Select Cyber Security Initiatives

National Institute of Standards and Technology

December 2022

Matthew Scholl, Chief, Computer Security Division

Presenter: Peter Mell, Senior Computer Scientist

Strategic Priorities in Cyber Security and Privacy (CSP)
Source: 2019 Federal Cybersecurity R&D Strategic Plan

1. Deter: The ability to efficiently discourage malicious cyber activities by increasing costs, diminishing the spoils of, and increasing risks and uncertainty for potential adversaries.
2. Protect: The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities, and to ensure confidentiality, integrity, availability, and accountability
3. Detect: The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and that systems should be assumed to be vulnerable to malicious cyber activities
4. Respond: The ability to dynamically react to malicious cyber activities by adapting to disruption, countering the malicious activities, recovering from damage, maintaining operations while completing restoration, and adjusting to be able to thwart similar future activities
5. Artificial Intelligence: Capabilities that enable computers and other automated systems to perform tasks that have historically required human cognition and what we typically consider human decision-making abilities
6. Quantum Information Science: Capabilities that harness quantum mechanics and quantum material properties to achieve computation, information processing, communications, and sensing in ways that cannot be achieved with classical physics principles
7. Trustworthy Distributed Digital Infrastructure: Technologies and solutions that facilitate secure telecommunications and information communications infrastructure that enables next generation wireless communication, edge and fog computing, and supports seamless integration with cyber-physical systems and IoT
8. Privacy: Solutions that minimize privacy risks or prevent privacy violations arising from the collection and use of peoples' private information
9. Secure Hardware and Software: Technologies and solutions that provide and improve security properties of hardware and software components in computing and communication systems
10. Education and Workforce development: Programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce

Deter

CRYPTOGRAPHY

- NIST develops, standardizes and tests strong cryptography and is a known trusted source – resulting in the use of NIST cryptography by default in globally available commercial products name or type of R&D
  - Other participating agencies – NSA, Other National Cryptographic Authorities, Academia

Trustworthy Hardware

- NIST develops guidance, standards, tools and reference for the protection of hardware, the creation of secure hardware and the use of hardware for security.
  - Other participating agencies – DoD, NSF, Industry

Trustworthy Software

- Under direction from EO 14028; NIST creates guidance, standards, tools and reference for securing the software supply chain and the SDLC.
  - Other participating agencies – DHS, GSA, Industry

Protect

Risk Management

- NIST produces a coordinated and cohesive portfolio of complementary resources that can be used individually or together to help public and private organizations to better manage cybersecurity and privacy risk at all levels of the enterprise.
- Other participating agencies, DoD, IC, DHS, Fed CIO, OMB
- Project Examples: CSF, RMF, SCRM, NVD, Automation Schema

Protect

Identity and Access Management

- NIST conducts a comprehensive program that improves stakeholders' ability to properly identify people, devices, and processes, and manage their access to systems and information resources.

Other participating agencies, DHS, GSA, FICAM, Fed CIO, OMB

- Project Examples: PIV, SP 800-63, NGAC, MdL,

Detect

- The National Vulnerability Database (NVD)
- The NVD is the U.S.G repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance.
- The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
- Other participating agencies DHS, FIRST, GFIRST, MITRE

- IT Forensics
  - NSRL – Computer Forensics Tool Verification (CFTT), Software Assurance Reference Dataset (SARD), Computer Forensics Reference Data Sets (CFReDS), Digital Evidence Preservation
  - **Other participating agencies DHS, DOJ, FBI**

Respond

Emerging Technologies R&D

- *Identification, research, development, and adoption of near- term and on-the-horizon emerging technologies with the goal of enhancing, improving, strengthening and advancing cybersecurity and privacy applications.*
- Project Examples: Blockchain, Edge Security, PSN, 5G and Beyond, VR/AR, Digital Twins, Quantum Sciences,

Artificial Intelligence

Trustworthy AI:

- As a non-regulatory research organization, NIST cultivates trust in AI-related research by using rigorous methods and decades-long experience to develop tools, technical guidance, and best practice guides, that accurately measure and understand the capabilities and limitations of AI technologies and the underlying data that catalyzes them. \
  - Project Examples: AI Risk Management Framework, AI Safety and Security, AI Bias, AI Explainability, AI Test Beds

Quantum Information Science

Post-Quantum Cryptography (PQC)

- NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the Post-Quantum Cryptography Standardization page.
  - Nov 29-Dec 1 Next PQC Conference – Standards Creation
  - First Round Selections Finished

- **QEDC** The Quantum Economic Development Consortium (QEDC) aims to expand U.S. leadership in global quantum research and development and the emerging quantum industry in computing, communications and sensing. Quantum technologies take advantage of the unusual rules that govern the behavior of the fundamental building blocks of matter, including electrons, protons, neutrons and photons.

- QIS Work Overall - https://www.nist.gov/quantum-information-science

- JQI/QUiCS UMD

Trustworthy Distributed Digital Infrastructure

Trustworthy Networks

- NIST works with industry partners to advance the research, standardization and adoption of technologies necessary to increase the security, privacy and resilience of networked systems.

- Project Examples: Resolving systemic vulnerabilities in critical network infrastructures and technologies, SDN/VFN, BGP, DNSSec, IPv6, IOT, ZTA.

Privacy

Privacy Program

- NIST carries out a robust program that provides relied-upon privacy resources and solutions that cultivate trust in information technologies and systems, is able to anticipate stakeholder challenges, and is agile enough to meet urgent societal or governmental needs.
  - OMB, FTC, Fed Privacy Officers
- Project Examples: Privacy Framework, SP 800-53r5, Privacy Enhancing Technologies and Privacy Enabled Tracing

- PEC – Private Set Intersections, Anonymous Certificates, Multi-Party Computations, HPE.

Education and Workforce Development

National Initiative for Cybersecurity Education (NICE)

- Build a nation equipped with a workforce and general public capable of managing cybersecurity and privacy risks because NIST information, products, and services are effectively used as the basis for awareness, training, and education

- OPM-DHS-Federal CHICOS-DoEd
- Project Examples; NICE Strategic Plan; NICE Workforce Framework; Annual NICE Conference, Privacy Workforce

NIST: Planned future programs or components supporting Administration priorities

- Administration Priority EO 14028 Improving the Nation's Cybersecurity
- Administration Priority CHIPS for America
- Administration Priority OMB M 22 09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- Administration Priority NSM 10 Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems