NIST CYBERSECURITY & PRIVACY PROGRAM

THE VITALS

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. We carry out cybersecurity assignments defined by federal statutes, executive orders, and policies, including developing cybersecurity standards and guidelines for federal agencies. 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. Some of our primary areas of focus are highlighted below. Find out more at NIST's Cybersecurity Program.

CRYPTOGRAPHY

NIST provides trusted tools and resources to increase the sound use of cryptography.

- **Workable approaches** to cryptographic protection to ensure practical security.
- **Validation of strong algorithms** and implementations to build confidence.
- **An eye to the future** to ensure the right cryptography for emerging technologies, including protecting data when quantum computing becomes a reality.
- **Continually evolving** standards to meet the needs of the changing IT landscape.

ENHANCED RISK MANAGEMENT

NIST develops frameworks to help measure and manage cybersecurity and privacy risks in the larger context of an enterprise.

- **The Cybersecurity Framework** (CSF) to help organizations understand and address risks with a flexible approach that offers a common language.
- **The Risk Management Framework** (RMF) to integrate security and risk management activities into the system development life cycle.
- **The Privacy Framework** to identify and manage privacy risk and to build innovative products and services while protecting privacy.
- **Cyber Supply Chain Risk Management** (C-SCRM) tools and metrics, case studies, and guidelines on mitigation strategies.

PRACTICAL SOLUTIONS

NIST's National Cybersecurity Center of Excellence (NCCoE) brings together stakeholders to develop practical cybersecurity solutions for specific industries and cross-sector challenges.

- **Guidelines for a wide variety of industries**, including healthcare, financial services, energy, public safety, and transportation.
- **Application of standards and best practices** to develop and document modular, easily adaptable example cybersecurity solutions using commercially available technology.
- **Development of trustworthy networks** and platforms by addressing identity and access management, data security integrity, mobile device security, and more.

INTERNET OF THINGS (IoT)

NIST supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices, or IoT.

- **A report on considerations for managing IoT** cybersecurity and privacy risks.
- **A core baseline of IoT device cybersecurity** capabilities for manufacturers.
- **Recommended activities to help manufacturers** address customer needs for IoT cybersecurity in the product development processes.
- **A profile using the IoT core baseline and non-technical baseline** for the federal government.

INDUSTRIAL CONTROL SYSTEMS (ICS)

NIST provides guidance on tailoring traditional IT security controls to accommodate unique ICS performance, reliability, and safety requirements.

- **The Guide to Industrial Control Systems (ICS) Security** to help in applying the cybersecurity approaches found in Security and Privacy Controls for Federal Information Systems and Organizations.
- **The Cybersecurity Framework Manufacturing Profile** to help reduce risk in alignment with manufacturing sector goals and best practices.
- **Practical example solutions** for manufacturers.
- **An approach for energy companies** to improve the overall security of information exchanges between and among distributed energy resource systems and electric power distribution facilities.

WORKFORCE EDUCATION & TRAINING

The National Initiative for Cybersecurity Education (NICE), a partnership between government, academia, and the private sector led by NIST, promotes a robust network and ecosystem of cybersecurity education, training, and workforce development.

- **The Workforce Framework for Cybersecurity** (NICE Framework) categorizes and describes cybersecurity roles and functions, establishing a much-needed taxonomy and common lexicon.
- **The NICE Framework increasingly is relied upon** across all sectors, helping to address an urgent shortage of workers for cybersecurity jobs.
- **The Cybersecurity Jobs Heat Map** 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