WINSTON & STRAWN LLP

BLOG

NIST Updates Cybersecurity Framework

MAY 7, 2018

The National Institute of Standards and Technology (NIST) has updated their original framework after over two years of development.

The goal of the framework is to provide a flexible, performance-based, and cost effective approach to help operators of critical infrastructure identify, assess, and manage cyber risks. While the framework recognizes that organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—the framework provides the tools, guidelines, and best practices needed to build a cybersecurity program.

The recently released version contains new sections on self-assessment to assist organizations in assessing their own cybersecurity risk, Cyber Supply Chain Risk Management to help prevent attacks in the supply chain sector, and a vulnerability disclosure lifecycle to educate users on events that can cause an increase in vulnerability and how that vulnerability can be exploited.

TIP: Organizations can use the NIST Framework for Improving Critical Infrastructure Cybersecurity 1.1 as a resource to help implement an effective cybersecurity program to manage cyber risk.

1 Min Read

Related Locations

Houston

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.