NIST Cybersecurity and Privacy Update
Information Security Privacy Advisory Board

Chuck Romine
Director, Information Technology Laboratory

National Institute of Standards and Technology
U.S. Department of Commerce

October 14, 2020

Happy World
Standards Day
14 OCTOBER 2020

Congratulations

NIST Cybersecurity Expert Donna Dodson Receives 2020 Samuel J. Heyman Service to America Medal in the Safety, Security and International Affairs category.

Privacy Framework

Growing a Workforce for Managing Privacy Risk Workshop was hosted by International Association of Privacy Professionals on Sept 22-24, 2020.

GDPR Crosswalk by Enterprivacy Consulting Group
ISO/IEC 27701 Crosswalk by Microsoft

Noteworthy Releases

SP 800-53 Rev 5
Security and Privacy Controls for Information Systems and Organizations

Cybersecurity Telework Resource Page

Began validating cryptographic modules to FIPS 140-3, Security Requirements for Cryptographic Modules.

Draft Workforce Framework for Cybersecurity (NICE Framework)

SP 800-207
Zero Trust Architectures

SP 800-211
Cybersecurity Program Annual Report

Responsible Use Of Positioning, Navigation & Timing Services

EXECUTIVE ORDERS

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

INFRASTRUCTURE & TECHNOLOGY | Issued on: February 12, 2020

https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/

The Executive Order directs the Department of Commerce and other agencies to work with the private sector to identify and promote responsible methods of using PNT services that appropriately manage risks.

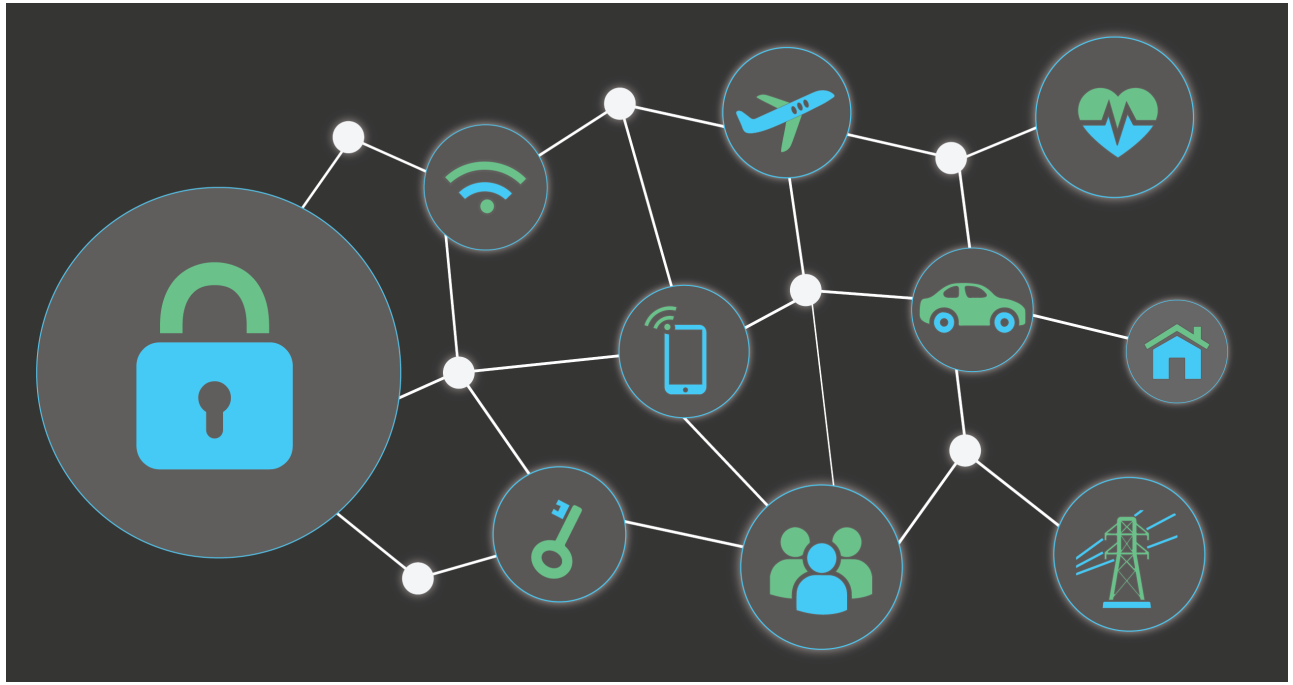
Cybersecurity Profile for the Responsible Use of PNT

