the WHITE HOUSE PRESIDENT BARACK OBAMA

Internet of Things: Examining Opportunities and Challenges

AUGUST 30, 2016 AT 7:15 PM ET BY AFUA BRUCE, DAN CORREA, AND SUHAS SUBRAMANYAM

Summary: The Administration is working with stakeholders to understand and harness the benefits of connected devices while also assessing and addressing potential challenges.

Through the integration of computers, sensors and networking in physical devices, the Internet of Things (IoT) fuses the physical and digital worlds to develop new capabilities and services, which in turn create new jobs, businesses and opportunities. Innovators and entrepreneurs across the country are leading the development and deployment of IoT systems and services, extending the Internet beyond laptops and smartphones to everyday devices of all types—from cars and clothing to homes and factories—while adding the sensors and computing capabilities that make them "smart." More than ever, we will need to work together to promote the advancement of these connected devices while also ensuring they are secure, safeguard our privacy, and remain worthy of our trust.

While IoT devices incorporate many technologies Americans have used for decades such as microprocessors, cameras, and other sensors, the truly ubiquitous nature of these devices present new opportunities and challenges for the nation. Small, ordinary-looking devices placed in homes and businesses can help keep us secure, but they also open important privacy questions; sensors in cars, trucks, airplanes, and ships help identify and prevent failures or accidents before they happen but also open new cybersecurity vulnerabilities; and complex IoT software and operating systems may contain bugs or are not updated regularly, raising questions about safe deployment in critical health, infrastructure, and even everyday uses.

In order to address some of these opportunities and challenges, the National Institute of Standards and Technology (NIST) is hosting a workshop on August 31 to help understand trustworthiness in IoT and Cyber-Physical Systems (CPS). Among the most important characteristic of any connected device is trustworthiness—it must be safe, secure, reliable, resilient, and privacy-enhancing. Trustworthiness is one of nine fundamental 'Aspects,' or dimensions, of IoT and CPS as described in the recently-released Framework developed by NIST's CPS Public Working Group.

In addition, the National Telecommunications and Information Agency (NTIA) is hosting a workshop on September 1 to discuss ways to help foster the growth of IoT. The workshop will build on the comments NTIA received this spring that called for public input on what elements, if any, are necessary for strategic government engagement related to IoT. It will help to inform the Commerce Department's forthcoming issue-spotting, agenda-setting green paper on IoT. The NTIA workshop will feature panel discussions on privacy, security and technology issues related to IoT, as well as a discussion on the potential role of government and whether there should be a national strategy related to IoT.

The workshops this week are one of several examples of the Administration taking bold action to ensure both safety, privacy and innovation as the IoT market continues to grow. As part of the Administration's Cybersecurity National Action Plan released earlier this year, the Department of Homeland Security is collaborating with industry partners to develop a Cybersecurity Assurance Program to test and certify networked IoT devices. The Administration is also working with and recognizing the importance of external security researchers through programs like the Department of Defense's Hack the Pentagon program, the first bug bounty in the history of the federal government. The Networking and Information Technology Research and Development (NITRD) Program has two Federal interagency working groups that examine IoT R&D areas. And through the Smart Cities Initiative, the Administration is investing more than $160 million in Federal research and forging new cross-sector collaborations to help communities use technologies like IoT to tackle key challenges such as traffic congestion, pollution and crime. To take new steps to advance the Smart Cities, the White House Office of Science and Technology Policy has issued a national call to action for new specific and measurable public and private actions to accelerate the development of smart cities.

Your input is critical to fostering the promise of IoT, and we want you to hear from you about this week's workshops. You can watch the NIST workshop online and email your thoughts to nistcps@nist.gov, and also tune into NTIA's workshop and learn more about its multistakholder process on IoT.

Afua Bruce is the Executive Director of the National Science and Technology Council

Dan Correa is a Senior Advisor on Innovation Policy in the White House Office of Science and Technology Policy

Suhas Subramanyam is a Special Assistant and Policy Advisor in the White House Office of Science and Technology Policy

THE FINAL STATE OF THE UNION

Watch President Obama's final State of the Union address.

THE SUPREME COURT

Read what the President is looking for in his next Supreme Court nominee.

FIND YOUR PARK

Take a look at America's three newest national monuments.

HOME BRIEFING ROOM ISSUES THE ADMINISTRATION PARTICIPATE 1600 PENN

En Español | Accessibility | Copyright Information | Privacy Policy | USA.gov

Exploring the Dimensions of Trustworthiness: Challenges and Opportunities

August 30-31, 2016 - *Gaithersburg, MD Campus*

AGENDA (FINAL)

Tuesday August 30, 2016 – Green Auditorium

7:30 am Registration

8:00 am Opening Session (Moderator: Dave Wollman, NIST)

- **Welcome** ~ Chris Greer, NIST
- **Importance and Context of Trustworthiness** ~ Ron Ross, NIST
- **Workshop Objectives** ~ Edward Griffor, NIST

8:30 am Keynote

- **CPS/IoT Trustworthiness – Future Vision and Challenges** ~ Vint Cerf, Google

9:15 am Elements of Risk management for Trustworthiness (Moderator: N. Ivy, NIST)

Trustworthiness Risk Management in Connected, Interacting Environments

- Todd Grams, Deloitte and Touche LLC
- Karen Hardy, U.S. Department of Commerce
- Michael Huth, Imperial College London

What are the key elements of risk management frameworks that are useful to consider in the context of the various Trustworthiness concerns?

How can risk management frameworks support consideration of risks across the various Trustworthiness concern areas?

How can existing risk management frameworks assist in measuring risks in Trustworthiness?

10:30 am White House Priorities for trustworthy CPS/IoT Systems

- Greg Shannon, Assistant Director for Cyber Strategy, Office of Science and Technology Policy

10:50 am Break

Trustworthiness Concerns Working Sessions

Working sessions will review current approaches to the trustworthiness concerns in question (e.g., standards and best practices that are process- or certification-based). Each session will consist of remarks by subject matter experts followed by a general Q&A session addressing:

How is safety/ security/ privacy/ resilience/ reliability currently addressed and how is that affected by new CPS/IoT challenges?

What types of metrics exist for safety/ security/ privacy/ resilience/reliability and what data/information is needed to develop or improve these metrics?

How do current methodologies for safety/security/privacy/resilience/reliability interact with those of the other dimensions of trustworthiness? What dependencies are recognized between these areas/disciplines?

Additional discussion will take place following initial remarks focusing on the challenges to the approaches posed by CPS and IoT. Key issues include:

- *Conflicts and Collaborations between CPS Concerns*
- *Cyber-Physical Interactions*
- *Unmanaged Composition in Future CPS/IoT*

11:05 am Session I: CPS Safety (Moderator: C. Vishik, Intel)

Safety Challenges in Freely Composed CPS

- James Boehm, McKinsey
- Albert Wavering, NIST

Tuesday August 30, 2016 – Green Auditorium

- Joe Miller, TRW/ZF
- Ravi Jain, FAA
- Pieter Mosterman, Mathworks

1:00 pm Lunch NIST Cafeteria, Bldg. 101

2:00 pm Session II: CPS Privacy (Moderator: N. Lefkovitz, NIST)

Privacy in a Highly Connected World of CPS

- Lorrie Cranor, Federal Trade Commission
- Stacey Gray, Future of Privacy Forum
- Ellen Nadeau, NIST
- Alvaro Cardenas, University of Texas, Dallas

3:15 pm First Day Review of Results and Next Day Objectives

4:00 pm Adjourn Day 1

Wednesday Morning, August 31, 2016 – Green Auditorium

8:30 am First Day Review

9:00 am Keynote

- **Trustworthiness – Government Perspectives ~** Tony Scott, U.S. Chief Information Officer

9:45 am Session III: CPS Resilience and Reliability (Moderator: T. McAllister, NIST)

Resilience and Reliability Challenges and CPS Game-Changers

- Bruce McMillin, Missouri University of Science and Technology
- Pat Muoio, G2 Inc.
- Janos Sztipanovits, Vanderbilt University
- Deb Bodeau, The MITRE Corporation

11:15 am Session IV: CPS Security (Moderator: R. Ross, NIST)

Challenges and Opportunities – Building Trustworthy Secure Systems

- Cynthia Irvine, Naval Postgraduate School
- Michael McEvilley, The MITRE Corporation
- Steve Lipner, Formerly Microsoft Corporation

12:30 pm Lunch NIST Cafeteria, Bldg. 101

1:30 pm Dialogue on Guiding Principles for Securing IoT

- Robert Silvers, Assistant Secretary for Cyber Policy, U.S. Department of Homeland Security

2:15 pm Crosscutting Scenario for Trustworthiness (Moderator: E. Griffor)

A high-profile, trustworthiness risk scenario, chosen at the end of the first day of the workshop, will be analyzed along the dimensions of safety/security/privacy/ resilience/reliability. The session participants will point out the tradeoffs between those concerns and assess the impact of the CPS and IoT challenges. On stage will be individuals representing the different Trustworthiness concerns.

- 'Pacemaker Syndrome' - ('Homeland Video')
- 'Deceiving the Operator: Hollywood Scenario' – ('Power Plant Gone Wild Video')
- 'Hacked Vehicle' – ('Vehicle Highjack Video')

Tuesday August 30, 2016 – Green Auditorium

3:15 pm	Closing Summary - Wrap up and Next Steps
3:45 pm	Adjourn

Questions/Challenges/Scenario Lists for Workshop Sessions

Trustworthiness Risk Management

- What are the key elements of risk management frameworks that are useful to consider in the context of the various Trustworthiness concerns?
- How can risk management frameworks support consideration of risks across the various trustworthiness concern areas?
- How can existing risk management frameworks assist in measuring risks in Trustworthiness?

CPS and IoT Challenges

- Conflicts and collaborations between CPS Concerns
- Cyber-Physical Interactions
- Unmanaged Composition in Future CPS/IoT

Trustworthiness Dimension Sessions

(Safety/Security/Privacy/Resilience/Reliability)

- How is safety/security/privacy/resilience/reliability currently addressed and how is that affected by new CPS/IoT challenges?
- What types of metrics exist for safety/security/privacy/resilience/reliability and what data/information is needed to develop or improve these metrics?
- How do current methodologies for safety/security/privacy/resilience/reliability interact with those of the other dimensions of trustworthiness? What dependencies are recognized between these areas/disciplines?

Crosscutting Scenarios

- ‘Pacemaker Syndrome’ - (‘Homeland Video’)
- ‘Deceiving the Operator: Hollywood Scenario’ – (‘Power Plant Gone Wild Video’)
- ‘Hacked Vehicle’ – (‘Vehicle Highjack Video’)

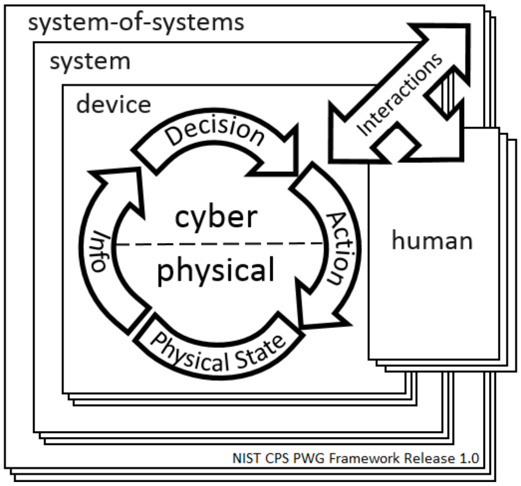
NIST Website (http://www.nist.gov) | About NIST (http://www.nist.gov/public_affairs/nandyou.cfm) | usnistgov on Github (https://github.com/usnistgov)

