing cybersecurity risks. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |

**Comments on the Introduction**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 108-110 | Determine where an | Determine where an | Remove unnecessary |

| | | | |
|---|---|---|---|
| | organization may have cybersecurity gaps, including with respect to existing or emerging threats or technologies, and assess progress towards addressing those gaps. | organization may have cybersecurity gaps, especially regarding existing or emerging threats or technologies, and assess progress towards addressing those gaps. | words (“including with respect to”) in order to shorten sentence, per Sections III.a.3 and III.b.1 of the Plain Language Guidelines. |
| 123-126 | Complement an organization’s risk management process by presenting a concise way for executives and others to distill the fundamental concepts of cybersecurity risk so that they express at a high level risks to be managed and how their organization uses cybersecurity standards, guidelines, and practices. | Complement an organization’s risk management process by providing a concise way for executives and others to simplify fundamental concepts of cybersecurity. Simplifying these concepts will support high-level communication of risk management and support organizations’ use of cybersecurity standards, guidelines, and practices. | Break the sentence in two to avoid overwhelming the reader. |
| 138-140 | The Framework applies to all information and communications technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT) used by an organization. | The Framework applies to all information and communications technology (ICT) used by an organization, including information technology (IT), the Internet of Things (IoT), and operational technology (OT). | Reorder sentence for clarity. |
| 146-149 | The Framework’s taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the Framework have been successfully leveraged by many governments and other organizations outside of the United States. | The Framework’s taxonomy, standards, guidelines, and practices are not country-specific, and previous versions of the Framework have been successfully leveraged by many governments and organizations outside of the United States. | Remove unnecessary words (“referenced”), per Section III.a.3 of the Plain Language Guidelines. |
| 150-151 | The primary audience for the Framework consists of | Individuals developing and leading cybersecurity | Remove unnecessary words, per Sections |

| | | | |
|---|---|---|---|
| | those responsible for developing and leading a cybersecurity program. | programs are the primary audience for the Framework. | III.a.3.ii and III.b.1 of the Plain Language Guidelines. |

**Comments on Section 2**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 179-180 | …the specific actions taken to achieve a cybersecurity outcome will vary by organization and use case, as will the individual responsible for those actions. | …the specific actions taken to achieve a cybersecurity outcome will vary by organization and use case as the framework provides guidance to enhancing cybersecurity | Remove unnecessary words and shorten sentence, per Sections III.a.3.ii and III.b.1 of the Plain Language Guidelines. |
| 181-184 | the Core is not intended to imply the sequence by which they should be implemented or their relative importance. The ordering of the Core is intended to resonate most with those charged with operationalizing risk management within an organization. | The core is intended to resonate most with those charged with operationalizing risk management within an organization. It does not specify order of implementation or relative importance. | Eliminate some wordiness to simplify sentence, per Section III.a.3.ii of the Plain Language Guidelines. Split into two sentences. |
| 193 | The GOVERN Function is cross-cutting and provides… | The GOVERN Function provides | Introduced earlier as cross-cutting, thus unnecessary and confusing |
| 201-204 | Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN. | …enables an organization to prioritize its efforts consistent with risk management strategy and the mission needs identified under GOVERN. | Remove unnecessary words (“referenced”), per Section III.a.3 of the Plain Language Guidelines. |
| 210-214 | Outcomes covered by this | Omit | Omit, no other |

| | | | |
|---|---|---|---|
| | Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure. | | section goes into as much detail about examples |
| 219-220 | RESPOND supports the ability to contain the impact of cybersecurity incidents. | RESPOND bolsters the ability to contain the impact of cybersecurity incidents | Reword for Clarity |
| 234-235 | To form and maintain a culture that addresses dynamic cybersecurity risk, the Functions should be addressed concurrently. | Use Functions holistically to form and maintain a culture that addresses dynamic cybersecurity risk. | Reverse sentence order for clarity. |

