Testimony of

Charles H. Romine, Ph.D.
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
United States Senate
Committee on Commerce, Science, and Transportation
Subcommittee on Security

“Strengthening the Cybersecurity of the Internet of Things”

April 30, 2019

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to testify today on *Strengthening the Cybersecurity of the Internet of Things* (IoT), which is of critical importance to the security and economic well-being of America.

The rapid proliferation of internet-connected devices and rise of the IoT come with great anticipation. These newly connected devices bring the promise of enhanced business efficiencies and increased customer satisfaction. As the landscape of IoT continues to expand, it is vital to foster cybersecurity for devices and data in the IoT ecosystem, across industry sectors and at scale. Today I will discuss NIST's role in cultivating trust in the security of the Internet of Things.

NIST's Role in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role is to provide technologies, approved tools, data references and testing methods to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services. This role was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

The Internet of Things (IoT)

The Internet of Things is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT devices are an outcome of combining the worlds of information technology (IT) and operational technology (OT). With the inexpensive rise of WIFI and other connective technology chip sets and wireless technologies, we can connect almost anything to the internet and harness computing power far beyond our traditional personal computer and laptop environments. Many IoT devices now take advantage of the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances.

IoT devices can use computing functionality, data storage, and network connectivity for equipment that previously lacked them, enabling new efficiencies and technological capabilities for the equipment. IoT also adds the ability to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events. While the full scope of IoT is not precisely defined, it is clearly vast. Every sector has its own types of IoT devices, such as specialized hospital equipment in the healthcare sector and smart road technologies in the transportation sector, and there are many enterprise IoT devices that every sector can use.

Also, versions of nearly every consumer electronics device, many of which are also present in organizations' facilities, have become connected IoT devices—kitchen appliances, thermostats, home security cameras, door locks, light bulbs, and televisions. Many organizations are not necessarily aware that they are using a large number of IoT devices. It is important that organizations understand their use of IoT because many IoT devices affect cybersecurity and privacy risks differently than conventional IT devices do.

Many IoT devices interact with the physical world in ways conventional IT devices usually do not. For example, IoT devices with actuators have the ability to make changes to physical systems and thus affect the physical world. Another important aspect of IoT device interactions with the physical world is the operational requirements devices must meet in various environments and use cases. Many IoT devices must comply with stringent requirements for performance, reliability, resilience, safety, and other objectives. These requirements may be at odds with common cybersecurity and privacy practices for conventional IT.

Once organizations are aware of their existing IoT usage and possible future usage, they need to understand the IoT device risk considerations and the challenges they may cause to mitigating cybersecurity and privacy risks; adjust organizational policies and processes to address the cybersecurity and privacy risk mitigation challenges throughout the IoT device lifecycle; and implement updated mitigation practices for the organization's IoT devices.

NIST's Cybersecurity for the Internet of Things Program

The growth of network-connected devices, systems, and services comprising the IoT creates immense opportunities and benefits for our society. However, to reap the great benefits of IoT and to minimize the potentially significant risks, these network-connected devices need to be secure and resilient. This depends in large part upon the timely availability and widespread adoption of clear and effective international cybersecurity standards.

Securing IoT devices is a major challenge, as manufactures tend to focus on functionality, compatibility requirements, customer convenience, and time-to-market rather than security. Meanwhile, security threats are increasing. For example, Symantec reported a 600 percent increase in attacks against IoT devices from 2016 to 2017.[2]

The IoT ecosystem's nature brings new security considerations. These considerations include—but are not limited to—constrained power and processing; the ability to manage, update, and patch devices at scale; and a diverse set of new applications across consumer and industrial sectors.

NIST's *Cybersecurity for the Internet of Things* program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Additionally, NIST is studying the usability factors affecting cybersecurity and privacy perceptions of consumers of smart home devices to understand how these factors influence buying decisions and home use.

- **Considerations for Managing IoT Cybersecurity and Privacy Risks: NIST Internal Report 8228 (NISTIR 8228)**
  In recognition of a critical cybersecurity gap, NIST released draft NIST Internal Report 8228[3], Considerations for Managing IoT Cybersecurity and Privacy Risks in September 2018. The purpose of this publication is to help organizations better understand and manage the cybersecurity and privacy risks associated with IoT devices throughout their lifecycles. This publication emphasizes what makes managing these risks different for IoT devices than conventional IT devices, and it omits all aspects of risk management that are largely the same for IoT and conventional IT. The publication provides insights to inform organizations' risk management processes. For some IoT devices, additional types of risks, including safety, reliability, and resiliency, need to be managed simultaneously with cybersecurity and privacy risks because of the effects addressing one type of risk can have on others. Only cybersecurity and privacy risks are in scope for this publication.

- **Status of International Cybersecurity Standardization for IoT: NIST Internal Report 8200 (NISTIR 8200)**
  NIST Interagency Report 8200[4], published in November 2018, examines the current state of international cybersecurity standards development by voluntary consensus standards bodies for IoT. NISTIR 8200 is intended for use by the government and the broader public. The report aims to inform and enable policymakers, managers, and standards participants as they seek timely development and use of such standards in IoT components, systems, and related services.

[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[3] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf
[4] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

NISTIR 8200 establishes a common understanding of IoT components, systems and applications for which standards could be relevant. Additionally, it provides a functional description of IoT components, which are the basic building blocks of IoT systems. To provide insights into the present state of IoT cybersecurity standardization, the report describes five IoT technology application areas. These areas are certainly not exhaustive, but they are sufficiently representative to use in analyzing the present state of IoT cybersecurity standardization:

- Connected vehicle IoT enables vehicles, roads, and other infrastructure to communicate and share vital transportation information.
- Consumer IoT consists of IoT applications in residences as well as wearable and mobile devices.
- Health IoT processes data derived from sources such as electronic health records and patient-generated health data.
- Smart building IoT includes energy usage monitoring systems, physical access control security systems and lighting control systems.
- Smart manufacturing IoT enables enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services.

IoT cybersecurity objectives, risks, and threats are then analyzed for IoT applications in general and for each of the five illustrative IoT technology application areas. Cybersecurity objectives for traditional IT systems generally prioritize confidentiality, then integrity, and lastly availability. IoT systems cross multiple sectors as well as use cases within those sectors. Accordingly, cybersecurity objectives may be prioritized very differently by various parties, depending on the application. The increased ubiquity of IoT components and systems heighten the risks they present. Standards-based cybersecurity risk management will continue to be a major factor in the trustworthiness of IoT applications. Analysis of the application areas makes it clear that cybersecurity for IoT is unique and requires tailoring existing standards and creating new standards to address challenges, for example: pop-up network connections, shared system components, the ability to change physical aspects of the environment, and related connections to safety.

NISTIR 8200 describes 12 cybersecurity core areas and provides examples of relevant standards that while not exhaustive, represent an extensive effort to identify presently relevant IoT cybersecurity standards. The report's conclusions focus upon the issue of standards gaps and the effective use of existing standards.

- **Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats**

  In May 2018, the Departments of Commerce and Homeland Security published the Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats. Known as the Botnet Report, this report was developed in response to the May 11, 2018, Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[5] As

[5] Exec. Order No. 13800, 82 Fed. Reg. 22391, at 22394 (May 11, 2017): https://federalregister.gov/d/2017-10004

explained in the Botnet Report, resilience against botnets will require a multi-pronged approach, with many of the report's recommended actions being mutually supportive by design. The report called for the federal government to clearly delineate priorities for action, and a road map[6] was later released to identify tasks and timelines for completion. Recognizing that there is no one-size-fits-all, each of these recommendations and associated actions and tasks works towards achieving the overall goal of a more secure internet ecosystem. The road map also helps to sequence actions and tasks to achieve maximum benefit. As explained in the road map, before assessment, labeling, or awareness initiatives for IoT devices can begin, there first needs to be the foundational task of describing a core cybersecurity baseline, which is a set of cybersecurity capabilities that are broadly applicable across many or all IoT devices. The road map calls on NIST, in collaboration with stakeholders, to identify a core set of cybersecurity capabilities, which can also be used to support sector-specific baselines as needed, such as the federal government or home consumers. An identified core set of these capabilities would encourage harmonization and indicate the minimum cybersecurity capabilities any IoT device should support. A core baseline can serve as a foundation upon which more detailed and rigorous baselines for individual sectors and verticals can be developed. For example, a connected medical device would likely require more cybersecurity capabilities than an IoT light bulb.

- **Considerations for a Core IoT Cybersecurity Capabilities Baseline**
  On February 4, 2019, NIST published a discussion draft[7] to gather feedback to help identify core IoT cybersecurity capabilities that are most vital for IoT devices. Through NIST research, related stakeholder engagement, comments received during the NISTIR 8228 public comment period, and, as described above, in the Botnet Report, NIST identified a critical gap area in guidance on baselines for IoT device cybersecurity. In particular, there was interest in baselines focused on the pre-market cybersecurity capabilities that could be built into the products, as opposed to the cybersecurity controls that consumers or organizations that use IoT in their enterprise operations, could apply post-market.

