The Internet of Things

Activities in the U.S. Government

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

CREATE EBOOKS IN 30 SECONDS WITHOUT WRITING A WORD

CLICK HERE TO SEE HOW

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits.

The growth of network-connected devices, systems and services comprising the IoT provides efficiencies and personalization of experience that is attractive to both manufacturers and consumers. Network connected devices, systems, and services are also increasingly integrated with and relied upon by our Nation's critical infrastructure, leading to a national dependency. The characteristics of the IoT ecosystem also result in multiple opportunities for malicious actors to manipulate the flow of information to and from network connected devices. Important processes that once were performed manually, and therefore enjoyed a measure of immunity against malicious cyber activity, are growing more vulnerable. Recent large scale distributed denial of service attacks foreshadow increasing in the US and elsewhere.

In 2008, the U.S. National Intelligence Council warned that the Internet of Things (IoT) would be a disruptive technology by 2025. The Council said that individuals, businesses, and governments were unprepared for a possible future when network interfaces reside in everyday things. Almost six years later, this warning remains valid, though it now seems certain that the IoT will be disruptive far sooner than 2025—if it is not so already. More recently in January 2014, the Director of National Intelligence (DNI) stated that "[t]he complexity and nature of these systems means that security and safety assurance are not guaranteed and that threat actors can easily cause security and/or safety problems in these systems."

Several statistics validate the Government's concerns: the number of Internet-connected devices first outnumbered the human population in 2008, and that number continues to grow faster than the human population. By 2013, there were as many as 13 billion Internet-connected devices, and projections indicate that this will grow to 50 billion or more by 2020, generating global revenues of greater than $8 trillion by 2020. Many of these systems are visible to any user, including malicious actors, as search engines are already crawling the Internet indexing and identifying connected devices.

The IoT is the latest development in the decades-old revolution in communications, networking, processing power, miniaturization, and application innovation and has radically altered communications, networks, and sensors. The IoT is a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a

variety of information or control devices in the physical world. However, the IoT differs from previous technological advances because it has surpassed the confines of computer networks and is connecting directly to the physical world. Just as modern communications have fundamentally altered national security and emergency preparedness (NS/EP), the IoT has had a similar transformative impact. Throughout the communications revolution, a plethora of existing and new technologies have led to astonishing improvements in the efficiency and effectiveness of Government and private sector operations and capabilities; yet the IoT differs in the pace, scale, and breadth of deployment of interconnected devices, which has resulted in immense benefits to individuals and organizations. Despite the benefits, the IoT is accompanied by risk associated with increased dependencies, expanded number of devices, and associated interconnections that will create a large attack surface with numerous potential threat vectors.

The increased attack surface and our Nation's dependence on these new systems, either directly or through the critical infrastructure systems in which they are embedded, has made the IoT and new systems natural targets for criminals, terrorists, and nation states that wish to exploit them. These dependencies will continue to increase as the IoT permeates all sectors of the economy and all aspects of people's lives.

While all users have to cope with this expanded attack surface, IoT applications in the NS/EP domain must be hardened against the potential risks. As IoT manufacturers and vendors Interests Out to 2025.

Source: https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf

The Federal Trade Commission IOT Report

January 27, 2015

The Internet of Things is already impacting the daily lives of millions of Americans through the adoption of health and fitness monitors, home security devices, connected cars and household appliances, among other applications. Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits. However, the FTC report also notes that connected devices raise numerous privacy and security concerns that could undermine consumer confidence.

"The only way for the Internet of Things to reach its full potential for innovation is with the trust of American consumers," said FTC Chairwoman Edith Ramirez. "We believe that by adopting the best practices we've laid out, businesses will be better able to provide consumers the protections they want and allow the benefits of the Internet of Things to be fully realized."

The Internet of Things universe is expanding quickly, and there are now over 25 billion connected devices in use worldwide, with that number set to rise significantly as consumer goods companies, auto manufacturers, healthcare providers, and other businesses continue to invest in connected devices, according to data cited in the report.