CPS Public Working Group

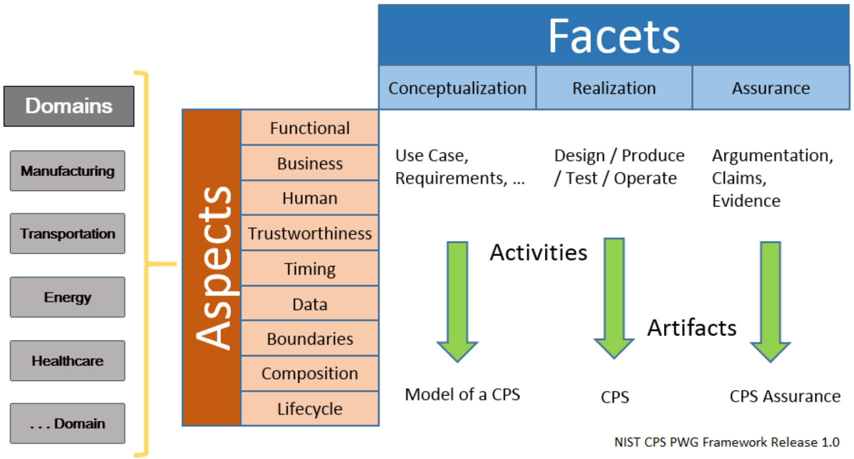
Robots for Manufacturing, Healthcare, and Disaster Response

Robots are CPS that can be designed to accomplish tasks that were not possible before. Robots are now being used to fabricate thin film solar photovoltaic cells with greater precision and speed, assemble complex manufacturing components, and guide delicate surgical operations.

CPS PWG Cyber-Physical Systems (CPS) Framework Release 1.0



CPS Conceptual Model



CPS Framework – Domains, Facets, Aspects

The CPS Public Working Group has completed the CPS Framework Release 1.0

The CPS Framework is freely available for download here (https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf). An additional Technical Annex, Timing Framework for Cyber-Physical Systems, is also freely available for download here (https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Timing_Annex_for_Draft_Framework_for_Cyber-Physical_Systems_Release_0.8_September_2015.pdf).

Note 20170513: NIST is convening a short term (summer 2017) collaboration to produce a white paper on communications requirements for federated testbeds. See here for more information. (/cpspwg/community/federatedcommunications) If you are interested contact Dr. Martin Burns (martin dot burns at nist dot gov) for more information.

What is this Collaboration?

The impacts of CPS will be revolutionary and pervasive – this is evident today in emerging smart cars, intelligent buildings, robots, unmanned vehicles, and medical devices. Realizing the future promise of CPS will require interoperability between elements and systems, supported by new reference architectures and common definitions and lexicons. Addressing the problems and opportunities of CPS requires broad collaboration to develop a consensus around these concepts, and a shared understanding of the essential roles of timing and cybersecurity. To this end, NIST has established the CPS Public Working Group (CPS PWG), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally.

About Us (/cpspwg/aboutus)

Learn about this collaboration

Working Groups (/cpspwg/community)

Vocabulary and Reference Architecture, Cybersecurity and Privacy, Timing, Data Interoperability, Use Cases

Resources (/cpspwg/library)

Videos, presentations, and documents

Working Groups

Vocabulary and Reference Architecture

Focus on developing a consensus definition of CPS and common taxonomy. The group will identify a classification model based on common features, capabilities, and characteristics to inform reference architecture. The reference architecture will include identification of foundational goals, characteristics, common roles, actors, and interfaces, across CPS domains, while considering cybersecurity and privacy.

Use Cases

Use Cases Identify CPS use cases, both current and envisioned, in specific sectors, domains, and applications. Use cases will provide an understanding of how actors within CPS systems will interact, as well as generate information on functional requirements for reference architecture. Use cases will also help to identify and evaluate common CPS characteristics, actors, interfaces, and associated applied cybersecurity objectives and considerations.

Timing

Timing and Synchronization Evaluate timing and synchronization needs, and ensure that reference architectures and use cases consider issues of timing and synchronization. The subgroup will identify research needed in this area, and optimal pathways for addressing the challenges of timing and synchronization. This sub-group includes an existing organization, Time Aware Applications, Computers and Communications Systems (TAACCS), led by NIST.

Cybersecurity and Privacy

Develop a cybersecurity and privacy strategy for the common elements of CPS. This includes identification, implementation, and monitoring of specific cybersecurity activities (including the identification, protection, detection, response and recovery of CPS elements) and outcomes for CPS in the context of a risk management program. Where applicable standards, guidelines, and measurement metrics do not exist, this subgroup will identify areas for further CPS cybersecurity research and development.

Data Interoperability

This subgroup will address the simplification and streamlining of cross-domain data interactions by developing a sound underlying framework and standards base for CPS data interoperability, in part by developing an inventory of relevant existing practices and standards. There are many CPS domains in which data is created, maintained, exchanged, and stored. Each datum has a data flow and a life cycle. Each domain naturally defines its own data semantics and exchange protocols, but those data can be difficult to understand and process when moved across domains and ownership boundaries, an increasing requirement of an increasingly connected world. This is as much, if not more so, the case in cyber physical systems as it is in other data management domains. We will address these cross-cutting data interoperability issues and point the way to the development of new efficient and scalable approaches to managing CPS data.

(/cpspwg/) About Us (/cpspwg/aboutus) Working Groups (/cpspwg/community) Resources (/cpspwg/library)

Get Started (mailto:CPSPWGCoordinator@energetics.com?subject=CPSPWG website Contact&body=Hi!%0A%0AI'd%20like%20to%20learn%20more%20about%20how%20our%2

PLEASE NOTE: This is a collaborative website. NIST does not endorse the views expressed, or necessarily concur with the information presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. All the material on this website is in the public domain and is intended for unrestricted use by interested parties, including any text, diagrams, or images, unless indicated explicitly.

Don't share anything on this site that you do not want to be public. Do not post any proprietary documents, information or data Anything placed on this site is considered public disclosure and it shall be deemed to have been disclosed on a non-confidential basis, without any restrictions on use by anyone, except that no valid copyright or patent right shall be deemed to have been waived by such disclosure.

