

Mike Sanderson
October 12, 2026

m@mikesand.com / mikesand.ai

Comment on draft Quick-Start Guide for Using AI for CSF Analysis and Reporting (NIST SP 1353 ipd, Initial Public Draft).

Intro: My background. I have been a mobile app developer for 13 years, and have focused on security. Earlier this year I gave a talk on security to a New York iOS developers group¹ and was happy to recommend using the NIST Cybersecurity Framework for its simplicity and universality.

Appreciation for NIST CSF. The simplicity and authority of the CSF make it easy to recommend to all audiences.² From senior executives to highly technical developers, everyone benefits from CSF's simple, high-level image of cybersecurity. Its six Functions fit on a PowerPoint slide, yet they rigorously link down to Categories and Subcategories that then map to technical standards.³ Graphics in the CSF show its structure and purpose visually: I think of the images "CSF Core structure" (Fig. 1) and "Using the CSF to improve risk management communication" (Fig. 5) in the main CSF white paper.⁴

Therefore, it's great that SP 1353 continues that focus, since CSF's real strength is its value to an audience of executive decision makers.

Signposts to the comment. This comment has four parts:

1. a suggestion to use the classic "Swiss cheese" metaphor for AI hallucinations;
2. a suggestion to provide guidance on selecting models;
3. importance of "Analysis and Reporting" emphasis;
4. uses of the CSF with agentic AI, in answer to your request for use case ideas.⁵

1. Swiss Cheese. Layers of sliced Swiss cheese laid on top of each other are a classic security metaphor for how to compensate for unavoidable holes. This ready-made image is also useful for thinking about the unavoidable problem of AI hallucinations. The bullet point on p. 3, right column box, "Consider using multiple AI tools and comparing results when validating AI output"⁶, would be an excellent point to use this metaphor, and in other places.⁷ Suggested change: add to the "Next steps" on p. 9: run the same prompt several times on the same material and compare the runs.⁸

2. Model Selection and Context Window Size. The selection of the model is a choice literally anyone using AI will need to make, yet it isn't mentioned beyond choosing an authorized tool (or tools)⁹; the nearest the guide comes to model advice is "use a more advanced processing option."¹⁰ Selecting different models could be linked to the Swiss cheese metaphor, as different models will have different results. However, it also could be mentioned how important the size of the context window is for the size and complexity of the possible analysis, given that the documents are of varying size. Users of agents face the choice of model immediately and will want to know how to approach the decision in the quick-start context. (NIST does not endorse models¹¹, but the guide can name basic criteria of context window size for size of documents.)

3. Importance of “Analysis and Reporting” emphasis. This point is made in the SP 1353 title¹²; nevertheless, I believe it must be emphasized for as wide an audience as possible, because I think it has the potential to be widely misunderstood. CSF is for communication, not investigation. CSF 2.0’s abstract says something similar: the CSF helps organizations “understand, assess, prioritize, and communicate” their cybersecurity efforts.¹³

Fig. 5 in CSF 2.0, “Using the CSF to improve risk management communication” (p. 10), is my go-to for visualizing this process—up and down the corporate ladder.¹⁴

4. Use-cases.

A. Use-cases for Executives. This is the audience CSF 2.0 says GOVERN serves (p. 11):

- To develop an understanding of how CSF relates to their industry, their platforms, and their specific concerns, and of what specific questions they could be asking.

B. Use-cases for developers and front-line security analysts.

- For interactively developing an understanding of potential issues in their industry, their specific platform and their codebase.
- For work-tracking tickets, to identify security requirements and attach them, so that product managers can see the additional, unseen work that developers need to perform.
- Translating reports for higher levels.¹⁵ The product of a highly technical security scan could be converted into bullet points, allowing, for example, high-level PowerPoint slides to be backed by CSF Categories and Subcategories off-page.¹⁶
- Educational exercises. Like the exercises in the supplemental materials, CSF with agents would be suitable for exercises with code problems aimed at new developers or even at non-developers who would like a sense of what these issues look like in code.

C. Use-cases to avoid for developers and front-line security analysts. An important caveat: CSF with agentic AI should *not* be considered best practice for:

- ⚠ hunting of weaknesses and vulnerabilities by front-line developers and security researchers.