The report is partly based on input from leading technologists and academics, industry representatives, consumer advocates and others who participated in the FTC's Internet of Things workshop held in Washington D.C. on Nov. 19, 2013, as well as those who submitted public comments to the Commission. Staff defined the Internet of Things as devices or sensors – other than computers, smartphones, or tablets – that connect, store or transmit information with or between each other via the Internet. The scope of the report is limited to IoT devices that are sold to or used by consumers.

Security was one of the main topics addressed at the workshop and in the comments, particularly due to the highly networked nature of the devices. The report includes the following recommendations for companies developing Internet of Things devices:

- build security into devices at the outset, rather than as an afterthought in the design process;
- train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;
- ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
- when a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;
- consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;

- monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.

Commission staff also recommend that companies consider data minimization – that is, limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely. The report notes that data minimization addresses two key privacy risks: first, the risk that a company with a large store of consumer data will become a more enticing target for data thieves or hackers, and second, that consumer data will be used in ways contrary to consumers' expectations.

The report takes a flexible approach to data minimization. Under the recommendations, companies can choose to collect no data, data limited to the categories required to provide the service offered by the device, less sensitive data; or choose to de-identify the data collected.

FTC staff also recommends that companies notify consumers and give them choices about how their information will be used, particularly when the data collection is beyond consumers' reasonable expectations. It acknowledges that there is no one-size-fits-all approach to how that notice must be given to consumers, particularly since some Internet of Things devices may have no consumer interface. FTC staff identifies several innovative ways that companies could provide notice and choice to consumers.

Regarding legislation, staff concurs with many stakeholders that any Internet of Things-specific legislation would be premature at this point in time given the rapidly evolving nature of the technology. The report, however, reiterates the Commission's repeated call for strong data security and breach notification legislation. Staff also reiterates the Commission's call from its 2012 Privacy Report for broad-based privacy legislation that is both flexible and technology-neutral, though Commissioner Ohlhausen did not concur in this portion of the report.

The FTC has a range of tools currently available to protect American consumers' privacy related to the Internet of Things, including enforcement actions under laws such as the FTC Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act; developing consumer education and business guidance; participation in multi-stakeholder efforts; and advocacy to other agencies at the federal, state and local level.

In addition to the report, the FTC also released a new publication for businesses containing advice about how to build security into products connected to the Internet of Things. "Careful Connections: Building Security in the Internet of Things" encourages companies to implement a risk-based approach and take advantage of best practices developed by security experts, such as using strong encryption and proper authentication.

The Commission vote to issue the staff report was 4-1, with Commissioner Wright voting no. Commissioner Ohlhausen issued a concurring statement, and Commissioner Wright issued a dissenting statement.

Source: https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

Securing the Internet of Things Security Tip (ST17-001)

Original release date: November 16, 2017

The Internet of Things is becoming an important part of everyday life. Being aware of the associated risks is a key part of keeping your information and devices secure. The Internet of Things refers to any object or device that sends and receives data automatically through the Internet. This rapidly expanding set of "things" includes tags (also known as labels or chips that automatically track objects), sensors, and devices that interact with people and share information machine to machine.

Why Should We Care?

Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to other machines and trigger additional actions. Examples include devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; control systems that deliver water and power to your workplace; and other tools that track your eating, sleeping, and exercise habits.

This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed.

What Are the Risks?

Though many security and resilience risks are not new, the scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones. Attackers take advantage of this scale to infect large segments of devices at a time, allowing them access to the data on those devices or to, as part of a botnet, attack other computers or devices for malicious intent. See Cybersecurity for Electronic Devices, Understanding Hidden Threats: Rootkits and Botnets, and Understanding Denial-of-Service Attacks for more information.

How Do I Improve the Security of Internet-Enabled Devices?

Without a doubt, the Internet of Things makes our lives easier and has many benefits; but we can only reap these benefits if our Internet-enabled devices are secure and trusted. The following are important steps you should consider to make your Internet of Things more secure.

