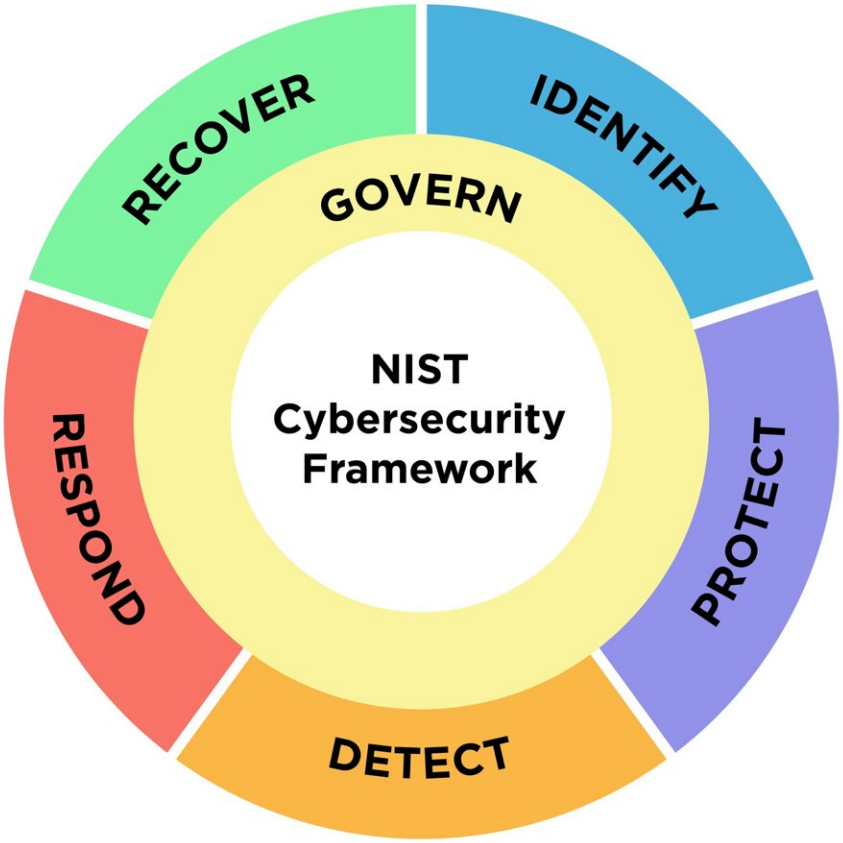
NIST drafts major update to its widely used cybersecurity framework

August 8 2023



To the five main pillars of a successful cybersecurity program, NIST now has added a sixth, the "govern" function, which emphasizes that cybersecurity is a major source of enterprise risk and a consideration for senior leadership. Credit: N. Hanacek/NIST

The world's leading cybersecurity guidance is getting its first complete makeover since its release nearly a decade ago.

After considering more than a year's worth of community feedback, the National Institute of Standards and Technology (NIST) has released a draft version of the Cybersecurity Framework (CSF) 2.0, a new version of a tool it first released in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The draft update, which NIST has released for public comment, reflects changes in the cybersecurity landscape and makes it easier to put the CSF into practice—for all organizations.

"With this update, we are trying to reflect current usage of the Cybersecurity Framework, and to anticipate future usage as well," said NIST's Cherilyn Pascoe, the framework's lead developer. "The CSF was developed for critical infrastructure like the banking and energy industries, but it has proved useful everywhere from schools and small businesses to local and foreign governments. We want to make sure that it is a tool that's useful to all sectors, not just those designated as critical."

NIST is accepting public comment on the draft framework until Nov. 4, 2023. NIST does not plan to release another draft. A workshop planned for the fall will be announced shortly and will serve as another opportunity for the public to provide feedback and comments on the draft. The developers plan to publish the final version of CSF 2.0 in

early 2024.

The CSF provides high-level guidance, including a common language and a systematic methodology for managing cybersecurity risk across sectors and aiding communication between technical and nontechnical staff. It includes activities that can be incorporated into cybersecurity programs and tailored to meet an organization's particular needs. In the decade since it was first published, the CSF has been downloaded more than two million times by users across more than 185 countries and has been translated into at least nine languages.

While responses to NIST's February 2022 request for information about the CSF indicated that the framework remains an effective tool for reducing cybersecurity risk, many respondents also suggested that an update could help users adjust to technological innovation as well as a rapidly evolving threat landscape.

"Many commenters said that we should maintain and build on the key attributes of the CSF, including its flexible and voluntary nature," Pascoe said. "At the same time, a lot of them requested more guidance on implementing the CSF and making sure it could address emerging cybersecurity issues, such as supply chain risks and the widespread threat of ransomware. Because these issues affect lots of organizations, including small businesses, we realized we had to up our game."

The CSF 2.0 draft reflects a number of major changes, including:

- The framework's scope has expanded—explicitly—from protecting critical infrastructure, such as hospitals and power plants, to providing cybersecurity for all organizations regardless of type or size. This difference is reflected in the CSF's official title, which has changed to "The Cybersecurity Framework," its colloquial name, from the more limiting "Framework for

Improving Critical Infrastructure Cybersecurity."

- Until now, the CSF has described the main pillars of a successful and holistic cybersecurity program using five main functions: identify, protect, detect, respond and recover. To these, NIST now has added a sixth, the govern function, which covers how an organization can make and execute its own internal decisions to support its cybersecurity strategy. It emphasizes that cybersecurity is a major source of enterprise risk, ranking alongside legal, financial and other risks as considerations for senior leadership.
- The draft provides improved and expanded guidance on implementing the CSF, especially for creating profiles, which tailor the CSF for particular situations. The cybersecurity community has requested assistance in using it for specific economic sectors and use cases, where profiles can help. Importantly, the draft now includes implementation examples for each function's subcategories to help organizations, especially smaller firms, to use the framework effectively.

A major goal of CSF 2.0 is to explain how organizations can leverage other technology frameworks, standards and guidelines, from NIST and elsewhere, to implement the CSF. Bolstering this last effort will be the launch of a CSF 2.0 reference tool, which NIST plans to release in a few weeks. This online resource will allow users to browse, search and export the CSF Core data in human-consumable and machine-readable formats. In the future, this tool will provide "Informative References" to show the relationships between the CSF and other resources to make it easier to use the framework together with other guidance to manage cybersecurity risk.

Pascoe said the development team is encouraging anyone with recommendations about the updated CSF to respond with comments by the Nov. 4 deadline.

"This is an opportunity for users to weigh in on the draft of CSF 2.0," she said. "Now is the time to get involved if you're not already."

More information: Dreaft: csrc.nist.gov/pubs/cswp/29/the … ity-framework-20/ipd

Provided by National Institute of Standards and Technology

Citation: NIST drafts major update to its widely used cybersecurity framework (2023, August 8) retrieved 27 April 2024 from https://techxplore.com/news/2023-08-nist-major-widely-cybersecurity-framework.html