**Comments on Section 3**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 276 | The Framework can be used in numerous ways. Its use will vary based on an organization's unique mission and risks. | The Framework's use will vary based on an organization's unique mission and risks. | Unnecessary use of the passive voice per Section 3.a.1.i of the Plain Writing Guidelines. |
| 295 - 297 | Regardless of the application of the Framework, organizations likely will find it helpful to think of the Framework as guidance to help them to understand, assess, prioritize, and communicate about those cybersecurity risks and the actions that will reduce those risks. | Regardless of its application organizations can think of the Framework as guidance to help them understand, assess, prioritize, and communicate cybersecurity risks and the risk reduction actions. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 355 - 356 | The use case defines the high-level facts and assumptions on which the | The use case defines the high-level facts and assumptions that | Unnecessary use of the passive voice per Section 3.a.1.i of the |

| | | | |
|---|---|---|---|
| | Profiles will be based, as a way of scoping the Profiles. | organizations will use as the basis for the Profiles. | Plain Writing Guidelines. |
| 364 - 367 | An organization can gather relevant resources prior to preparing the Profiles, such as organizational policies, risk management priorities and resources, cybersecurity requirements and standards followed by the organization, and work roles. | An organization can gather resources before preparing the Profiles, such as organizational policies, risk management priorities and resources, requirements and standards, and work roles. | Remove unnecessary words like “prior to”, per Section III.a.3 of the Plain Language Guidelines. |
| 370 - 372 | Determine what types of supporting information (also known as elements) each Profile should include for each of the selected Framework outcomes, and fill in the elements for each selected outcome. | Determine what types of information (also known as elements) the Profile should include for the Framework outcomes, and fill in the elements for each selected outcome. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 383 - 386 | Identifying and analyzing the differences between the Current and Target Profiles enables an organization to identify gaps and develop a prioritized action plan for addressing those gaps to improve cybersecurity. | Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan to address those gaps. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 390 - 392 | The organization follows the action plan to adjust its cybersecurity practices to address gaps and move toward the Target Profile. | The organization addresses gaps and moves toward the Target Profile by executing the action plan to adjust its cybersecurity practices. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 399 - 401 | Profile development can be improved through communication across an organization, including but not limited to key stakeholders from executive leadership, risk management, security, legal, human resources, acquisition, and operations. | Organizations can improve how they develop internal communication with key stakeholders. | Use the active voice and eliminate the unnecessary list. (Section 3.a.1.i of the Plain Writing Guidelines) |
| 450 - 452 | Tiers characterize the rigor | Tiers characterize the rigor | Remove unnecessary |

| | | | |
|---|---|---|---|
| | of an organization's cybersecurity risk governance and management outcomes, and they provide context on how an organization views cybersecurity risks and the processes in place to manage those risks. | of an organization's risk governance and management outcomes. *They* provide context on how an organization views cybersecurity risks and its risk management processes. | words (Section III.a.3 of the Plain Language Guidelines). |
| 459 - 461 | For example, an organization can use the Tiers to communicate internally as a benchmark for a more organization-wide approach to managing cybersecurity risks as necessary to progress to a higher Tier. | An organization can use the Tiers to communicate internally a benchmark for an organization-wide approach to managing cybersecurity risks and move to a higher Tier. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 484 - 485 | One of the most common benefits of using the Framework is improving communication regarding cybersecurity risks and posture with those inside and outside of an organization. | One of the most common benefits of using the Framework is improving internal and external communication on cybersecurity risks and posture. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |
| 550 - 551 | The Framework can be used to foster an organization's oversight and communications related to cybersecurity risks with stakeholders across supply chains. | Organizations can use the framework to foster oversight and communications with stakeholders related to cybersecurity risks across supply chains. | Unnecessary use of the passive voice per Section 3.a.1.i of the Plain Writing Guidelines. Also, we are unsure what you mean by *"foster oversight with stakeholders."* |
| 565 - 567 | Today, nearly all organizations depend on supply chains. As such, it is increasingly important that they develop capabilities and implement practices to identify, assess, and respond to cybersecurity risks throughout the supply chain. | Since nearly all organizations depend on supply chains, it is increasingly important that they develop capabilities and implement practices to identify, assess, and respond to cybersecurity risks throughout those chains. | Remove unnecessary words, per Section III.a.3 of the Plain Language Guidelines. |