Evaluate your security settings. Most devices offer a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of software, or if you become aware

of something that might affect your device, reevaluate your settings to make sure they are still appropriate. See Good Security Habits for more information.

Ensure you have up-to-date software. When manufacturers become aware of vulnerabilities in their products, they often issue patches to fix the problem. Patches are software updates that fix a particular issue or vulnerability within your device's software. Make sure to apply relevant patches as soon as possible to protect your devices. See Understanding Patches for more information.

Connect carefully. Once your device is connected to the Internet, it's also connected to millions of other computers, which could allow attackers access to your device. Consider whether continuous connectivity to the Internet is needed. See Securing Your Home Network for more information.

Use strong passwords. Passwords are a common form of authentication and are often the only barrier between you and your personal information. Some Internet-enabled devices are configured with default passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Choose strong passwords to help secure your device. See Choosing and Protecting Passwords for more information.

The following organizations offer additional information about this topic:

Online Trust Alliance: https://otalliance.org/smarthome
Open Web Application Security Project (OWASP):
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
https://www.owasp.org/index.php/IoT_Security_Guidance
Atlantic Council: http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
Networks of 'Things' (NIST Special Publication 800-183):
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
Department of Homeland Security: https://www.dhs.gov/securingtheIoT
Stop.Think.Connect.: https://www.dhs.gov/stopthinkconnect

Authors: Stop.Think.Connect. and National Cybersecurity and Communications Integration Center (NCCIC)

Source: https://www.us-cert.gov/ncas/tips/ST17-001

Strategic Principles for Securing the Internet Of Things (IoT) Version 1.0

U.S. Department of Homeland Security

November 15, 2016

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IoT is almost without limit.

Prioritizing IoT Security

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security. In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure. In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the need for urgent action. IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally.... there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.

The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely-adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

- Incorporate Security at the Design Phase
- Advance Security Updates and Vulnerability Management
- Build on Proven Security Practices
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

As with all cyber security efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security. Specifically, these principles are designed for:

- IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
- IoT manufacturers to improve security for both consumer devices and vendor managed devices;

- Service providers, that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
- Industrial and business-level consumers (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.

There is, however, no one-size -fits -all solution for mitigating IoT security risks. Not all of the practices listed below will be equally relevant across the diversity of IoT devices. These principles are intended to be adapted and applied through a risk-based approach that takes into account relevant business contexts, as well as the particular threats and consequences that may result from incidents involving a network-connected device, system, or service.

Incorporate Security at the Design Phase

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed.

By focusing on security as a feature of network-connected devices, manufacturers and service providers also have the opportunity for market differentiation. The practices below are some of the most effective ways to account for security in the earliest phases of design, development, and production.

What are the potential impacts of not building security in during design? Failing to design and implement adequate security measures could be damaging to the manufacturer in terms of financial costs, reputational costs, or product recall costs. While there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.

Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable. Build the device using the most recent operating system that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Use hardware that incorporates security features to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.

Promote Security Updates and Vulnerability Management Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies. In designing these strategies, developers should consider the implications of a device failure, the durability of the associated product, and the anticipated cost of repair. In the absence of the ability to deploy security updates, manufacturers may be faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

FOCUS ON: NTIA Multi-Stakeholder Process on Patching and Updating The National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the "Internet of Things Upgradability and Patching" to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption.

SUGGESTED PRACTICES:

Consider ways in which to secure the device over network connections or through automated means. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities. Consider coordinating software updates among third-party vendors to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

Develop automated mechanisms for addressing vulnerabilities. In the software engineering space, for example, there are mechanisms for ingesting information from critical vulnerability reports sourced from the research and hacker communities in real time. This allows developers to address those vulnerabilities in the software design, and respond when appropriate. Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities.

A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT),

Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.

Develop an end-of-life strategy for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.

