NIST Laboratories

NIST’s work enables
- Science
- Technology innovation
- Trade
- Public benefit

NIST works with
- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations
<table>
<thead>
<tr>
<th>Group</th>
<th>Some Major Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Technologies</td>
<td>Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, E-Voting, Quantum Computing,</td>
</tr>
<tr>
<td>Security Management and Assurance</td>
<td>FISMA, Health IT, Smart Grid, Supply Chain, NICE, Crypto Validation Programs, Outreach and Awareness</td>
</tr>
<tr>
<td>Security Components and Mechanisms</td>
<td>Virtualization, Security Automation (S CAP), Trust Roots, Continuous Monitoring, USGv6</td>
</tr>
<tr>
<td>Security Test and Metrics Group</td>
<td>CAVP, CMVP, S-CAP Validation, Attack Graphs, NVD</td>
</tr>
</tbody>
</table>
NIST’s Cybersecurity Role in National Priorities

- **Legislation**
  - Federal Information Security Management Act (FISMA) of 2002
  - Cyber Security Research and Development Act (CSRDA) of 2002
  - Help America Vote Act (HAVA) of 2002
  - Energy Independence and Security Act (EISA) of 2007
  - Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

- **Presidential Directives**
  - HSPD-7
  - HSPD-12

- **Office of Management and Budget (OMB) Policy**
  - OMB Circular A-130 Appendix III

- **Administration Priorities**
  - Comprehensive National Cybersecurity Initiative (CNCI)
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)
NIST’s Cybersecurity work spans ...

- Security Research, Development, and Specifications
- Secure System and Component Configuration
- Test, Validation, and Measurement of Security Properties of Products and Systems
- Cryptographic Technologies
- Security Awareness and Outreach

NIST’s Cybersecurity work results in...

- Federal Information Processing Standards
- NIST Special Publications
- NIST Interagency Reports
- Security Models
- Open Software
- Reference & Prototype Implementations
- Journal and Conference Papers
- ANSI, ISO, ITU-T, IEEE, IETF Standards
- Patents
- Conferences and Workshops
<table>
<thead>
<tr>
<th>NIST IR</th>
<th>Publication ID</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST IR-7848</td>
<td>DRAFT Specification for the Asset Summary Reporting Format 1.0</td>
<td>May</td>
<td></td>
</tr>
<tr>
<td>NIST IR-7511 Rev. 3.01.165</td>
<td>DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements</td>
<td>April</td>
<td></td>
</tr>
<tr>
<td>FIPS</td>
<td>FIPS-186-3 Proposed Change</td>
<td>DRAFT Proposed Change Notice for Digital Signature Standard (DSS)</td>
<td>April</td>
</tr>
<tr>
<td>SP</td>
<td>Description</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>SP 800-130</td>
<td>DRAFT A Framework for Designing Cryptographic Key Management Systems</td>
<td>April</td>
<td></td>
</tr>
<tr>
<td>SP 800-66 Rev.2</td>
<td>An Introductory Resource Guide for Implementing the HIPAA Security Rule</td>
<td>In progress</td>
<td></td>
</tr>
<tr>
<td>SP 800-53 Rev. 4</td>
<td>DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft)</td>
<td>February</td>
<td></td>
</tr>
<tr>
<td>SP 800-61 Rev. 2</td>
<td>DRAFT Computer Security Incident Handling Guide</td>
<td>January</td>
<td></td>
</tr>
<tr>
<td>SP 800-159</td>
<td>Guidelines for Access Control System Evaluation Metrics</td>
<td>In progress</td>
<td></td>
</tr>
<tr>
<td>SP 800-XXX</td>
<td>K-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Attacks</td>
<td>In progress</td>
<td></td>
</tr>
</tbody>
</table>
- NIST IR 7816, 2011 Computer Security Division Annual Report
- FIPS 180-4, Secure Hash Standard (SHS)
Upcoming/Recent Events

FY12 Conferences / Workshops
Computer Security Division

2012

• Technical Aspects of Botnets Workshop, NIST, May 30
• Fifth Annual Safeguarding Health Information, Ronald Reagan Building and International Trade Center, June 6-7
• National Cybersecurity Center of Excellence Workshop, June 26
• ICT Supply Chain Risk Management (SCRM) Workshop, NIST, July 11-12
• Cryptographic Key Management Workshop (Fall 2012-TBD)
Upcoming Events
FY12 Conferences / Workshops
Computer Security Division

2012

• Revised Draft FIPS 201-2 Workshop, July 25
• Federal Computer Security Program Managers’ Forum, August 9
• NICE “Shaping the Future of Cybersecurity Education” Workshop, NIST, October 30 – November 1
Past Events
FY12 Conferences / Workshops
Computer Security Division

2012

- NSTIC Identity Ecosystem Governance Workshop, March 15
- Cybersecurity for Cyber Physical Systems Workshop, April 23-24
National Cybersecurity Center of Excellence (NCCoE)

Mission

To foster an environment that aligns diverse communities to adopt and utilize comprehensive cybersecurity solutions that support immediate, operational needs.