**Comments on Section 4**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 4, 623-625 | In addition to cybersecurity risks, every organization faces numerous other types of risk and may use frameworks and management tools that are specific to them. Sometimes two types of risk have commonalities, as Fig. 7 depicts through overlapping cybersecurity and privacy risks. | Organizations face many types of risk beyond cybersecurity and may use frameworks and management tools specific to each risk. These risks can have commonalities, overlapping multiple risk types (as shown in Fig. 7). | Readability and consistency with previous parenthetical introductions of figures (such as Fig. 6, introduced at 3.4.1 492). |
| 4, 633-635 | The outer border of Fig. 7 indicates an organization's full range of ERM risks, with examples of risks including financial, legal, operational, physical security, reputational, and safety — in addition to cybersecurity and privacy risks. | The outer border of Fig. 7 indicates an organization's full range of ERM risks. It includes examples of financial, legal, operational, physical, security, reputational, cybersecurity, and privacy risks. | Split into two sentences and remove unnecessary words in line with the Plain Language Guidelines, sec. III.a.3.ii. |
| 4.1, 642 - 643 | However, privacy risks can also be unrelated to cybersecurity incidents. | In other cases, privacy risks and cybersecurity risks are distinct. | Removal of unnecessary words for conciseness in line with the Plain Language Guidelines, sec. III.a.3.ii. |
| 4.1, 644-654 | Organizations process data to achieve mission or business purposes, which can give rise to privacy events whereby individuals may experience problems as a result of the data processing.<br>NIST describes these problems as ranging from dignity-type effects, such as embarrassment or<br>stigma, to more tangible harms, such as discrimination, economic | Organizations process data to achieve mission or business purposes. Data processing can create privacy issuers for individuals. Cybersecurity activities can result in over-collecting or retaining personal information or disclosing or using | Paragraph argues circuitously; Remove unnecessary words and write short sentences per sec. III.a.3.ii and sec. III.b.1, respectively. |

| | | | |
|---|---|---|---|
| | loss, or physical harm.2 Consequently, when organizations are processing data to conduct cybersecurity activities, they can create privacy risks. For example, some types of incident detection or monitoring activities — particularly those conducted in a manner disproportionate to the intended purpose — may lead individuals to feel surveilled. Additionally, cybersecurity activities can result in the over-collection or over-retention of personal information or the disclosure or use of personal information unrelated to cybersecurity activities. These activities can lead to problems such as embarrassment, discrimination, and loss of trust. | personal information unrelated to cybersecurity activities. NIST describes these problems as ranging from harm to an individual's dignity, such as embarrassment or stigma and a feeling of being under surveillance, to more tangible harm, such as discrimination, economic loss, loss of trust, and even physical harm. | |
| 4.1, 655-662 | The NIST Cybersecurity Framework and the NIST Privacy Framework can be used together to collectively address cybersecurity and privacy risks, as illustrated by Fig. 8. As the right side of the Venn diagram depicts, organizations using the Cybersecurity Framework to manage cybersecurity risks can leverage the Privacy Framework Identify-P, Govern-P, Control-P, and Communicate-P Functions to identify and manage privacy risks unrelated to cybersecurity incidents, such as those described above. The Cybersecurity Framework DETECT, RESPOND, and RECOVER Functions and the Privacy Framework Protect-P Function can be collectively leveraged to support the | Organizations may use the NIST Cybersecurity Framework and NIST Privacy Framework to address cybersecurity and privacy risks, as illustrated by Fig. 8. As shown by the right side of the Venn diagram, organizations may use the Privacy Framework Identify-P, Govern-P, Control-P, and Communicate-P Functions to identify and manage privacy risks that are unrelated to cybersecurity incidents. In contrast, organizations may collectively leverage the Cybersecurity Framework DETECT, RESPOND, and RECOVER Functions | Keep subject, verb and object close together per Plain Language Guidelines III.b.2. Use active voice, per sec III.a.1.i. |