Build on Recognized Security Practices Many tested practices used in traditional IT and network security can be applied to IoT . These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices. Start with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

Refer to relevant Sector-Specific Guidance, where it exists, as a starting point from which to consider security practices. Some federal agencies address security practices for the unique sectors that they regulate. For example, the National Highway Traffic Safety Administration (NHTSA) recently released guidance on Cybersecurity Best Practices for Modern Vehicles that address some of the unique risks posed by autonomous or semi-autonomous vehicles. Similarly, the Food and Drug Administration released draft guidance on Postmarket Management of Cybersecurity in Medical Devices.

Practice defense in depth. Developers and manufacturers should employ a holistic approach to security that includes layered defenses against cybersecurity threats, including user-level tools as potential entry points for malicious actors. This is especially valuable if patching or updating mechanisms are not available or insufficient to address a specific vulnerability. Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.

The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), as well as multi-state and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

Prioritize SecurityMeasures According to Potential Impact Risk models differ substantially across the IoT ecosystem. For example, industrial consumers (such as nuclear reactor owners and operators) will have different considerations than a retail consumer. The consequences of a security failure across different customers will also vary significantly.

Focusing on the potential consequences of disruption, breach, or malicious activity across the consumer spectrum is therefore critical in determining where particular security efforts should be directed, and who is best able to mitigate significant consequences.

Should IoT security measures focus on the IoT device? Since the purpose of all IoT processes is to take in information at a physical point and motivate a decision based on that information (som etimes with physical consequences), security measures can focus on one or more parts of the IoT process.

SUGGESTED PRACTICES:

Know a device's intended use and environment, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary. Perform a "red-teaming" exercise, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures.

Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Reliance on the many low -cost, easily accessible software and hardware solutions used in IoT can make this challenging. Because developers and manufactures rely on outside sources for low -cost, easily accessible software and hardware solutions, they may not be able to accurately assess the level of security built into component parts when developing and deploying network-connected devices. Furthermore, since many IoT devices leverage open source packages, developers and manufacturers many not be able to identify the sources of these component parts. Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers, and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

SUGGESTED PRACTICES:

Conduct end-to-end risk assessments that account for both internal and third party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.

Consider creating a publicly disclosed mechanism for using vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

Consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues.

A list can serve as valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption. IoT consumers can also help contain the potential threats posed by network connectivity by connecting carefully and deliberately, and weighing the risks of a potential breach or failure of an IoT device against the costs of limiting connectivity to the Internet.

In the current networked environment, it is likely that any given IoT device may be disrupted during its lifecycle. IoT developers, manufacturers, and consumers should consider how a disruption will impact the IoT device's primary function and business operations following the disruption.

Does every networked device need continuous, automated connection to the Internet? In 2015, the Federal Trade Commission published a guide called "Start with Security: A Guide for Businesses" to help them determine this very question. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device – and systems; for example, nuclear reactors, where a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.

SUGGESTED PRACTICES:

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions.

Make intentional connections. There are instances when it is in the consumer's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://ics-cert.us-cert.gov/recommended_practices.

Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.

Source:
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Draft Interagency Report, NISTIR 8200, Summarizes International Efforts to Standardize Internet of Things Cybersecurity

February 14, 2018

The Interagency International Cybersecurity Standardization Working Group (IICS WG) was established in December 2015 by the National Security Council's Cyber Interagency Policy Committee. The purpose of the IICS WG is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization.

The IICS WG has developed this report, Draft NIST Interagency Report (NISTIR) 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT). The intended audience is both the government and the public. The purpose is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services.

This draft report:

provides a functional description for IoT (Section 4);

describes several IoT applications that are representative examples of IoT (Section 5);

summarizes the cybersecurity core areas and provides examples of relevant standards (Section 6);

describes IoT cybersecurity objectives, risks, and threats (Section 7);

provides an analysis of the standards landscape for IoT cybersecurity (Sections 8 and 9); and

maps IoT relevant cybersecurity standards to cybersecurity core areas (Appendix D).

