NIST Cybersecurity Activities
August 7, 2019
Cultivating Trust in IT and Metrology
ITL’s work

- Fundamental Research
- Applied Research
- Standards + Best Practice Guides
- Adoption

Image Credit: wsj.com
NIST Priority Areas

Quantum Science  Engineering Biology

Artificial Intelligence  Internet of Things
President’s FY 2020 Budget Request. [https://www.whitehouse.gov/omb/budget/](https://www.whitehouse.gov/omb/budget/)
Pending Legislations

**H.R. 1668**

*116th Congress 1st Session*

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

**S. 734**

*116th Congress 1st Session*

To leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes.

**IoT Cybersecurity Improvement Act of 2019**

*Rep. Robin Kelly [D-IL-2]*

*House - Oversight and Reform; Science, Space, and Technology*

*Sen. Mark Warner [D-VA]*

*Senate - Homeland Security and Governmental Affairs*
Testimonies

1. **Small Business Cybersecurity**
   - March 13, 2019
   - Senate Committee on Small Business and Entrepreneurship

2. **IoT Vulnerabilities**
   - April 30, 2019
   - Senate Committee on Commerce, Science, and Transportation

3. **Facial Recognition Technology**
   - June 4, 2019
   - House Committee on Oversight and Gov. Reform
   - July 10, 2019
   - House Committee on Homeland Security

4. **Facial Recognition Technology**
   - June 4, 2019
   - House Committee on Oversight and Gov. Reform

5. **Election Security**
   - June 25, 2019
   - Subcommittee on Investigations & Oversight
   - House Committee on Science, Space and Technology
1. Develop and Issue a Privacy Framework by Fall 2019.

2. Develop and Issue FIPS 140-3, Security Requirements for Cryptographic Modules.

3. Advance the Cybersecurity Framework and other cybersecurity, privacy, and supply chain risk management practices through a series of workshops.

The existing foundations of both fundamental cryptography and cryptographic standards that established trust in our global information technology infrastructure were largely developed in the United States, primarily by NIST in partnership with the private sector.
Envisioned to be a voluntary enterprise risk management tool to help organizations manage individuals’ privacy risk

April 30, 2019: Discussion draft
June 26, 2019: Supplemental materials to the discussion draft
July 8-9, 2019: Workshop #3 Boise, ID
August 2019: Preliminary draft
December 2019: Version 1.0

https://www.nist.gov/privacy-framework
Cybersecurity for Internet of Things

• NISTIR 8228 Consideration for a core IoT cybersecurity capabilities baseline. Published in June, 2019

• Workshop on core IoT cybersecurity baseline. August 13, 2019
Building **trust** in technology by driving adoption of **standards-based cybersecurity solutions** to address business needs

<table>
<thead>
<tr>
<th>Practice guides</th>
<th>SP 1800 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>New programs</td>
<td></td>
</tr>
</tbody>
</table>

40+ NCEP
Within 180 days of the date of this order, NIST is tasked with developing a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies.
Plan for Federal engagement in the development of AI standards

- Bolster AI knowledge and coordination among Fed agencies.
- Support and expand public-private partnerships.
- Plan, support, and conduct research and evaluation.
- Strategically engage with international parties.
Joint NSTC + NITRD Workshop on AI & Cybersecurity

Office of Science and Technology Policy

NSTC

MLAI Subcommittee
Chaired by NIST, OSTP, DoE

AI Select Committee
Chaired by OSTP, NSF, DARPA

Joint NITRD and NSTC workshop on AI and Cybersecurity
June 3-5
University Maryland College Park.
Save the Date

2022
Celebrating 50 years of Cybersecurity research at NIST