| | | | |
|---|---|---|---|
| | management of overlapping cybersecurity and privacy risks. | and the Privacy Framework Protect-P Function to manage privacy and cybersecurity risks that do overlap. | |
| 4.1, 665-666 | When reviewing cybersecurity programs for privacy risks, an organization can consider taking actions such as the following: | Organizations reviewing cybersecurity programs for privacy risks can consider taking the following actions: | Reorganize the sentence and remove unnecessary words in line with the Plain Language Guidelines, sec. III.a.3.ii. |
| 4.1, 677-678 | Conduct privacy reviews of an organization's asset monitoring and detection of adverse cybersecurity events and incidents, as well as its cybersecurity incident mitigation efforts | Review an organization's asset monitoring, detection of adverse cybersecurity events, and cybersecurity mitigation efforts for privacy issues. | Consistency in list per Plain Language Guidelines sec. III.a.3. |
| 4.1, 679-681 | Put processes in place to assess and address whether, when, how, and the extent to which individuals' data is shared outside of the organization as part of cybersecurity information-sharing activities | Implement processes to assess and address whether, when, how, and the extent to which cybersecurity information-sharing leads to the sharing of individuals' data outside of the organization | Clarity, omitting unnecessary words per Plain Language Guidelines III.a.3.ii. |
| 4.2, 688-690 | Integrated data about a broad set of risks, including cybersecurity risk data, helps leaders understand potential risk changes so that they can make informed decisions about the direction of the enterprise. | Integrated data about a broad set of risks, including cybersecurity risks, helps leaders make informed decisions about the direction of the enterprise. | Conciseness, cutting unnecessary elaboration pursuant to Plain Language Guidelines sec. 3.a.ii. |
| 4.2, 694 | …in conjunction with the Cybersecurity Framework, to… | …along with the Cybersecurity Framework (CSF), to… | Enumerates the meaning of CSF for its later use at 696, |

| | | | |
|---|---|---|---|
| | | | consistent with recommendations for definitions from Plain Language Guidelines 3.a.iii. |
| 4.2, 697 | …Cybersecurity Framework users. | …CSF users. | Consistent with the above comment. |

**Comments on Section 5**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| 5, 726 | Whether an organization uses the Cybersecurity Framework for the first time or has used it previously, | *omit* | Omit for brevity |
| 5. 727<br>728 | it is important to remember that the CSF is designed to be used in727<br>conjunction with other cybersecurity frameworks, standards, and guidance. | Organizations should implement CSF in tandem with other cybersecurity frameworks, standards, and guidance. | Replace passive voice with active |
| 5.<br>729-730 | NIST provides many resources that are specific to the Framework and its use on the Cybersecurity Framework website, | NIST provides many resources that are specific to the Framework and its use on the Cybersecurity Framework website. | Removed run-on sentence; changed comma to period |
| 5.<br>730-732 | as well as hundreds of cybersecurity publications and other resources hosted on the NIST Computer Security Resource Center (CSRC) website and the NIST<br>National Cybersecurity Center of Excellence (NCCoE) website. | Additionally, NIST hosts hundreds of cybersecurity publications and other resources on the Computer Security Resource Center (CSRC) website and the National | Removed run-on sentence. Removed passive voice for active. |

| | | | |
|---|---|---|---|
| | | Cybersecurity Center of Excellence (NCCoE) website. | |
| 5.<br>732-734 | While these resources are not part of the Framework Core, they provide detailed information on cybersecurity risk management that supports use of the Framework. | Although not a part of the CSF Framework Core, these resources provide detailed information on cybersecurity risk management that supports using the Framework. | Reworded; and removed hidden verb |
| 5.<br>741-742 | As organizations continue on their cybersecurity journey, NIST is committed to providing guidance to address current and future cybersecurity challenges. | As organizations continue to strengthen their cybersecurity posture, NIST is committed to helping address cybersecurity challenges of the present and future. | Reworded |