The Interagency International Cybersecurity Standardization Working Group (IICS WG) was established in December 2015 by the National Security Council’s Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization. Effective U.S. government participation involves coordinating across the U.S. government and working with the U.S. private sector. There is a much greater reliance in the U.S. on the private sector for standards development than in many other countries. Companies and industry groups, academic institutions, professional societies, consumer groups, and other interested parties are major contributors. Further, the many Standards Developing Organizations (SDOs) who provide the infrastructure for the standards development are overwhelmingly private sector organizations. On April 25, 2107, the IICS WG

established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. This Report is intended for use by the IICS WG member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT. Other organizations may also find this useful in their planning.

This draft report is based upon the information available to the participating agencies. Comments are now being solicited to augment that information, especially on the information about the state of cybersecurity standardization for IoT that is found in Sections 8, 9, 10, and Annex D.

Source: https://csrc.nist.gov/News/2018/Report-International-IoT-Cybersecurity-Standards

Executive Summary

The Interagency International Cyber Security Working Group (IICS WG) was created in response to recommendations from NISTIR 8074 Volume 1 [1]. The IICS WG coordinates on major issues in international cybersecurity standardization. The IICS WG established an Internet of Things (IoT) Task Group to develop this Report on the status of international cybersecurity standards that are relevant to IoT.

The Internet of Things (IoT) consists of network connected devices, systems, and resulting services. The adoption of IoT and its applications is rapidly growing and the ensuing opportunities and benefits are significant. However, to reap the substantial benefits and to minimize the potentially significant risks, IoT security and resiliency are critical.

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 intended audience is both the government and public. The purpose is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of such standards in IoT components, systems, and services.

The Report relies upon terms and definitions that are defined in Annex A

– Terms and Definitions of NISTIR 8074 Volume 2

Rather than attempting to define “IoT,” employs a functional description to establish a common understanding of IoT components, systems and applications for which the standards could be relevant. This analysis starts with a functional description of IoT components, which are the basic building blocks of IoT systems.

To gain insight on the present state of IoT cybersecurity standardization, five IoT technology application areas are described. These application areas are not exhaustive but are sufficiently representative to use in an analysis of the present state of IoT cybersecurity standardization.

- Connected vehicle (CV) IoT enables vehicles, roads, and other infrastructure to communicate and share vital transportation information.
- Consumer IoT consists of IoT applications in the residence 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.

Building upon NISTIR 8074 Volume 2, this Report describes eleven cybersecurity core areas and provides examples of relevant standards. IoT cybersecurity objectives, risks, and threats are then analyzed for IoT applications in general and for each of the five 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. As such, the priority of the individual's cybersecurity objectives may be prioritized very differently, depending on the application. The proliferation and increased ubiquity of IoT components and systems are likely to heighten the risks they present.

Standards-based cybersecurity risk management will continue to be a major factor in the trustworthiness of IoT applications. Through analysis of the application areas, cybersecurity for IoT is unique and will require tailoring of existing standards, as well as, creation of new standards to address pop-up network connections, shared system components, the ability to change physical aspects of the environment, and related connections to safety.

With this foundational basis, this Report provides an analysis of the standards landscape for IoT cybersecurity. The basis for this analysis is the information in Annex D, which maps IoT relevant cybersecurity standards to the eleven cybersecurity core areas. The annotated listings in Annex D are not exhaustive but do represent an extensive effort to identify presently relevant IoT cybersecurity standards. The market impacts of existing standards are noted and possible gaps in standards identified. While the Annex D listing is a onetime snapshot, Annex D should prove useful as a point of departure for maintaining awareness of the evolving standards landscape. A summary on the status of cybersecurity standardization for the five specific examples of IoT applications is provided in Table 4:

Status of Cybersecurity Standardization for Several IoT Applications.

