NIST CYBERSECURITY & PRIVACY PROGRAM

The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public. Our work ranges from specific information that can be put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

As part of our efforts to cultivate trust in information, systems, and technologies and to help organizations measure and manage risk, we carry out cybersecurity assignments defined by federal statutes, executive orders, and policies, including developing cybersecurity standards and guidelines for federal agencies. Our cybersecurity activities are driven by the needs of U.S. industry, government agencies, and the broader public, and they are undertaken only if our expertise is appropriate for NIST, which is a non-regulatory agency, and can make a difference. We manage very few operational programs, recognizing that other agencies and organizations focus on those aspects of cybersecurity, often using NIST-developed resources to inform their work.

We work closely with organizations in the public and private sectors to ensure that our information can be readily leveraged to address specific issues that they face. We listen, communicate, coordinate, and cooperate with industry and other agencies to prioritize and deliver the most effective information and services. When NIST produces documents and tools for federal agencies, we take their special needs into account while recognizing that many of these resources will be applied in the private sector and by state and local government agencies. These activities take place primarily in the NIST Information Technology Laboratory (ITL) but also involve other parts of the agency.

Our priorities include cryptography, emerging technologies, enhanced risk management, identity and access management, cybersecurity measurements, privacy, trustworthy networks, trustworthy platforms, and education, training, and workforce development. Some of our primary areas of focus are highlighted below. NIST places special emphasis on focused areas to reflect evolving private and public sector needs and the cybersecurity landscape – such as cybersecurity in supply chains and ransomware. Find out more at NIST's Cybersecurity Program.

CRYPTOGRAPHY

Mobile computing, e-commerce, and the proliferation of connected devices bring unprecedented benefits to our lives. But to protect individuals, businesses, and the government from the risks these technological advances bring, we need strong cryptography. NIST provides trusted tools and resources to increase the sound use of cryptography.

- We work with stakeholders around the world to develop strong, trusted cryptographic standards and guidelines. This open process brings together industry, government, and academia to develop workable approaches to cryptographic protection that ensure practical security.
- NIST has cryptographic standards for a variety of IT needs. Since publishing the first Data Encryption Standard for federal systems and financial transactions in the 1970s, our work in cryptography has continually evolved to meet the needs of the changing IT landscape. Today, NIST cryptography is used everywhere, from tablets and cellphones to ATMs and top secret federal data.

- NIST helps to design and test cryptographic algorithms used to create locks and keys. We also assist in their use and help guide how those locks are installed and how effectively they suit the intended purpose. NIST's validation of strong algorithms and implementations builds confidence in cryptography, increasing its use to protect the privacy and well-being of individuals and businesses in the digital age.
- NIST looks to the future to make sure we have the right cryptographic mechanisms ready to protect our identity, data, economy, and way of life as new technologies are brought from research into operation. For example, NIST has selected the new kinds of cryptography to protect our data when quantum computing becomes a reality. At the other end of the spectrum, we are advancing so-called lightweight cryptography to balance security needs for circuits smaller than were dreamed of just a few years ago.

ENHANCED RISK MANAGEMENT

More than ever, organizations must balance a rapidly evolving cybersecurity threat landscape against the need to fulfill business requirements on an enterprise level. To help them measure and manage their cybersecurity risk in this larger context, NIST has convened stakeholders to develop:

- **Integrating Cybersecurity and Enterprise Risk Management (ERM)** promotes greater understanding of the relationship between cybersecurity risk management and ERM, and the benefits of integrating those approaches. The increasing frequency, creativity, and variety of cybersecurity attacks means that all enterprises should ensure cybersecurity risk receives the appropriate attention along with other risk disciplines – legal, financial, etc. – within their ERM programs. This document helps cybersecurity risk management practitioners at all levels of the enterprise, in private and public sectors, to better understand and practice cybersecurity risk management within the context of ERM. NIST risk management disciplines are being integrated under the umbrella of ERM, and additional guidance is being developed to support this integration.

- The **NIST Cybersecurity Framework (CSF)** helps organizations to understand their cybersecurity risks (threats, vulnerabilities and impacts) and how to reduce those risks with customized measures. Initially intended for U.S. private-sector owners and operators of critical infrastructure, the voluntary Framework's user base has grown dramatically across the nation and globe. The Framework integrates industry standards and best practices. It provides a common language that allows staff at all levels within an organization – and at all points in a supply chain – to develop a shared understanding of their cybersecurity risks. NIST worked with private-sector and government experts to create the Framework. Congress ratified it as a NIST responsibility in the Cybersecurity Enhancement Act of 2014 and a 2017 Executive Order directed federal agencies to use the Framework. The CSF's five functions are used by the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and many others as the organizing approach in reviewing how organizations assess and manage cybersecurity risks.

- The **Risk Management Framework (RMF)** provides a flexible and tailorable seven-step process that integrates cybersecurity and privacy, along with supply chain risk management activities, into the system development life cycle. The NIST RMF links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA), including control selection, implementation, assessment, and continuous monitoring. NIST updated the RMF to support privacy risk management and to incorporate key Cybersecurity Framework and systems engineering concepts. Originally targeted at federal agencies, today the RMF is also used widely by state and local agencies and private sector organizations.

- The **Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management** was modeled after the NIST Cybersecurity Framework to enable organizations to use them together to manage cybersecurity and privacy risks collectively. This tool helps organizations to understand how their data processing activities may create privacy risks for individuals and provides the building blocks for the policies and technical capabilities necessary to manage these risks and build trust in their products and services while supporting compliance obligations. The framework provides a common language that allows staff at all levels within an organization – and throughout the data processing ecosystem – to develop a shared understanding of their privacy risks. NIST developed the voluntary framework in an open and public process with private-sector and public-sector experts.