**Comments on the Appendices**

| Location | Original | Proposed | Commentary |
|---|---|---|---|
| Appendix A, 744-745 | This appendix provides notional templates that organizations can choose to use and adapt for their own Profiles and action plans. | This appendix offers example templates that organizations have the option to use and adapt for creating their own Profiles and action plans. | Make clear. |
| Appendix A, 751-753 | Organizations may downselect outcomes or add their own Functions, Categories, or Subcategories to address specific needs or unique organizational risks. | Organizations may narrow down outcomes or incorporate their own Functions, Categories, or Subcategories to | Use familiar words, per Sections III.a.3.i Plain Language Guidelines. |

| | | | |
|---|---|---|---|
| | | address specific needs or unique organizational risks. | |
| Appendix A.1. 754-757 | Elements chosen by the organization… posture. Elements chosen by…goals. | Categories specific to the organization … posture. Categories specific to the organization…goals. | Use concrete, rather than abstract words, per Sections III.a.3.i Plain Language Guidelines. |
| Appendix A.1. 777-780 | For example, a policy might state that access to resources requires a certain degree of authorization and a supporting procedure might specify the correct access control rules for requesting and approving access to a specific software component. | For example, a policy might require specific authorization to access resources. A supporting procedure might then specify the access control rules for a particular software component. | Make concise. |
| Appendix B, | Entirety | Section should incorporate language of “responsible parties” to reduce use of passive voice and establish agents. | |
| Appendix B 812 | Table 3 describes the Framework Tiers discussed in Section 3.2. | Table 3 describes the Framework Tiers discussed in Section 3.3. | Section 3.3, not 3.2, discusses Framework Tiers. |
| Appendix B Tier 2: Risk Informed | Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. | Management prioritizes cybersecurity activities and protection needs based on organizational risk objectives, the threat environment, or business/mission requirements. | Incorporate actor responsible for implementing change. Use active voice. (Plain Language Guidelines III.a.1.i) |
| Appendix B Tier 2: Risk Informed | Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. | Some but not all levels of the organization may consider cybersecurity in their | Use active voice. (Plain Language Guidelines III.a.1.i) |

| | | | |
|---|---|---|---|
| | | objectives and programs. | |
| Appendix B Tier 2: Risk Informed | The organization understands the cybersecurity risks in its supply chains that are associated with the products and services that either support the business and mission functions of the organization or are utilized in the organization's products or services. | The organization understands the cybersecurity risks in its supply chains that either support the business and mission functions of the organization or are utilized by the organization's products or services | Make more concise. (Plain Language Guidelines III.a.3.ii) |
| Appendix B Tier 3: Repeatable | An organization-wide approach to managing cybersecurity risks in its supply chains is instantiated in the organization's enterprise risk management policies, processes, and procedures, which are in turn implemented consistently and as intended and continuously monitored and reviewed. | An organization-wide approach to managing cybersecurity risks in its supply chains is integrated in the organization's enterprise risk management policies, processes, and procedures. The organization consistently implements and continuously monitors this approach. | Split long sentence into two sentences. (Plain Language Guidelines III.b.1)<br><br>Find a better word for instantiated |
| Appendix B Tier 4: Adaptive | The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. | Decision-makers clearly understand and consider the relationship between cybersecurity risks and organizational objectives. | Use active voice. (Plain Language Guidelines III.a.1.i) |