The Report's conclusions focus upon the issue of standards gaps and the effective use of existing standards. For identified priorities, agencies should work with industry to initiate new standards projects in Standards Developing Organizations (SDOs) to close such gaps. In accordance with USG policy, agencies should participate in the development of IoT cybersecurity standards and, based upon each agency's mission, agencies should cite appropriate standards in their procurements. Also, in accordance with USG policy, agencies should work with industry to support the development of appropriate conformity assessment schemes to the requirements in such standards.

Source: https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

Testimony of Assistant Secretary Strickling before the Senate Committee on Commerce, Science, and Transportation on “Preserving the Multistakeholder Model of Internet Governance”

February 25, 2015

Testimony of The Honorable Lawrence E. Strickling Assistant Secretary for Communications and Information National Telecommunications and Information Administration United States Department of Commerce

Before the Committee on Commerce, Science, and Transportation United States Senate Hearing entitled:

"Preserving the Multistakeholder Model of Internet Governance"

Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for this opportunity to testify on behalf of the National Telecommunications and Information Administration (NTIA) regarding NTIA's role in the Internet's domain name system and the transition of NTIA's stewardship over certain technical functions related to the Internet domain name system to the global multistakeholder community. I am pleased to appear before you to update you on the current status of the transition planning process as the global Internet community works to develop a transition proposal that will ensure the stability, security, and openness of the Internet.

I. Background

The Domain Name System (DNS) is a critical component of the Internet infrastructure. It allows users to identify websites, mail servers, and other Internet destinations using easy-to-understand names (e.g., www.ntia.doc.gov) rather than the numeric network addresses (e.g., 170.110.225.163) necessary to retrieve information on the Internet. In this way, it functions similar to an "address book" for the Internet.

On July 1, 1997, President Clinton issued an Executive Memorandum directing the Secretary of Commerce to privatize the Internet DNS in a manner that increases competition and facilitates international participation in its management.[1] In June 1998, following a public comment process, NTIA issued a statement of policy on the privatization of the Internet DNS, known as the DNS White Paper.[2] The White Paper concluded that the core functions relevant to the

DNS should be performed under private sector management to promote the development of robust competition and facilitate global participation in Internet management.

NTIA recognized that the Internet has succeeded in great measure because it is a decentralized system that encourages innovation and maximizes individual freedom. Where possible, market mechanisms that support competition and consumer choice should drive the management of the Internet because they lower costs, promote innovation, encourage diversity, and enhance user choice and satisfaction. Moreover, a private sector coordinating process would be more flexible than a government process and more likely to move rapidly enough to meet the changing needs of the Internet and of Internet users.

To accomplish these policy objectives, NTIA stated that it was prepared to enter into an agreement with a new not-for-profit corporation formed by private sector Internet stakeholders to coordinate and manage policy for the Internet DNS. Private sector interests formed NewCo for this purpose, which was subsequently re-named the Internet Corporation for Assigned Names and Numbers (ICANN). In the fall of 1998, NTIA entered into a Memorandum of Understanding (MOU) with ICANN to transition technical DNS coordination and management functions to the private sector.

The MOU did not simply turn over management of the DNS to ICANN. Rather, the MOU outlined a process to design, develop, and test mechanisms, methods, and procedures to ensure that the private sector had the capability and resources to assume important responsibilities related to the technical coordination and management of the DNS. The MOU evolved through several iterations and revisions as ICANN tested these principles, learned valuable lessons, and matured as an organization.

II. Internet Assigned Numbers Authority (IANA) Functions

In 1998, NTIA announced its intent to ensure the continued secure and stable performance of the IANA functions until the transition was complete. In 2000, NTIA entered into a sole-source, no-cost-to-the-government contract with ICANN, designating it to perform these functions. NTIA and ICANN have subsequently entered into contracts for the performance of the IANA functions in 2001, 2003, and 2006. On July 2, 2012, NTIA awarded ICANN the current IANA functions contract after conducting a full and open competitive procurement process. The base period of performance for this contract is October 1, 2012, to September 30, 2015. The contract also provides for two option periods of two years each; however, the parties have discretion to extend

the contract for a shorter period than two years upon mutual agreement. If no action is taken, the contract will automatically expire on September 30 of this year.