Certain commercial equipment, instruments, materials, systems, software, and trade names may be identified throughout this site in order to specify or identify technologies adequately. Such identification is not intended to imply recommendation or endorsement by NIST or any other party, nor is it intended to imply that the systems or products identified are necessarily the best available for the purpose. All data and other information posted on this site is provided as a public service and is provided “AS IS.” NIST MAKES NO WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND DATA ACCURACY.

By selecting external links, you will be leaving NIST webspace. Links to other websites are provided because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose.
Privacy Policy (http://www.nist.gov/public_affairs/privacy.cfm#privpolicy) | Security Notice (http://www.nist.gov/public_affairs/privacy.cfm#secnot) | Accessibility Statement (http://www.nist.gov/public_affairs/privacy.cfm#accesstate) | Send feedback (mailto:sgwikisupport@nist.gov?subject=Feedback%20on%20cpspwg%20Web%20Site)

National Telecommunications
& Information Administration
United States Department of Commerce

Search this site Search

TOPICS | NEWSROOM | PUBLICATIONS | BLOG | OFFICES | ABOUT | CONTACT

- Spectrum Management
- Broadband
- Internet Policy
- Domain Name System
- Public Safety
- Grants
- Institute for Telecommunication Sciences
- Data Central

Home » Publications » Federal Register Notices » 2016

Fostering the Advancement of the Internet of Things Workshop

Printer-friendly version

Topics: Internet Policy Internet Policy Task Force Internet of Things

Date:
August 30, 2016

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene a workshop on behalf of the U.S. Department of Commerce's Internet Policy Task Force and the Digital Economy Leadership Team on Fostering the Advancement of the Internet of Things.

DATES: The workshop will be held on September 1, 2016, from 9:00 a.m. to 3:00 p.m., Eastern Daylight Time.

ADDRESSES: The workshop will be held at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia 22314. Please refer to NTIA's Web site, http://www.ntia.doc.gov/category/internet-things, for the most current information.

FOR FURTHER INFORMATION CONTACT: Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230; telephone (202) 482-3522; email thall@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002; email press@ntia.doc.gov.

Workshop presentations

- IoT Workshop Notice
- IoT Workshop Agenda

Featured Initiatives

- Digital Literacy
- BroadbandUSA
- Internet Policy Task Force
- Wireless Broadband: 500MHz
- National Broadband Map

National Telecommunications and Information Administration
1401 Constitution Ave., NW Washington, DC 20230

COMMERCE.GOV | PRIVACY POLICY | WEB POLICIES | FOIA | ACCESSIBILITY | USA.GOV

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Fostering the Advancement of the Internet of Things Workshop

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of open meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene a workshop on behalf of the U.S. Department of Commerce's Internet Policy Task Force and the Digital Economy Leadership Team on Fostering the Advancement of the Internet of Things.

DATES: The workshop will be held on September 1, 2016, from 9:00 a.m. to 3:00 p.m., Eastern Daylight Time.

ADDRESSES: The workshop will be held at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia 22314. The location of the meeting is subject to change. Please refer to NTIA's Web site, *http://www.ntia.doc.gov/category/internet-things*, for the most current information.

FOR FURTHER INFORMATION CONTACT: Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230; telephone (202) 482–3522; email *thall@ntia.doc.gov.* Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482–7002; email *press@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION: Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education, and civic and cultural life, the Department of Commerce has made it a top priority to encourage growth of the digital economy and ensure that the Internet remains an open platform for innovation and free expression. As part of the Department's Digital Economy Agenda, the National Telecommunications and Information Administration (NTIA) initiated an inquiry regarding the Internet of Things (IoT) to review the current technological and policy landscape, which included a Request for Comment on ''The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.'' [1] This workshop will build on the comments received in the Request for Comment, focusing specifically on the potential benefits and challenges of these technologies and what role, if any, the U.S. Government should play in this area. This workshop will help to inform the Department's forthcoming issue-spotting, agenda-setting green paper on IoT.

NTIA will post a detailed agenda on its Web site, *www.ntia.doc.gov/category/internet-things*, prior to the meeting. The workshop will consist of a number of panels and speakers that will explore in more depth the obstacles and opportunities raised by commenters on the federal government's role in IoT deployment. Agenda topics and format are subject to change.

The meeting is open to the public and the press. The meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Travis Hall at (202) 482–3522 or *thall@ntia.doc.gov* at least seven (7) business days prior to the meeting. The meeting will also be webcast. Requests for real-time captioning of the webcast or other auxiliary aids should be directed to Travis Hall at (202) 482–3522 or *thall@ntia.doc.gov* at least seven (7) business days prior to the meeting. Please refer to NTIA's Web site, *http://www.ntia.doc.gov/category/internet-things*, for the most current information.

Dated: August 5, 2016.

Angela M. Simpson,

Deputy Assistant Secretary, National Telecommunications and Information Administration.

[FR Doc. 2016–19048 Filed 8–10–16; 8:45 am]

BILLING CODE 3510–60–P

COMMODITY FUTURES TRADING COMMISSION

Agency Information Collection Activities Under OMB Review

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995 (PRA), this notice announces that the Information Collection Request (ICR) abstracted below has been forwarded to the Office of Management and Budget (OMB) for review and comment. The ICR describes the nature of the information collection and its expected costs and burden.

DATES: Comments must be submitted on or before September 12, 2016.

ADDRESSES: Comments regarding the burden estimated or any other aspect of the information collection, including suggestions for reducing the burden, may be submitted directly *to the Office of Information and Regulatory Affairs (OIRA) in OMB, within 30 days* of the notice's publication, by email at *OIRAsubmissions@omb.eop.gov.* Please identify the comments by OMB Control No. 3038–NEW. Please provide the Commodity Futures Trading Commission (''CFTC'' or ''Commission'') with a copy of all submitted comments at the address listed below. Please refer to OMB Reference No. 3038–NEW, found on *http://reginfo.gov.* Comments may also be mailed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Commodity Futures Trading Commission, 725 17th Street NW., Washington, DC 20503, and to: Nisha Smalls, Office of Customer Education and Outreach, Commodity Futures Trading Commission, 1155 21st Street NW., Washington, DC 20581; or through the Agency's Web site at *http://comments.cftc.gov.* Follow the instructions for submitting comments through the Web site.

