INFORMATION
TECHNOLOGY
LABORATORY

NIST Update

Information Security and Privacy Advisory Board

October 25, 2017

P(A|B) = P(B|A) P(A) / P(B)
01001100001001000111000110
00101110101000011110101010
1101000010 10 11111000001001
$i\hbar\frac{\partial\Psi}{\partial t} = \hat{H}\Psi(x,t)$

Outline

- Administration Action
  - Executive Order 13800
- 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
- ITL’s Purpose and Current Priorities
- Potential Future Priorities

Administration Action:

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)

- EO 13800 requires federal agencies to use the Cybersecurity Framework to manage their cybersecurity risks.
- **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

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

NIST's Actions

- May: NIST issued *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* (NISTIR 8170)
- August: NIST issued an initial public draft of SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.
- September: NIST issued a discussion draft of SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*.
- NIST also in the process of updating the Cybersecurity Framework (second draft of version 1.1 expected in late October 2017 for public comment).

EO 13800: Cybersecurity of Critical Infrastructure (1 of 2)

- EO 13800 directs the Secretaries of DoC and DHS to 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:**
  - Preliminary report for public comment within 240 days.
  - Final report to the President within 365 days.

EO 13800: Cybersecurity of Critical Infrastructure (2 of 2)

NIST’s Actions

- July: NIST’s NCCoE hosted a workshop, “*Enhancing Resilience of the Internet and Communications Ecosystem*.”
- September: NIST released NISTIR 8192, which documents the proceedings of the workshop.
- This workshop and proceedings + public input received in response to NTIA-issued Request for Comments + report from NSTAC will inform development of preliminary report to be released in January 2018 for public comment.

EO 13800: Cybersecurity for the Nation (1 of 2)

- EO 13800 states that it is the policy of the United States “to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.”
- The Secretaries of DoC and DHS were directed to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, from elementary through higher education
- **Lead Agencies:** Commerce (NIST) and DHS
- **Deliverable:** Report to the President (within 120 days)

EO 13800: Cybersecurity for the Nation (2 of 2)

NIST's Actions

- Development of the report: *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*.
- July: NIST issued a Request for Information to gather information from the public to inform report's findings and recommendations.
- August: NIST hosted a workshop on cybersecurity workforce development at Illinois Institute of Technology to seek public input to inform report.
- August: Report publicly released.
- Report currently in clearance process in the offices of the Secretaries of Commerce and Homeland Security.

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

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

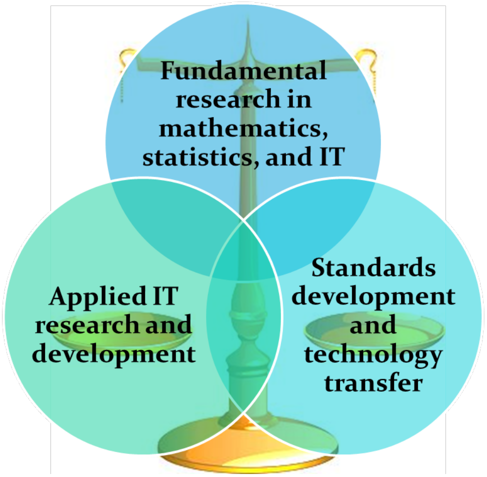
- Establish a Vulnerability Equities Review Board.
- Department of Commerce Role: Serve as permanent board member and coordinate with DHS to establish a process by which DHS shares or releases vulnerability information.

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.

ITL's Purpose and Current Priority Areas

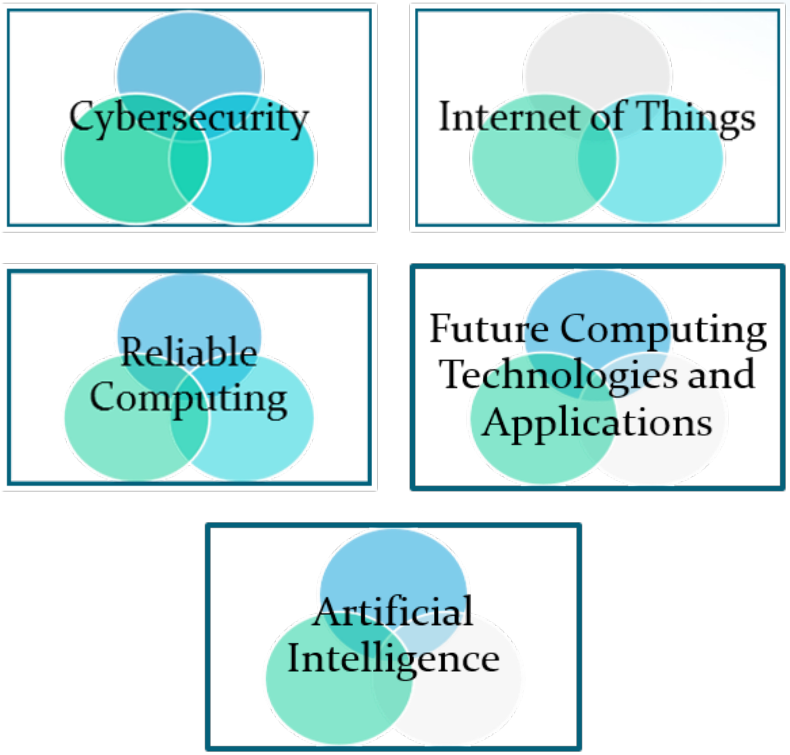
Cultivating Trust in IT and Metrology through Measurements, Standards and Testing



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)

Questions?