June 27, 2025

Invitation for Public Comments on the “(Draft)OT Security Guidelines for Semiconductor Device Factories”

１．Background and purpose

Cyberattacks have increasingly becoming diverse and sophisticated, and various control systems with operational technology (OT) have been attacked, causing serious damage such as interruptions of factory production. Additionally, there is also an increasing risk that various confidential information for development (i.e., intellectual property) could be leaked through cyberattacks. Considering the economic and national security importance of the semiconductor industry and the growing cyber threats and risks at present, it is imperative to implement and strengthen security measures, including countermeasures against advanced cyberattacks. On the international stage, global semiconductor industry association SEMI has developed the E187 and E188 Standards for semiconductor manufacturing equipment. Furthermore, National Institute of Standards and Technology (NIST) is working on the development of a semiconductor manufacturing profile for its Cybersecurity Framework 2.0 (hereinafter referred to as NIST CSF 2.0).

On the other hand, in Japan, the Ministry of Economy, Trade and Industry (METI) formulated and published the "Cyber/Physical Security Guidelines for Factory Systems" in 2022, which are aimed at generic assembly-type factories. However, semiconductor factories, which are generally categorized as process automation (PA) type factories, are characterized by their large scale and the significant number of manufacturing equipment that utilize general-purpose operating systems (OS). As a result, it has been observed that these guidelines are not well-suited to the specific needs of semiconductor factories.

Under this awareness of the issues at hand, METI has convened the Semiconductor Industry Sub-Working Group, under the Industrial Cybersecurity Study Group, since November 2024. Chaired by Professor Ezaki of the University of Tokyo, this sub-working group has engaged in discussions on the optimal approaches to security measures for OT in semiconductor device factories in Japan. These discussions have involved a diverse range of stakeholders, including domestic and international companies and organizations, such as semiconductor device manufacturers and semiconductor manufacturing equipment providers.

As a result of these discussions, we have compiled the outcomes into a draft document titled the "(Draft)OT Security Guidelines for Semiconductor Device Factories." This document serves as a set of guidelines for factory security measures tailored to semiconductor device factories, ensuring alignment with various international security standards established within the global semiconductor industry. Given that Japan’s semiconductor industry operates within the framework of an international supply chain, we aim to gather broad feedback from stakeholders both domestically and internationally. To this end, we will conduct a 60-day public comments starting today, making both the Japanese and English versions of the draft guidelines available for review and comment.

２.　Topic for comments

・ “(Draft)OT Security Guidelines for Semiconductor Device Factories”

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, June 27, 2025, until Tuesday, August 26, 2025 (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：bzl-cybersec_comment@meti.go.jp

(Please include "Comments on the OT Security Guidelines for Semiconductor Device Factories (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.

Division in Charge

Cybersecurity Division / Information Industry Division, Commerce and Information Policy Bureau

Comments on the “(Draft)OT Security Guidelines for Semiconductor Device Factories”

［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)	