Comments may also be mailed to: Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW., Washington, DC 20581; or sent by hand delivery/courier to the same address.

A copy of the supporting statements for the collection of information discussed above may be obtained by visiting *reginfo.gov.* All comments must be submitted in English, or if not, accompanied by an English translation. Comments will be posted as received to *http://www.cftc.gov.*

FOR FURTHER INFORMATION CONTACT: Nisha Smalls, Office of Customer Education and Outreach, Commodity Futures Trading Commission, 1155 21st Street NW., Washington, DC 20581, (202) 418–5895; FAX: (202) 418–5541; email: *nsmalls@cftc.gov* and refer to this **Federal Register** notice. A copy may also be obtained from this contact.

SUPPLEMENTARY INFORMATION: The Commission's Office of Customer Education and Outreach (OCEO) develops campaigns to change customer behaviors, so that customers can better avoid fraud as defined under the Commodity Exchange Act. The OCEO intends to survey the public by

[1] Request for Comments on the Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things (Apr. 5, 2016) available at *https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.*

Briefing Room

Your Weekly Address

Speeches & Remarks

Press Briefings

Statements & Releases

White House Schedule

Presidential Actions

Executive Orders

Presidential Memoranda

Proclamations

Legislation

Pending Legislation

Signed Legislation

Vetoed Legislation

Nominations & Appointments

Disclosures

The White House

Office of the Press Secretary

For Immediate Release February 09, 2016

SHARE THIS:

FACT SHEET: Cybersecurity National Action Plan

Taking bold actions to protect Americans in today’s digital world.

From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation, and for more than seven years he has acted comprehensively to confront that challenge. Working together with Congress, we took another step forward in this effort in December with the passage of the Cybersecurity Act of 2015, which provides important tools necessary to strengthen the Nation's cybersecurity, particularly by making it easier for private companies to share cyber threat information with each other and the Government.

But the President believes that more must be done – so that citizens have the tools they need to protect themselves, companies can defend their operations and information, and the Government does its part to protect the American people and the information they entrust to us. That is why, today, the President is directing his Administration to implement a **Cybersecurity National Action Plan (CNAP)** that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.

The Challenge

From buying products to running businesses to finding directions to communicating with the people we love, an online world has fundamentally reshaped our daily lives. But just as the continually evolving digital age presents boundless opportunities for our economy, our businesses, and our people, it also presents a new generation of threats that we must adapt to meet. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. Identity theft is now the fastest growing crime in America. Our innovators and entrepreneurs have reinforced our global leadership and grown our economy, but with each new story of a high-profile company hacked or a neighbor defrauded, more Americans are left to wonder whether technology's benefits could risk being outpaced by its costs.

The President believes that meeting these new threats is necessary and within our grasp. But it requires a bold reassessment of the way we approach security in the digital age. If we're going to be connected, we need to be protected. We need to join together—Government, businesses, and individuals—to sustain the spirit that has always made America great.

Our Approach

That is why, today, the Administration is announcing a series of near-term actions to enhance cybersecurity capabilities within the Federal Government and across the country. But given the complexity and seriousness of the issue, the President is also asking some of our Nation's top strategic, business, and technical thinkers from outside of government to study and report on what more we can do to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. Bold action is required to secure our digital society and keep America competitive in the global digital economy.>/p>

The President's **Cybersecurity National Action Plan (CNAP)** is the capstone of more than seven years of determined effort by this Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions. This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives. Highlights of the CNAP include actions to:

- **Establish the "Commission on Enhancing National Cybersecurity."** This Commission will be comprised of top strategic, business, and technical thinkers from outside of Government – including members to be designated by the bi-partisan Congressional leadership. The Commission will make recommendations on actions that can be taken over the next decade to strengthen cybersecurity in both the public and private sectors while protecting privacy; maintaining public safety and economic and national security; fostering discovery and development of new technical solutions; and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies, and best practices.
- Modernize Government IT and transform how the Government manages cybersecurity through the proposal of a **$3.1 billion Information Technology Modernization Fund**, which will enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain, as well as the formation of a new position – the **Federal Chief Information Security Officer** – to drive these changes across the Government.
- **Empower Americans to secure their online accounts** by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single use code delivered in a text message, Americans can make their accounts even more secure. This focus on **multi-factor authentication** will be central to a new **National Cybersecurity Awareness Campaign** launched by the **National Cyber Security Alliance** designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world. The National Cyber Security Alliance will partner with leading technology firms like **Google**, **Facebook**, **DropBox**, and **Microsoft** to make it easier for millions of users to secure their online accounts, and financial services companies such as **MasterCard**, **Visa**, **PayPa**l, and **Venmo** that are making transactions more secure. In addition, the Federal Government will take steps to safeguard personal data in online transactions between citizens and the government, including through a **new action plan** to drive the Federal Government's adoption and use of effective identity proofing and strong multi-factor authentication methods and a systematic review of where the Federal Government can reduce reliance on Social Security Numbers as an identifier of citizens.
- **Invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget**. This represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity, a necessary investment to secure our Nation in the future.

Through these actions, additional new steps outlined below, and other policy efforts spread across the Federal Government, the Administration has charted a course to enhance our long-term security and reinforce American leadership in developing the technologies that power the digital world.

Commission on Enhancing National Cybersecurity

For over four decades, computer technology and the Internet have provided a strategic advantage to the United States, its citizens, and its allies. But if fundamental cybersecurity and identity issues are not addressed, America's reliance on digital infrastructure risks becoming a source of strategic liability. To address these issues, we must diagnose and address the causes of cyber-vulnerabilities, and not just treat the symptoms. Meeting this challenge will require a long-term, national commitment.

To conduct this review, the President is establishing the **Commission on Enhancing National Cybersecurity**, comprised of top strategic, business, and technical thinkers from outside of Government – including members to be designated by the bi-partisan Congressional leadership. The Commission is tasked with making detailed recommendations on actions that can be taken over the next decade to enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security. The National Institute of Standards and Technology will provide the Commission with support to allow it to carry out its mission. The Commission will report to the President with its specific findings and recommendations before the end of 2016, providing the country a roadmap for future actions that will build on the CNAP and protect our long-term security online.