- Draft annotated outline issued on August 31, 2020.
- Workshop on Sept 15-16, 2020.
- Draft Profile for public comment expected mid October 2020.

https://www.nist.gov/itl/pnt

7

Cybersecurity for Internet of Things



1. NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

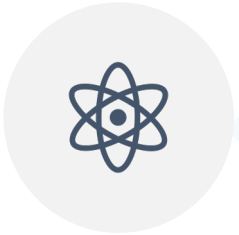
2. NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline

Federal Profile of NISTIR 8259A

3. Catalog of IoT Device Cybersecurity Capabilities published on GitHub

4. Workshop on Cybersecurity Risks in Consumer Home IoT Products on October 22, 2020.

Industries of the Future



QUANTUM INFORMATION SCIENCES

5G AND ADVANCED COMMUNICATIONS

ARTIFICIAL INTELLIGENCE

ADVANCED MANUFACTURING

BIOTECHNOLOGY

Updates on NIST Work in Encryption

Credit: E. Edwards/JQI

Post Quantum Cryptography
Round Three selections completed.

Lightweight Encryption
The Fourth Lightweight Cryptography Workshop (virtual) on October 19-21, 2020.

Trustworthy AI

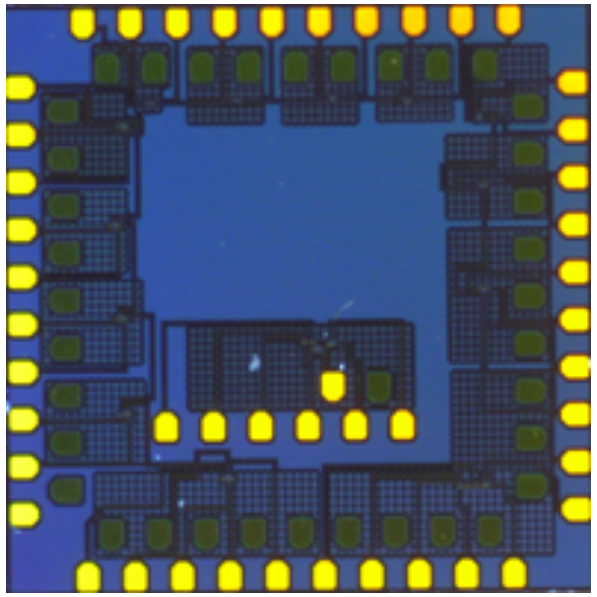
NIST develops vocabulary and measurements needed for technical requirements of trustworthy AI.

Bias in AI: workshop on August 18, 2020.

NISTIR 8312 Four Principles of Explainable AI, public comment Aug 17-Oct 15, 2020.

Secure AI: NISTIR 8269 Terminology and Taxonomy; Final draft expected in Fall.

