INFORMATION TECHNOLOGY LABORATORY

NIST Update

Information Security and Privacy Advisory Board

June 28, 2017

P(A|B) = P(B|A) P(A) / P(B)
010011000010 010001110001 10
0010111010100001110101010
1101000010 10 11111000001001
$i\hbar\frac{\partial\Psi}{\partial t} = \hat{H}\Psi(x,t)$

Outline

- Administration Actions
  - Executive Order 13800
  - President’s FY 2018 Budget Request
- Congressional Actions
  - H.R. 1224: NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
  - H.R. 2481: Protecting our Ability to Counter Hacking (PATCH) Act of 2017
  - S.770: MAIN STREET Cybersecurity Act of 2017
  - Hearing on WannaCry Ransomware
- ITL’s Purpose and Current Priorities
- Potential Future Priorities
- Question for ISPAB

Administration Actions

- Executive Order 13800
- President’s FY 2018 Budget Request

Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- Cybersecurity of Federal Networks
- Cybersecurity of Critical Infrastructure
- Cybersecurity for the Nation

EO 13800: Cybersecurity of Federal Networks (1 of 2)

- **Risk Management:** Federal agencies shall use the Cybersecurity Framework to manage their cybersecurity risk
- **Lead Agencies:** OMB and DHS
- **NIST's Role**
  - Raise agencies' awareness of the Cybersecurity Framework
  - Update NIST cybersecurity risk management guidelines to integrate Cybersecurity Framework and support agencies' improved enterprise-risk management
  - On May 12, issued draft NIST IR 8170 on federal use of the Cybersecurity Framework one day after the EO was issued

EO 13800: Cybersecurity of Federal Networks (2 of 2)

- **IT Modernization:** Coordinate a report to the President regarding modernization of IT
- **Lead Agency:** Director of the American Technology Council
- **NIST's Role**
  - Provide input on technical feasibility of IT modernization, network consolidation, and shared services.
  - Clarify, reconcile, and reissue standards and guidelines.

EO 13800: Cybersecurity of Critical Infrastructure

- Resilience Against Botnets and Other Automated, Distributed Threats
- Lead an open and transparent process to
  - Identify and promote action by stakeholders to improve resilience of the internet and communications ecosystem
  - Encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks
- Lead Agencies: Commerce (NIST, NTIA) and DHS
- Deliverables
  - Issue preliminary report for public comment (within 240 days)
  - Submit final report to the President (within 365 days)

EO 13800: Cybersecurity for the Nation

- Workforce Development
  - Assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future from elementary through higher education
  - Provide a report to the President within 120 days with findings and recommendations on how to support the growth and sustainment of the nation’s cybersecurity workforce in both the public and private sectors
- Lead Agencies: Commerce (NIST) and DHS
- Deliverable: Report to the President (within 120 days)

President’s FY 2018 Budget Request: Budgeting to Preserve Core NIST

- The President’s FY 2018 Budget Request reflects the Administration’s stated priority to rebuild the military, make critical investments in the nation’s security, and keep the nation on a responsible fiscal path
- Funds will maintain core capabilities in measurement science, so NIST can continue to meet its mission to provide the measurements and standards that accelerate innovation

	FY 2017	FY 2018	% Change
NIST Research	$717M	$607M	−13%
ITL Research	$123M	$114M	−13%
Cybersecurity	$66M	$60M	−9%

Congressional Actions

- H.R. 1224: NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
- H.R. 2481: Protecting our Ability to Counter Hacking (PATCH) Act of 2017
- S.770: MAIN STREET Cybersecurity Act of 2017
- Hearing on WannaCry Ransomware, before Joint Subcommittee of House Committee on Science, Space, and Technology

H.R. 1224: NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017

- Amend the NIST Act to implement a framework, assessment, and audits for improving U.S. cybersecurity
- NIST's Role
  - Provide guidance for agencies to incorporate the Cybersecurity Framework into their information security risk management efforts
  - NIST must chair a federal working group and establish a public-private working group to coordinate the development of metrics and tools to measure the effectiveness of the Cybersecurity Framework
  - NIST must initiate an individual cybersecurity audit of certain agencies to assess the extent to which they meet information security standards

H.R. 2481: Protecting our Ability to Counter Hacking (PATCH) Act of 2017

- Establish a Vulnerability Equities Review Board
- Department of Commerce Role: Serve as permanent board member and coordinate with DHS to establish a process by which DHS shares or releases vulnerability information