Raise the Level of Cybersecurity across the Country

While the Commission conducts this forward looking review, we will continue to raise the level of cybersecurity across the Nation.

Strengthen Federal Cybersecurity
The Federal Government has made significant progress in improving its cybersecurity capabilities, but more work remains. To expand on that progress and address the longstanding, systemic challenges in Federal cybersecurity, we must re-examine our Government's legacy approach to cybersecurity and information technology, which requires each agency to build and defend its own networks. These actions build upon the foundation laid by the **Cybersecurity Cross-Agency Priority Goals** and the **2015 Cybersecurity Strategy and Implementation Plan**.

- The President's 2017 Budget proposes a **$3.1 billion Information Technology Modernization Fund**, as a down payment on the comprehensive overhaul that must be undertaken in the coming years. This revolving fund will enable agencies to invest money up front and realize the return over time by retiring, replacing, or modernizing antiquated IT infrastructure, networks, and systems that are expensive to maintain, provide poor functionality, and are difficult to secure.

- The Administration has created the position of **Federal Chief Information Security Officer** to drive cybersecurity policy, planning, and implementation across the Federal Government. This is the first time that there will be a dedicated senior official who is solely focused on developing, managing, and coordinating cybersecurity strategy, policy, and operations across the entire Federal domain.
- The Administration is requiring agencies to identify and prioritize their **highest value and most at-risk IT assets** and then take additional concrete steps to improve their security.
- The Department of Homeland Security, the General Services Administration, and other Federal agencies will increase the availability of **government-wide shared services for IT and cybersecurity**, with the goal of taking each individual agency out of the business of building, owning, and operating their own IT when more efficient, effective, and secure options are available, as well as ensuring that individual agencies are not left on their own to defend themselves against the most sophisticated threats.
- The Department of Homeland Security is **enhancing Federal cybersecurity by expanding the EINSTEIN and Continuous Diagnostics and Mitigation programs**. The President's 2017 Budget supports all Federal civilian agencies adopting these capabilities.
- The Department of Homeland Security is dramatically **increasing the number of Federal civilian cyber defense teams to a total of 48**, by recruiting the best cybersecurity talent from across the Federal Government and private sector. These standing teams will protect networks, systems, and data across the entire Federal Civilian Government by conducting penetration testing and proactively hunting for intruders, as well as providing incident response and security engineering expertise.
- The Federal Government, through efforts such as the National Initiative for Cybersecurity Education, will enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure Federal agencies. As part of the CNAP, the President's Budget invests **$62 million in cybersecurity personnel** to:
    - Expand the Scholarship for Service program by establishing a **CyberCorps Reserve** program, which will offer scholarships for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal government;
    - Develop a **Cybersecurity Core Curriculum** that will ensure cybersecurity graduates who wish to join the Federal Government have the requisite knowledge and skills; and,
    - Strengthen the **National Centers for Academic Excellence in Cybersecurity Program** to increase the number of participating academic institutions and students, better support those institutions currently participating, increase the number of students studying cybersecurity at those institutions, and enhance student knowledge through program and curriculum evolution.
- The President's Budget takes additional steps to expand the cybersecurity workforce by:
    - Enhancing **student loan forgiveness programs for cybersecurity experts** joining the Federal workforce;

  - Catalyzing investment in cybersecurity education as part of a robust computer science curriculum through **the President's Computer Science for All Initiative**.

Empower Individuals

The privacy and security of all Americans online in their daily lives is increasingly integral to our national security and our economy. The following new actions build on the President's **2014 BuySecure Initiative** to strengthen the security of consumer data.

- The President is calling on Americans to move beyond just the password to leverage **multiple factors of authentication** when logging-in to online accounts. Private companies, non-profits, and the Federal Government are working together to help more Americans stay safe online through a new public awareness campaign that focuses on broad adoption of multi-factor authentication. Building off the Stop.Think.Connect. campaign and efforts stemming from the National Strategy for Trusted Identities in Cyberspace, the National Cyber Security Alliance will **partner with leading technology companies and civil society** to promote this effort and make it easier for millions of users to secure their accounts online. This will support a broader effort to increase public awareness of the individual's role in cybersecurity.
- The Federal Government is **accelerating adoption of strong multi-factor authentication and identity proofing** for citizen-facing Federal Government digital services. The General Services Administration will establish a new program that will better protect and secure the data and personal information of Americans as they interact with Federal Government services, including tax data and benefit information.
- The Administration is conducting a systematic review of where the Federal Government can **reduce its use of Social Security Numbers** as an identifier of citizens.
- The Federal Trade Commission recently relaunched **IdentityTheft.Gov**, to serve as a one-stop resource for victims to report identity theft, create a personal recovery plan, and print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors.
- The Small Business Administration (SBA), partnering with the Federal Trade Commission, the National Institute of Standards and Technology (NIST), and the Department of Energy, will offer **cybersecurity training to reach over 1.4 million small businesses** and small business stakeholders through 68 SBA District Offices, 9 NIST Manufacturing Extension Partnership Centers, and other regional networks across the country.
- The Administration is announcing new milestones in **the President's BuySecure Initiative** to secure financial transactions. As of today the Federal Government has supplied over **2.5 million more secure Chip-and-PIN payment cards**, and transitioned to this new technology the entire fleet of card readers managed by the Department of the Treasury. Through government and private-sector leadership, more secure chip cards have been issued in the United States than any other country in the world.

Enhance Critical Infrastructure Security and Resilience

The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure. A continued partnership with the owners and operators of critical infrastructure will improve cybersecurity and enhance the Nation's resiliency. This work builds off the President's previous cybersecurity focused Executive Orders on **Critical Infrastructure** (2013) and **Information Sharing** (2015).