Novel Computational Paradigms for AI

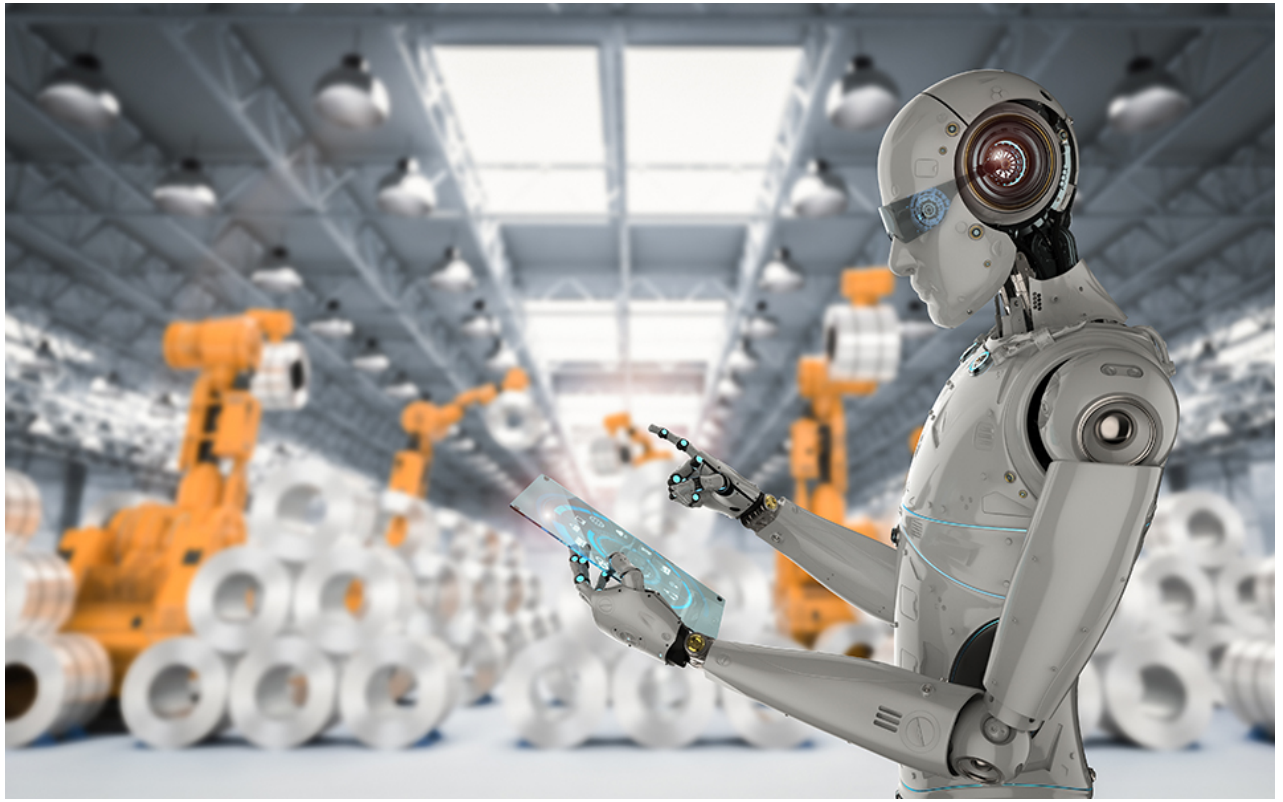


- Establishing metrics and benchmarks for AI hardware.
- Foundational analysis of the computational capacity of a physical system.
- Analysis and development of algorithms for spike-based computation.

Schneider, M.L., Donnelly, C.A., Haygood, I.W. et al. Synaptic weighting in single flux quantum neuromorphic computing. Sci Rep 10, 934 (2020)

12

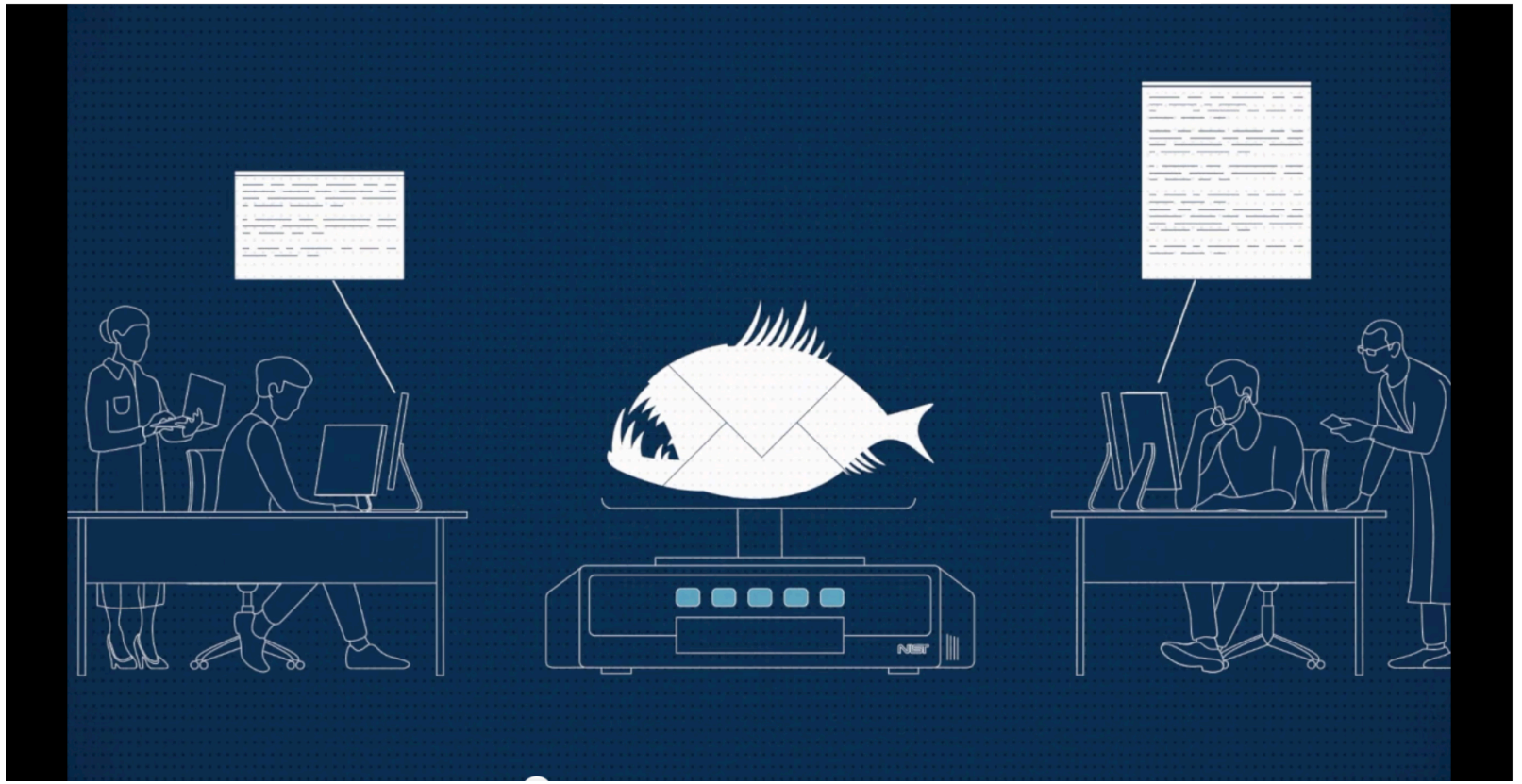
Upcoming Symposium: U.S. Strategy for Resilient Manufacturing Ecosystems Through AI