S. 770: MAIN STREET Cybersecurity Act of 2017

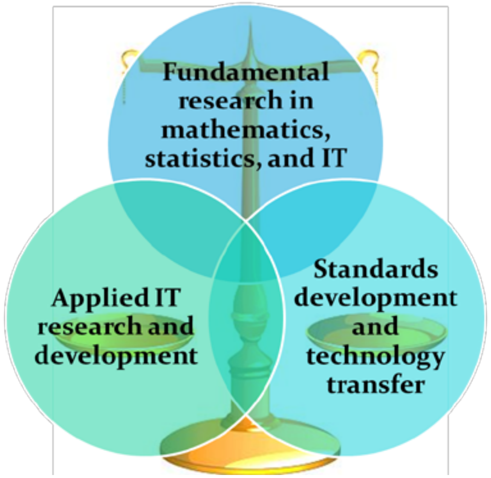
- Require NIST to disseminate resources to help reduce small-business cybersecurity risks
- NIST's Role: Provide and update tools, methodologies, guidelines, and other resources so small businesses can use them on a voluntary basis

Hearing on WannaCry Ransomware

- Title: “Bolstering Government Cybersecurity Lessons from WannaCry” (June 15, 2017)
- Purpose: “to examine the recent WannaCry ransomware attack and the benefits of public-private partnerships for cybersecurity, as well as the President’s recent Executive Order”
- My testimony emphasized these ITL’s cybersecurity-related resources:
  - Cybersecurity Framework
  - Guide for Cybersecurity Event Recovery (800-184)
  - National Software Reference Library
  - National Vulnerability Database

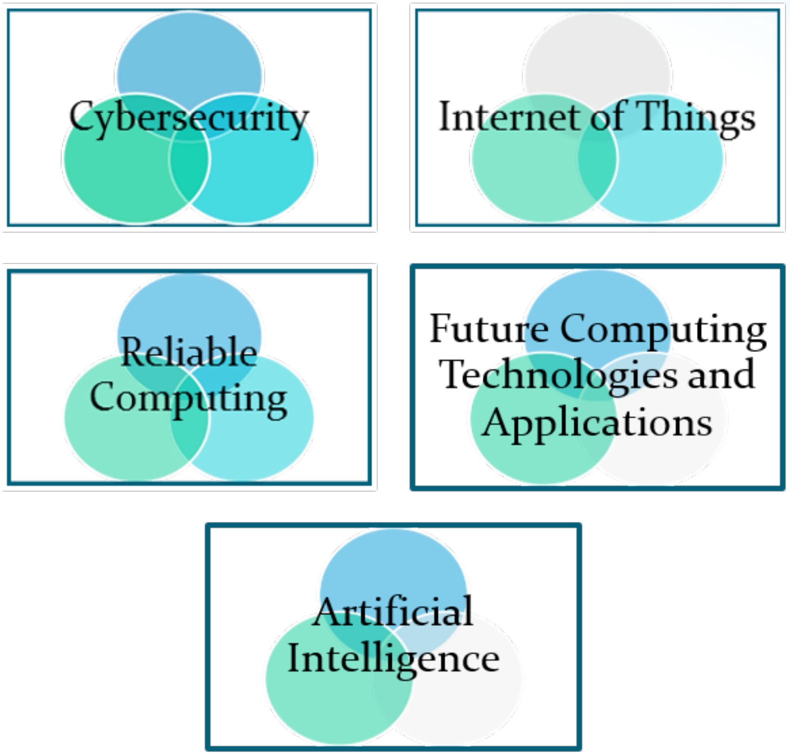
ITL's Purpose and Current Priority Areas

Cultivating Trust in IT and Metrology through Measurements, Standards and Testing


Fundamental research in mathematics, statistics, and IT

Applied IT research and development

Standards development and technology transfer


Cybersecurity

Internet of Things

Reliable Computing

Future Computing Technologies and Applications

Artificial Intelligence

Potential ITL’s Future Priority Areas

- Data Science
  - Open repositories
  - Data analytics
  - Testing and evaluation
- Improving Software Reliability through Software Metrology
- Cultivating Trust in Metrology through Uncertainty Quantification (Applied Mathematics, Statistics)

Question for ISPAB

What are the cybersecurity and privacy implications of ITL’s current and potential future priority areas?

Questions?