PUBLIC SUBMISSION

As of: 4/25/22 12:41 PM
Received: April 22, 2022
Status: Pending_Post
Tracking No. l2a-jfd4-cuq3
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-0029
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Institute for Information Industry

General Comment

Supply-chain management (SCM) will be vital for the global high-tech industry especially in the post-pandemic era. The Taiwanese government has been dedicated in building a reliable global supply chain for ICT industry by enhancing the digital resilience in SCM practices. CSF by NIST has been the most discussed framework document since the delegates of BSMI (Bureau of Standards, Metrology and Inspection) under MoEA (Ministry of Economic Affairs) visited NIST in 2019 and CSF had been heavily promoted it to the industry ever since. All these efforts, eventually, rolled into the SCM development in the areas of high-tech industry such as 5G communications and semiconductor.

We appreciate NIST's efforts and hope NIST can continue working on the cybersecurity related matters for enterprises and help the industry understand that corporate cybersecurity protection is a responsibility an enterprise cannot dodge and should invest adequately. Furthermore, we hope NIST can continue providing the guidance for the managing level of the corporate team to help them understand their role is crucial in assisting the cybersecurity implementors.

Based on our experience over the past three years, in order to effectively increase the adoption level of the cybersecurity standards in the industry, it is necessary to have the government policy and the requirements from the industry working together. For example:
1. It should be a government policy that an enterprise above certain level (based on the revenue) should set up a department to focus on information protection and cyber security management with dedicated personnel.
2. An industrial control system should also take the life cycle of the installed software so that adequate security protection measure can be applied to prevent the addition of new equipment or new software from putting the existing machines (installed base) at risk.

The aforementioned point one is to streamline the flow of cybersecurity management in a global complex supply-chain. Most often, the entities in a supply chain are not from the same corporation and the conventional management structure do not apply. With assigned role and responsibility, a dedicated department or person will ensure the security measures and processes that are adequately followed and effectively enhance the speed of response to any security breaches.

On the second point, since the information security depreciation of legacy systems has long been neglected when enterprises or factories need to upgrade their systems, the outdated software operated in the system can be the weakest link and may jeopardize the overall security. . These problems usually cannot be solved by a single enterprise; as a matter of fact, it is necessary to solve the problem through cross-functional and cross-enterprise collaborations in the supply chain.

The roles of Taiwan have become more important especially in the global high-tech industry sector. The visibility also makes Taiwan's organizations to be the potential targets of malicious attacks. We are hoping to strengthen the work relation with NIST by providing more real cases to share the industry practices and measures based on the CSF.

Contributed by
1. Institute for Information Industry (Organization)
2. Mitch Tseng, Ph.D. (Managing Member, Tseng InfoServ, LLC)
3.Ming-Chang(Bright) Wu, WTW Taiwan (The views here are my own and do not necessarily reflect those of my employer)

Attachments

Request for Information_NIST-2022-0001

Request for Information

Supply-chain management (SCM) will be vital for the global high-tech industry especially in the post-pandemic era. The Taiwanese government has been dedicated in building a reliable global supply chain for ICT industry by enhancing the digital resilience in SCM practices. CSF by NIST has been the most discussed framework document since the delegates of BSMI (Bureau of Standards, Metrology and Inspection) under MoEA (Ministry of Economic Affairs) visited NIST in 2019 and CSF had been heavily promoted it to the industry ever since. All these efforts, eventually, rolled into the SCM development in the areas of high-tech industry such as 5G communications and semiconductor.

We appreciate NIST's efforts and hope NIST can continue working on the cybersecurity related matters for enterprises and help the industry understand that corporate cybersecurity protection is a responsibility an enterprise cannot dodge and should invest adequately. Furthermore, we hope NIST can continue providing the guidance for the managing level of the corporate team to help them understand their role is crucial in assisting the cybersecurity implementors.

Based on our experience over the past three years, in order to effectively increase the adoption level of the cybersecurity standards in the industry, it is necessary to have the government policy and the requirements from the industry working together. For example:

1. It should be a government policy that an enterprise above certain level (based on the revenue) should set up a department to focus on information protection and cyber security management with dedicated personnel.
2. An industrial control system should also take the life cycle of the installed software so that adequate security protection measure can be applied to prevent the addition of new equipment or new software from putting the existing machines (installed base) at risk.

The aforementioned point one is to streamline the flow of cybersecurity management in a global complex supply-chain. Most often, the entities in a supply chain are not from the same corporation and the conventional management structure do not apply. With assigned role and responsibility, a dedicated department or person will ensure the security measures and processes that are adequately followed and effectively enhance the speed of response to any security breaches.

On the second point, since the information security depreciation of legacy systems has long been neglected when enterprises or factories need to upgrade their systems, the outdated software operated in the system can be the weakest link and may jeopardize the overall security. . These problems usually cannot be solved by a single enterprise; as a matter of fact, it is necessary to solve the problem through cross-functional and cross-enterprise collaborations in the supply chain.

The roles of Taiwan have become more important especially in the global high-tech industry sector. The visibility also makes Taiwan’s organizations to be the potential targets of malicious attacks. We are hoping to strengthen the work relation with NIST by providing more real cases to share the industry practices and measures based on the CSF.

Contributed by

1. Institute for Information Industry (Organization)

2. Mitch Tseng, Ph.D. (Managing Member, Tseng InfoServ, LLC)

3.Ming-Chang(Bright) Wu, WTW Taiwan (The views here are my own and do not necessarily reflect those of my employer)