

Invitation for Public Comments on “The Cyber/Physical Security Framework version 1.1 (Draft)”

1. Background and purpose

The Ministry of Economy, Trade and Industry (METI) formulated the Cyber/Physical Security Framework (CPSF) Version 1.0 in April 2019, recognizing the growing importance of security measures in the “Value Creation Process,” where supply chains dynamically change, in line with the advancement of “Society 5.0,” which aims to highly integrate cyberspace and physical space, and “Connected Industries,” seeking to create new value through cross-industry data collaboration utilizing digital technologies.

Since first publication of CPSF, the cybersecurity landscape has changed significantly. While advances in digital technologies, such as the widespread adoption of cloud services and the increasing sophistication of IoT devices, have made supply chain connections more complex, cyberattacks have also become more sophisticated and organized. As a result, threats facing industries have reached unprecedented levels. In this context, the globally referenced NIST Cybersecurity Framework (NIST CSF) and ISO/IEC 27001 have been revised, creating a greater need for more practical cybersecurity measures.

In light of these developments, METI have compiled a draft revision of the Cyber/Physical Security Framework (CPSF) in order to further promote efforts to ensure cybersecurity across the entire supply chain of Japanese industry.

In this revision, particular emphasis has been placed on reflecting international developments, including NIST CSF 2.0. Furthermore, from the next fiscal year onward, we plan to consider additional revisions in response to developments related to the utilization of AI and evolving threat trends.

We hereby invite comments from the public in accordance with the procedures outlined below. We would appreciate receiving your candid opinions and suggestions.

2. Topic for comments

- “The Cyber/Physical Security Framework version 1.1(Draft)”
- Appendix A (Use case) (Draft)
- Appendix B (Relationship between risk source and measure requirements) (Draft)
- Appendix C (Examples of security measures according to measure requirements) (Draft)
- Appendix D (Relationship with major overseas standards) (Draft)
- Appendix E (Glossary) (Draft)

3. Access to the documents

The materials are available on the e-Gov portal, the comprehensive website for electronic government services.

4. Due date

Submissions must be received by the deadline from Friday, October 23, 2026, until Monday, December 21, 2026 (Japan Standard Time, UTC+0900).

5. Submission of comments

Please proceed to the comment submission form available via the e-Gov portal (Note: instructions are provided in Japanese only) and submit your comments in either Japanese or English.

If accessing the e-Gov is difficult, you may complete the comment submission form provided in the attached document in either Japanese or English and send it via email to the address below:

- Email address : bz1-cyber-guideline_pubcon@meti.go.jp

(Please include "Comments on the Cyber/Physical Security Framework version 1.1(Draft)" in the subject line and attach the completed submission form.)

Note: Comments cannot be submitted via telephone. We appreciate your understanding.

6. Notes

The comments received will be used as a reference for making final decisions. However, please note that individual responses to submitted comments will not be provided. We kindly ask for your understanding in this regard.

Please note that the submitted comments may be made publicly available, excluding personal information such as names, addresses, phone numbers, fax numbers, and email addresses. However, if the submitted comments include personal information that could identify specific individuals or contain descriptions that may harm the rights or interests of individuals, corporations, or other entities, those portions will be redacted before publication.

Any personal information, such as names and contact details, provided with your comments will be properly managed and used solely for the purpose of contacting or confirming unclear points regarding the submitted comments as part of this public consultation process.

Cybersecurity Division and Digital Economy Division, Commerce and Information Policy Bureau

Comments on “The Cyber/Physical Security Framework version 1.1(Draft)”

[Name]	
[Address]	
[Tel]	
[Email]	
[Comment]	
▪ Corresponding passage (Please specify which headings in the draft your comments are addressing) ▪ Content ▪ Reason (If possible, please attach or include any supporting references or sources as evidence)	