Cybersecurity Supply Chain Risk Management (C-SCRM) helps organizations to manage the increasing risk of supply chain compromise related to cybersecurity, whether intentional or unintentional. These aspects of the supply chain include information technology (IT), operational technology (OT), Communications, Internet of Things (IoT), and Industrial IoT. NIST collaborates with public and private sector stakeholders to research and develop C-SCRM tools and metrics, producing case studies and widely used guidelines on mitigation strategies. NIST also convenes stakeholders to assist organizations in managing these risks.

PRACTICAL SOLUTIONS

NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where companies, government agencies, and academic institutions work together to address businesses' most pressing, practical cybersecurity issues.

- This public-private partnership has provided cybersecurity guidelines for a wide variety of industries, including healthcare, financial services, energy, public safety, and transportation.
- Through consortia – including Fortune 50 market leaders and smaller companies specializing in security – the NCCoE applies standards and best practices to develop and document modular, easily adaptable example cybersecurity solutions using commercially available technology.
- The NCCoE addresses identity and access management (including multifactor authentication), data security integrity, mobile device security, and many other issues. Its work helps to build more trustworthy networks and platforms in areas such as telehealth, Internet of Things, cloud services, 5G communications, and Zero Trust architectures.

INTERNET OF THINGS (IoT)

NIST supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices, often referred to as the Internet of Things (IoT).

- NIST's *Considerations for Managing IoT Cybersecurity and Privacy Risks* report helps IoT users protect themselves, their data, and their networks from potential compromise.
- *IoT Device Cybersecurity Core Baseline* defines capabilities generally needed to support common cybersecurity controls.
- Recommended activities help manufacturers address customer needs for IoT cybersecurity in their product development processes.
- The *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* provides guidance for manufacturers.
- IoT devices are considered in the NIST guidance, *Security and Privacy Controls for Information Systems and Organizations*, which is heavily relied upon by public- and private-sector organizations.

Legislation signed into law in December 2020 formally assigned NIST with producing specific IoT guidance and some additional responsibilities.

INDUSTRIAL CONTROL SYSTEMS (ICS)

Widely available software applications and internet-enabled devices have been integrated into most ICS, delivering benefits but also increasing system vulnerability. Sophisticated malware that specifically targets weaknesses in ICS is on the rise, posing threats to U.S. economic and national security. Despite the threats of attacks, utilities and other users of these systems can be hesitant to adopt common security technologies out of concern about impacts on system performance. These systems are used in industries such as utilities and manufacturing to automate or remotely control product production, handling, or distribution. By providing guidance on how to tailor traditional IT security controls to accommodate unique ICS performance, reliability, and safety requirements, NIST helps industry reduce the vulnerability of computer-controlled systems to malicious attacks, equipment failures, and other threats. For example:

- Our popular Guide to Industrial Control Systems (ICS) Security helps industry understand and implement cybersecurity approaches to protect them from these threats. The document offers guidance for how ICS users can apply the approaches to cybersecurity described in the widely used *Security and Privacy Controls for Federal Information Systems and Organizations*. With this information, utilities, chemical companies, food manufacturers, automakers, and other ICS users can adapt and refine security controls to address their specialized needs.
- NIST is developing practical example solutions to help manufacturers protect industrial control systems from data integrity attacks and address other cybersecurity challenges.
- We are helping energy companies to improve the overall security of information exchanges between

and among distributed energy resource systems and electric power distribution facilities.

- NIST's *Cybersecurity Framework Manufacturing Profile* can be used as a roadmap for reducing cybersecurity risk for manufacturers in a way that aligns with manufacturing sector goals and industry best practices.

WORKFORCE EDUCATION & TRAINING

The National Initiative for Cybersecurity Education (NICE), led by NIST, is a partnership among government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Its mission is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.

- The NICE Cybersecurity Workforce Framework is a fundamental reference for describing and sharing information about cybersecurity work. It establishes a much-needed taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed.
- The NICE Framework increasingly is relied upon across all sectors and is helping organizations as they address an urgent shortage of workers to fill cybersecurity jobs.
- NICE also helps visualize the need for and supply of cybersecurity workers across the country via a Cybersecurity Jobs Heat Map. The tool provides data to help employers, job seekers, policy makers, training providers, and guidance counselors meet today's increasing demand.

NIST CYBERSECURITY FUNDAMENTALS

- ✓ **OPEN AND TRANSPARENT: NIST's processes bring together stakeholders in an open forum.**
- ✓ **COLLABORATIVE: NIST provides a space for government agencies, businesses, and academic institutions to collaborate.**
- ✓ **PRACTICAL: NIST helps develop practical example solutions to address real-world challenges.**
- ✓ **FORWARD-THINKING: NIST looks to the future and anticipates challenges that lie ahead.**

Recent Milestones Driven by Federal Statutes, Executive Orders, and Policies

2014 — **Cybersecurity Framework released; Cybersecurity Enhancement Act assigns NIST workforce, other responsibilities**

2016 — **NIST launches public key Post-Quantum Cryptography Standardization initiative**

2018 — **Law designates NIST to Federal Acquisition Security Council, produce supply chain guidance**

2019 — **NIST launches Small Business Cybersecurity Corner website following 2018 statute**

2020 — **NIST produces IoT guidance per IoT Cybersecurity Improvement Act; NIST issues Security and Privacy Controls, Rev 5; NIST updates NICE strategic plan**

2021 — **NIST launches effort to enhance software supply chain security in response to Executive Order and technology supply chain partnership**