- The Department of Homeland Security, the Department of Commerce, and the Department of Energy are contributing resources and capabilities to establish a **National Center for Cybersecurity Resilience** where companies and sector-wide organizations can test the security of systems in a contained environment, such as by subjecting a replica electric grid to cyber-attack.
- The Department of Homeland Security will **double the number of cybersecurity advisors** available to assist private sector organizations with in-person, customized cybersecurity assessments and implementation of best practices.
- The Department of Homeland Security is collaborating with UL and other industry partners to develop a **Cybersecurity Assurance Program** to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.
- The National Institute of Standards and Technology is **soliciting feedback** in order to inform further development of its **Cybersecurity Framework** for improving critical infrastructure cybersecurity. This follows two years of adoption by organizations across the country and around the world.
- Yesterday, Commerce Secretary Pritzker cut the ribbon on the new **National Cybersecurity Center of Excellence**, a public-private research and development partnership that will allow industry and government to work together to develop and deploy technical solutions for high-priority cybersecurity challenges and share those findings for the benefit of the broader community.
- The Administration is calling on major health insurers and healthcare stakeholders to help them take new and significant steps to enhance their data stewardship practices and ensure that consumers can trust that their sensitive health data will be safe, secure, and available to guide clinical decision-making.

Secure Technology

Even as we work to improve our defenses today, we know the Nation must aggressively invest in the science, technology, tools, and infrastructure of the future to ensure that they are engineered with sustainable security in mind.

- Today the Administration is releasing its **2016 Federal Cybersecurity Research and Development Strategic Plan**. This plan, which was called for in the 2014 Cybersecurity Enhancement Act, lays out strategic research and development goals for the Nation to advance cybersecurity technologies driven by the scientific evidence of efficacy and efficiency.
- In addition, the Government will work with organizations such as the Linux Foundation's **Core Infrastructure Initiative** to fund and secure commonly used internet "utilities" such as open-

source software, protocols, and standards. Just as our roads and bridges need regular repair and upkeep, so do the technical linkages that allow the information superhighway to flow.

Deter, Discourage, and Disrupt Malicious Activity in Cyberspace

Better securing our own digital infrastructure is only part of the solution. We must lead the international effort in adopting principles of responsible state behavior, even while we take steps to deter and disrupt malicious activity. We cannot pursue these goals alone – we must pursue them in concert with our allies and partners around the world.

- In 2015, members of the G20 joined with the United States in affirming important norms, including the applicability of international law to cyberspace, the idea that states should not conduct the cyber-enabled theft of intellectual property for commercial gain, and in welcoming the report of a United Nations Group of Governmental Experts, which included a number of additional norms to promote international cooperation, prevent attacks on civilian critical infrastructure, and support computer emergency response teams providing reconstitution and mitigation services. The Administration intends to institutionalize and implement these norms through **further bilateral and multilateral commitments** and confidence building measures.
- The Department of Justice, including the Federal Bureau of Investigation, is **increasing funding for cybersecurity-related activities by more than 23 percent** to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors.
- U.S. Cyber Command is building a **Cyber Mission Force** of 133 teams assembled from 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The Cyber Mission Force, which will be fully operational in 2018, is already employing capabilities in support of U.S. Government objectives across the spectrum of cyber operations.

Improve Cyber Incident Response

Even as we focus on preventing and deterring malicious cyber activity, we must also maintain resilience as events occur. Over the past year, the country faced a wide array of intrusions, ranging from criminal activity to cyber espionage. By applying lessons learned from past incidents we can improve management of future cyber incidents and enhance the country's cyber-resilience.

- By this spring, the Administration will publicly release **a policy for national cyber incident coordination** and an accompanying **severity methodology** for evaluating cyber incidents so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response.

Protect the Privacy of Individuals

In coordination with the information technology and cybersecurity efforts above, the Administration has launched a groundbreaking effort to enhance how agencies across the Federal Government protect the privacy of individuals and their information. Privacy has been core to our Nation from its inception, and in today's digital age safeguarding privacy is more critical than ever.

- Today, the President signed an Executive Order that created a permanent **Federal Privacy Council,** which will bring together the privacy officials from across the Government to help ensure the implementation of more strategic and comprehensive Federal privacy guidelines. Like cyber security, privacy must be effectively and continuously addressed as our nation embraces new technologies, promotes innovation, reaps the benefits of big data and defends against evolving threats.

Fund Cybersecurity

In order to implement these sweeping changes, the Federal Government will need to invest additional resources in its cybersecurity. That is why the 2017 Budget allocates more than $19 billion for cybersecurity – a more than 35 percent increase over the 2016 enacted level. These resources will enable agencies to raise their level of cybersecurity, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents.

HOME BRIEFING ROOM ISSUES THE ADMINISTRATION PARTICIPATE 1600 PENN

En Español | Accessibility | Copyright Information | Privacy Policy | USA.gov

the WHITE HOUSE PRESIDENT BARACK OBAMA

Launching a Smart Cities Initiative to Tackle City Challenges with Innovative Approaches

SEPTEMBER 16, 2015 AT 3:03 PM ET BY DAN CORREA

Summary: Over $160M in Federal research investments and more than 25 new technology collaborations to help cities solve problems announced at the Smart Cities Forum this week.

With more than 50 percent of people worldwide living in cities – a number projected to grow to nearly 70 percent by 2050 – the challenges cities face will also continue to grow. This includes everything from sustainability and energy use to safety and effective service delivery.

But, if researchers, public officials, citizens and companies can develop effective solutions to these challenges, the impact at home and abroad will be enormous.

Technology is creating new opportunities to reduce traffic congestion, fight crime, foster economic development, reduce greenhouse gases, and make local governments more open, responsive, and efficient. Around the world, cities are beginning to harness the power of sensors, engage citizens equipped with smartphones, cloud computing, high-speed networks, and data analytics.

Earlier this week, the Administration held a Smart Cities Forum and announced a new Smart Cities Initiative, which will invest over $160 million in Federal research and create more than 25 new technology collaborations to help local communities tackle 21st century challenges. By harnessing the growing data revolution and things like low-cost sensors and research collaborations, this Initiative is designed to support community efforts to come up with solutions to everyday problems.