  This paper presents one possible approach to developing baselines, which includes initial thoughts about what a core baseline of cybersecurity capabilities that are important for most IoT devices would look like. In this paper, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations. These could be used by IoT device manufacturers to guide the cybersecurity capabilities they implement in their products, as well as be used as a starting point by communities of interest to develop baselines appropriate to their community.

- **National Vulnerability Database**
  NIST's National Vulnerability Database (NVD)[8], supported by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, is the U.S. government

[6] https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[7] https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

[8] https://nvd.nist.gov

repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. NIST maintains the U.S. *National Vulnerability Database*, which is the worldwide public repository used to communicate vulnerabilities to the nation. NIST receives publicly available vulnerability information, standardizes it for use in scanners and vulnerability identification and mediation tools, and provides analysis and metrics for vulnerability severity. IoT vulnerabilities are one type of many items that are collected, scored and communicated in the NVD.

- **Lightweight Cryptography**
  There are many IoT areas in which highly-constrained devices are interconnected, typically communicating wirelessly with one another, and working in concert to accomplish some task. Security and privacy can be very important in all of these areas. Because the majority of current cryptographic algorithms were designed for desktop/server environments, many of these algorithms do not fit into the constrained resources. If current algorithms can be made to fit into the limited resources of constrained environments, then their performance may not be acceptable.

  NIST has initiated a process to solicit, evaluate, and standardize lightweight cryptographic algorithms[9] that are suitable for use in constrained environments where the performance of current NIST cryptographic standards is not acceptable. Today NIST is evaluating 56 potential lightweight encryption algorithms for use in these environments. As part of our plans for identifying the best, NIST will start to down select this initial set this Fiscal Year.

National Cybersecurity Center of Excellence (NCCoE)

Established in 2012, NIST's National Cybersecurity Center of Excellence (NCCoE)[10] is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.

Through consortia under Cooperative Research and Development Agreements, including private sector collaborators—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. Working with communities of interest, the NCCoE has produced practical cybersecurity solutions that benefit large and small businesses, and third-party service providers in diverse sectors including healthcare, energy, financial services, retail, and manufacturing.

The NCCoE has many published practice guides, on-going projects exploring solutions, and upcoming projects exploring new challenges and building communities of interest that all directly support the cybersecurity of the Internet of Things. Recently, the *Mitigating IoT-Based Distributed Denial of Service (DDoS)* project published practice guides demonstrating how use

[9] https://csrc.nist.gov/Projects/Lightweight-Cryptography
[10] https://www.nccoe.nist.gov/

of the Manufacturer Usage Description specifications could be used to reduce the ability of IoT devices from participating in a DDoS attack.

In the healthcare space, the NCCoE previously published practice guides demonstrating an example solution for *Securing Wireless Infusion Pumps* that applies security controls to the pump's environment to create a defense-in-depth approach for protecting infusion pumps and their surrounding systems against various risk factors. Additionally, as many IoT devices rely on cloud services, the example solutions identified in the NCCoE's *Trusted Cloud* practice guides help IoT environments by providing assurance that business processes in the cloud are running on trusted hardware and in trusted environments while also increasing the protection of data as it processed and transmitted.

In addition to these published example solutions, the NCCoE has several upcoming projects and ideas that may address cybersecurity challenges seen in many IoT devices and environments. The *Securing Picture Archiving and Communication System* project is currently exploring solutions that allow healthcare delivery organizations to apply cybersecurity controls to their imaging systems that provide significant integrity, availability, and confidentiality assurances since this data is about patients and used by doctors for determining health condition, follow-on visits, patient care, and other actions. Also, in the healthcare space, the *Securing Telehealth Remote Patient Monitoring Ecosystem* will explore cybersecurity controls to protect remote patient monitoring platforms, which commonly incorporate home medical devices that are part of the IoT. Home use of IoT is not limited to medical purposes. The NCCoE has initiated a *Consumer Home IoT Security* project, which will explore how specific devices, platforms, and/or software may provide additional cybersecurity to home IoT networks.

Conclusion

Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in information technology. IT products and services need to provide sufficient levels of cybersecurity and resilience. The timely availability of international cybersecurity standards is a dynamic and critical component for the cybersecurity and resilience of all information and communications systems and supporting infrastructures.

The Internet of Things is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. Many organizations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may affect cybersecurity and privacy risks differently than conventional information technology devices do.

The NIST's Cybersecurity for the Internet of Things program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

NIST is proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the robust collaborations enjoyed with its federal government partners, private sector collaborators, and international colleagues.

Thank you for the opportunity to present NIST’s activities on securing Internet of Things. I will be pleased to answer any questions you may have.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $160 million, nearly 400 employees, and approximately 300 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.