Credit: Phonlamai Photo/shutterstock.com

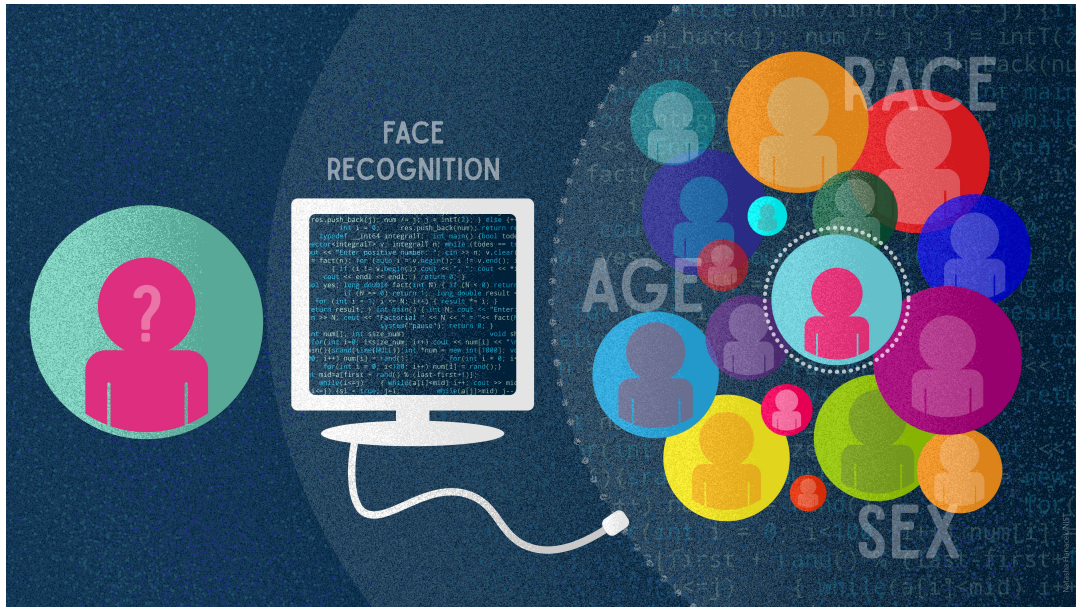
Hosted by the National Science and Technology Council (NSTC)
Subcommittee on Advanced Manufacturing and
Subcommittee on Machine Learning and Artificial Intelligence

The Phish Scale



NIST developed a new method called the Phish Scale that could help organizations better train their employees to avoid a particularly dangerous form of cyberattack known as phishing.

Effect of Masks on Face Recognition Accuracy



NISTIR 8311 - Face recognition accuracy with face masks using pre-COVID-19 algorithms

The next report will document accuracy values for more recent algorithms, some developed with capabilities for recognition of masked faces.

National Institute of Standards and Technology
U.S. Department of Commerce

MARYLAND
ITL ROX
Treasure the Chesapeake