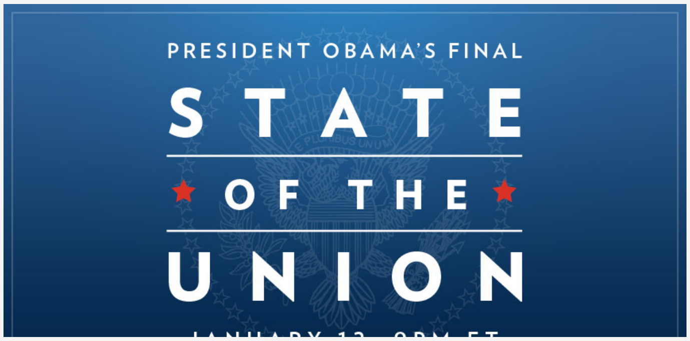
As part of the Smart Cities Initiative, many Federal agencies are also stepping up their efforts. The National Science Foundation (NSF) announced over $35 million in Smart Cities grants. The National Institute of Standards and Technology (NIST) is launching a new round of the Global City Teams Challenge – a project that brings together different organizations to develop Smart City goals and advance Smart City technologies to improve residential quality of life. The Environmental Protection Agency and the Departments of Homeland Security, Energy, Transportation, and Commerce are also investing in smart city applications with projects that will help improve air-quality monitoring, increase the effectiveness of first responders, reduce traffic congestion, enhance energy-efficiency, and foster entrepreneurship.

Additional efforts will be led by new collaborations among industry, city governments, universities, and local stakeholders. Mayors Pete Buttigieg of South Bend, Indiana, and William Peduto of Pittsburgh, Pennsylvania, on behalf of 22 city-university pairs of collaborators, announced the launch of the MetroLab Network, which will pilot over 60 Smart City projects in the next year to improve the efficiency and effectiveness of infrastructure and services in our communities. Supported by the John D. and Catherine T. MacArthur Foundation, the MetroLab Network builds on successful models of university-city collaboration across the country by supporting new projects, sharing ideas, and striving to create a "new normal" of city-university collaboration for research and policy development.

Several private companies also made commitments that will help further these efforts. The Array of Things in Chicago – receiving over $3 million in funding from NSF on Monday – is a terrific example of the new collaborations underway that bring together Federal support with university and city collaborators. Comprised of 500 nodes deployed throughout the city of Chicago, each with power, Internet, and a base set of sensing and embedded information systems capabilities, the Array of Things will continuously measure the physical environment of urban areas at the city block scale and unlock promising new research trajectories. It is transformative projects like these that create the foundation for a new urban science to enable a deeper understanding of cities and what it will take to make them more livable, sustainable, equitable, and resilient.

As the new Smart Cities Initiative continues to mature, we hope to continue to grow the scale and scope of these collaborations, which are key to finding new approaches that will address the pressing urban challenges of our time.

Dan Correa is a Senior Advisor for Innovation Policy at the White House Office of Science and Technology Policy.



THE FINAL STATE OF THE UNION

Watch President Obama's final State of the Union address.

THE SUPREME COURT

Read what the President is looking for in his next Supreme Court nominee.

National Telecommunications & Information Administration
United States Department of Commerce

Search this site Search

TOPICS | NEWSROOM | PUBLICATIONS | BLOG | OFFICES | ABOUT | CONTACT

- Spectrum Management
- Broadband
- Internet Policy
- Domain Name System
- Public Safety
- Grants
- Institute for Telecommunication Sciences
- Data Central

Home » Blog

Increasing the Potential of IoT through Security and Transparency

August 02, 2016 by Angela Simpson, Deputy Assistant Secretary for Communications and Information

The Internet of Things (IoT) offers a wide range of consumer benefits - from the ability to control your thermostat or light fixtures through a smartphone, to an Internet-connected home security system, to wearables such as Internet-connected fitness bands and watches and beyond. To help realize the full innovative potential of IoT, users need reasonable assurance that IoT devices and applications will be secure.

One particular area of concern is whether and how to address potential security vulnerabilities in IoT devices or applications through patching and security upgrades. In the early IoT market, there has sometimes been limited consideration for supporting future security patches, even though many devices will eventually need them. Enabling a thriving market for devices that support security upgrades requires common definitions so consumers know what they are getting.

Currently, no such common, widely accepted definitions exist, and manufacturers can struggle to effectively communicate to consumers the security features of their devices. This is detrimental to the digital ecosystem as a whole, as it does not reward companies that invest in patching and it prevents consumers from making informed purchasing choices.

A range of **commenters** on NTIA's recent IoT Request for Comment and last year's **Request for Comment** related to cybersecurity identified security upgradability as an issue that required attention and coordination. In response, NTIA is planning to launch a new multistakeholder process to support better consumer understanding of IoT products that support security upgrades. We have utilized this approach to help make progress on issues such as **cybersecurity vulnerability disclosure** and **providing more transparency** about data collected by mobile apps. Given the burgeoning consumer adoption of IoT, the time seems ripe to bring stakeholders together to help drive some guidelines to encourage the growth of IoT.

The goal of the new multistakeholder process will be to promote transparency in how patches or upgrades to IoT devices and applications are deployed. Potential outcomes could include a set of common, shared terms or definitions that could be used to standardize descriptions of security upgradability or a set of tools to better communicate security upgradability.

As with our other multistakeholder processes, it will be up to stakeholders to determine what outcome they want and when they have reached consensus on it. NTIA will act as a neutral convener. We welcome broad participation and diverse perspectives. For more information, and to indicate your interest in participating, **please contact NTIA**. Stay tuned for an announcement on the first meeting of this new process, which we hope to convene in early fall.

Topics: Internet Policy Task Force Cybersecurity Internet of Things Internet Policy

SHARE Printer-friendly version

Featured Initiatives

- Digital Literacy
- BroadbandUSA
- Internet Policy Task Force
- Wireless Broadband: 500MHz
- National Broadband Map

National Telecommunications and Information Administration
1401 Constitution Ave., NW Washington, DC 20230