wiley

NEWSLETTER

The Private Sector Should Watch NIST's Broad Work on Privacy and Cybersecurity Guidance

September 2022

Privacy In Focus®

NIST continues to work on several cybersecurity and privacy workstreams of interest to the private sector. While NIST has traditionally supported federal agencies' IT security, over the past several years it has taken on (and been delegated) several workstreams under Executive Orders and legislation to address multiple aspects of privacy and security, including key areas of technological innovation. Examples of open workstreams that may impact the private sector include:

- Mitigating AI/ML Bias in Context: Establishing Practices for Testing, Evaluation, Verification, and Validation of AI Systems, comments were due September 16, 2022. NIST has several efforts underway to examine aspects of emerging technology, including artificial intelligence and machine learning. Additionally, NIST is developing an AI Risk Management Framework (RMF), and comments on the latest AI RMF draft are due September 29. It is vital that organizations inform the government of the consumer benefits and the innovation in risk management in use of AL and ML across the private sector.
- Implementing a Zero Trust Architecture (Preliminary Draft), comments were due September 9, 2022. This workstream is one of many efforts looking to implement the "zero trust" security concepts, or to help agencies address Executive branch directives about use of zero trust, which may have impacts on federal contractors and other organizations.
- Internet of Things (IoT). NIST IR 8425, the Profile of the IoT Core Baseline for Consumer IoT Products, was released in Draft on

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

June 17, 2022, along with Ideas for the Future of IoT Cybersecurity at NIST: IoT Risk Identification Complexity. IoT security remains a focus of several federal agencies concerned about device security, and NIST and other agencies have been delegated tasks related to consumer communications, security, and privacy that should be of interest to anyone in the IoT space.

- Government contractors should pay close attention to NIST's work on cyber, including its special publications for federal information systems as well as its revisions to the SP 800-171 series, including the Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, on which comments were due September 16, 2022. We expect the government's work on this and related documents to shape expectations for contractors in areas of system boundaries, data governance, and related areas.

Perhaps of more critical and widespread importance, NIST is revising its foundational Framework for Critical Infrastructure Cybersecurity, created in 2014 and revised in 2018 as version 1.1. Public comments on the pending revision suggested a variety of paths, some modest and some transformational. NIST has touted its first workshop on the NIST Cybersecurity Framework update, "Beginning our Journey to the NIST Cybersecurity Framework 2.0", which was held virtually on August 17, 2022 with almost 4,000 attendees from 100 countries. Given the foundational role of the NIST Framework to many private organizations' cyber strategies, major changes should be watched carefully for potential need for compliance program adjustments.

There are myriad other projects underway at NIST and at the National Cybersecurity Center of Excellence (NCCoE) that examine practical applications in privacy, network security, digital identity, and other important parts of organizations' risk management strategies. The staff at NIST and NCCoE are accessible and interested in meaningful private input to inform their workstreams.