

NIST CYBERSECURITY FRAMEWORK 2.0

Update Process for Cybersecurity Framework

Why NIST is updating the Cybersecurity Framework



The NIST Cybersecurity Framework (CSF) is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risks. It is widely used by public and private organizations of all sectors and sizes around the world. As the CSF is a living document, it will be refined, improved, and evolved to keep pace with increasing cybersecurity risks, technology, threat, and policy trends, integrate lessons learned, and establish best practice as common practice. NIST intends to use a public-private dialogue to guide the effort to update the CSF.

How to Engage in the Update Process

Stakeholder engagement will guide the update. Specific ways to engage include:

Visit our website. Visit the CSF [website](#) for updates, upcoming events, resources, and other opportunities to weigh in. NIST has set up a new [CSF 2.0 update page](#) to increase awareness of the update process.

Join us at an upcoming workshop. NIST intends to hold virtual and in-person workshops over the next year. As with prior workshops, attendees will roll up their sleeves to identify specific updates to the CSF. Workshops will be announced on the [CSF events](#) page.

Submit comments on the CSF. Along the path to update the CSF, NIST intends to post at least one draft of the Framework for input. Please submit input on what we got right, and most importantly, what we can improve in the draft. Submit a Success Story or resources. NIST welcomes submissions for CSF [Resources](#), [Success Stories](#), and [Perspectives](#) pages.

Contribute to the National Online Informative Reference Program (OLIR). NIST welcomes contributions to [OLIR](#) to facilitate informative references (or mapping) between the NIST CSF and other guidance resources.

Follow and engage in our international efforts.

The CSF has been translated and adapted throughout the world, and international stakeholder participation will be critical to the update process. Check out the various international adaptations and translations of the CSF and other NIST cybersecurity and privacy resources, as well as updates on our international engagement and how to get involved at the [International Cybersecurity and Privacy](#) site.

Meet us at a cybersecurity conference. NIST staff participate in conferences around the world to increase awareness of the CSF and the update process, as well as learn how organizations are using it. You can see where we will be at on the [CSF events](#) page.

Participate in a NIST forum or community of interest. NIST will be leveraging several existing forums on the CSF update. Forums can be found on our [cybersecurity and privacy stakeholder engagement](#) page.

Email Updates. To receive updates on the CSF, sign up for email alerts via the [Email Subscription](#) page.

Contact us. You can always contact us at cyberframework@nist.gov.