The reason is the focus of the agent and the size of the context window: every token spent on a high-level framework is a dot not connected down the line. It should not be best practice to use the CSF in agentic AI to find vulnerabilities—although certainly better than nothing—but instead, in my estimation, best practice would be stripping the prompt down to the minimum for the platform and area being scanned. The guide already treats scan results as “assessment artifacts” inputs (p. 5)¹⁷, and treats the CSF as a way to interpret outcomes in them; that is an effective use for agents applying the CSF.¹⁸

Conclusion: Thank you for the work NIST puts into the CSF and all its initiatives. Its simplicity and authority improve communication about cybersecurity in all audiences.

Notes

1. Mike Sanderson, "Beyond the Sandbox: Secure iOS Development in an Era of New Security Standards," talk at iOsoho, New York, February 26, 2026; video, starting at 18:55: <https://www.youtube.com/watch?v=HhBOKaw4rFQ&t=1135s>
2. CSF 2.0 (NIST CSWP 29), p. 1: its outcomes "can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise."
3. NIST, "CSF 2.0 Informative References," <https://www.nist.gov/cyberframework/csf-20-informative-references>. It lists CSF 2.0 mappings for SP 800-53 Rev. 5.2.0, SP 800-171 Rev. 3, ISO/IEC 27001:2022, PCI DSS 4.0.1, CIS Controls 8.1 and the Cloud Controls Matrix 4.0.
4. CSF 2.0, Fig. 1, "CSF Core structure" (p. 3), and Fig. 5, "Using the CSF to improve risk management communication" (p. 10).
5. SP 1353 ipd, p. 2: "Have an interesting AI use case for the CSF? Submit additional use case ideas to: csf@nist.gov."
6. SP 1353 ipd, p. 3: "Consider using multiple AI tools and comparing results when validating AI output."
7. Other places in SP 1353 ipd where the metaphor fits: p. 3: "Effective Prompt Engineering Helps Support Consistent and Repeatable CSF 2.0 Outcomes"; p. 7, which repeats the p. 3 bullet; and p. 9: "Results can change over time or may vary."
8. SP 1353 ipd, p. 9: "Next steps might include: repeat the process with a new use case, try a different AI tool and compare results, or explore how refining the prompts impacts outputs."
9. SP 1353 ipd, p. 7: "Choose an AI tool (or tools) authorized for use by the organization's security and privacy team."
10. SP 1353 ipd, p. 9: "When presented with options, use a more advanced processing option to reduce likelihood of hallucinations (though they can still occur)."
11. SP 1353 ipd, p. 3: "This usage does not imply that the models, software, profiles or services are the best available for this purpose, nor does it imply recommendation or endorsement by NIST."
12. SP 1353 ipd, cover.
13. CSF 2.0, p. i (Abstract).
14. CSF 2.0, p. 10, Fig. 5 and Section 5.1: "The CSF fosters bidirectional information flow (as shown in the top half of Fig. 5) between executives ... and managers ..."
15. SP 1353 ipd, p. 6 (Use Case 3): "Translating technical outcomes into plain-language descriptions suited to different audiences (e.g., executives, auditors, technical teams)."
16. Use Case 3 - Full Prompt.txt, AUDIENCE: "Write so that a row can be lifted into any of those three contexts without rewriting." (the Board risk committee, the Chief Compliance Officer and Internal Audit)
17. SP 1353 ipd, p. 5: "Assessment artifacts (e.g., prior risk assessments, internal/external audit findings, penetration test reports, and vulnerability scan results)."
18. Use Case 2 - Full Prompt.txt, CONTEXT, "Sources": "CSF and CRI text may be used to interpret what an outcome means, never as evidence of what this organization does."

References

- National Institute of Standards and Technology (2026) NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using Artificial Intelligence (AI) for CSF Analysis and Reporting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1353 ipd. <https://doi.org/10.6028/NIST.SP.1353.ipd>
- National Institute of Standards and Technology (2026) Supplemental files for NIST SP 1353 ipd: Use Case 1–3 prompt files (UseCase1-GovernanceReview.zip, UseCase2-CurrentStateProfile.zip, UseCase3-TargetStateProfile.zip). <https://csrc.nist.gov/pubs/sp/1353/ipd>

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. <https://doi.org/10.6028/NIST.CSWP.29>

National Institute of Standards and Technology, "CSF 2.0 Informative References."
<https://www.nist.gov/cyberframework/csf-20-informative-references>

Sanderson M (2026) Beyond the Sandbox: Secure iOS Development in an Era of New Security Standards. Talk at iOSoho, New York, February 26, 2026. Video (talk starts at 18:55):
<https://www.youtube.com/watch?v=HhBOKaw4rFQ&t=1135s>