PUBLIC SUBMISSION

As of: 4/25/22 12:55 PM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2e-gloe-od1d
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0038
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Keidanren Japan Business Federation

General Comment

Views on Revision of the NIST Cybersecurity Framework

April 25, 2022

Cybersecurity Enhancement Working Group
Committee on Cyber Security
Keidanren

1. Relationships among Frameworks
We would suggest clarifying the relationship among NIST SP800 series publications in the cybersecurity framework (CSF) documents. For example, if companies also apply SP800-207 (Zero-Trust Architecture) when taking measures using the NIST CSF and SP800-171, it would be useful to have some indication of effects on the five core functions.

2. Relative Importance of the CSF Function Categories/Subcategories
Since recent updates to the NIST CSF have tended to emphasize the “respond” and “recover” functions, we suggest a review of the relative importance of the function categories/subcategories.

3. Request for Future Framework Updates
Japan is looking ahead to a society where all people and things are connected via the Internet of Things, a concept we call “Society 5.0.” Many companies in Japan utilize the NIST CSF when implementing cybersecurity measures. As part of such measures, companies need to minimize shutdowns of system interoperability and thus minimize “respond” and “recover” actions. When an incident occurs, business must be halted once the “respond” and “recover” phases are reached.

To avoid reaching this point, it is important to introduce the Zero-Trust Architecture (ZTA) concepts of

SP800-207, establish a new “prevent” phase between the “protect” and “detect” phases, and take preventive measures before an incident forces business to halt.

In the “prevent” phase, authenticity of all people (authentication), things (procurement, economic security), and processes related to the supply chain should always be confirmed on a zero-trust basis.

Attachments

Keidanren 20220425 Views on Revision of the NIST Cybersecurity Framework

Views on Revision of the NIST Cybersecurity Framework

April 25, 2022

Cybersecurity Enhancement Working Group
Committee on Cyber Security
Keidanren

1. Relationships among Frameworks
   We would suggest clarifying the relationship among NIST SP800 series publications in the cybersecurity framework (CSF) documents. For example, if companies also apply SP800-207 (Zero-Trust Architecture) when taking measures using the NIST CSF and SP800-171, it would be useful to have some indication of effects on the five core functions.

2. Relative Importance of the CSF Function Categories/Subcategories
   Since recent updates to the NIST CSF have tended to emphasize the "respond" and "recover" functions, we suggest a review of the relative importance of the function categories/subcategories.

3. Request for Future Framework Updates
   Japan is looking ahead to a society where all people and things are connected via the Internet of Things, a concept we call "Society 5.0." Many companies in Japan utilize the NIST CSF when implementing cybersecurity measures. As part of such measures, companies need to minimize shutdowns of system interoperability and thus minimize "respond" and "recover" actions. When an incident occurs, business must be halted once the "respond" and "recover" phases are reached.

   To avoid reaching this point, it is important to introduce the Zero-Trust Architecture (ZTA) concepts of SP800-207, establish a new "prevent" phase between the "protect" and "detect" phases, and take preventive measures before an incident forces business to halt.

   In the "prevent" phase, authenticity of all people (authentication), things (procurement, economic security), and processes related to the supply chain should always be confirmed on a zero-trust basis.