The IANA functions are a set of interdependent technical functions that enable the continued efficient operation of the Internet. The IANA functions include: (1) the coordination of the assignment of technical Internet protocol parameters; (2) the administration of certain responsibilities associated with DNS root zone management; (3) the allocation of Internet numbering resources; and (4) other services related to the management of the .ARPA and .INT top-level domains (TLDs).

As the IANA functions operator, ICANN performs administrative responsibilities associated with the registries related to the three primary IANA functions. First, ICANN is the registry for the protocol parameters, as defined by the Internet Engineering Task Force (IETF).[3] Second, ICANN coordinates allocations of IP (Internet Protocol) and AS (Autonomous System) numbers to the Regional Internet Registries (RIRs).[4] Third, ICANN processes root zone file change requests for TLDs and makes publicly available a Root Zone WHOIS database with current and verified contact information for all TLD registry operators. In all three cases, ICANN, as the IANA functions operator, applies the policies developed by the customers of the IANA functions. The ICANN Board does not have authority to make policy decisions or changes on its own.

NTIA's responsibilities under the IANA functions contract are limited and clerical in nature. For example, NTIA does not have an operational role in the management of Internet numbering resources, Internet protocol parameters, the .ARPA TLD, or .INT TLD. In the root zone management function, NTIA verifies that ICANN has followed the policies and procedures established by the community when processing change requests, then authorizes the implementation of those changes. NTIA's role in root zone management does not involve the exercise of discretion or judgment with respect to such change requests.[5] NTIA does not have a similar role in the management of Internet numbering resources, Internet protocol parameters, the .ARPA TLD, or .INT TLD.

From the inception of ICANN, the U.S. Government and Internet stakeholders envisioned that the U. S. Government's role in the IANA functions would be temporary. The DNS White Paper stated that "agreement must be reached between the U.S. Government and the new corporation (ICANN) relating to the transfer of the functions currently performed by IANA."[6]

NTIA has fulfilled this temporary role not because of any statutory or legal responsibility, but as a temporary measure at the request of the President. Indeed, Congress never designated NTIA or any other specific agency responsibility for managing the Internet DNS. Thus, NTIA has no legal or statutory responsibility to manage the DNS. Just as Federal agencies can enter into contracts they need to fulfill their missions without specific legislative authority, Federal agencies can discontinue obtaining such services when they no longer need them. As NTIA made clear at the time of its Statement of Policy, it intended only to procure the IANA functions services until such time as the transition to private sector management of the Internet DNS was complete.

III. Affirmation of Commitments

Since the formation of ICANN, NTIA has worked diligently with the global Internet community to improve ICANN's accountability and transparency to the community of stakeholders it serves. In 2009, NTIA and ICANN entered into the Affirmation of Commitments (Affirmation).[7] The Affirmation signified a critical step in the transition to a multistakeholder, private sector-led model for DNS technical coordination, while also establishing an accountability framework of ongoing multistakeholder reviews of ICANN's performance. Key elements of the Affirmation include: an endorsement of the multistakeholder, private sector-led model; a commitment by ICANN to act in the interests of global Internet users (or public interest); and the establishment of mechanisms and timelines for continuing reviews of ICANN's execution of core tasks. The four subjects of the ongoing Affirmation Reviews are: ensuring accountability, transparency, and the interests of global Internet users; preserving the security, stability, and resiliency of the Internet DNS; promoting competition, consumer trust, and consumer choice in connection with any implementation of generic Top Level Domains (gTLDs); and meeting the needs of law enforcement and consumer protection in connection with WHOIS implementation and recognizing national laws. The success of the framework established by the Affirmation depends upon the full participation of stakeholders in reviewing ICANN's performance.

ICANN has made significant progress in fulfilling the commitments established by the Affirmation. To date, two iterations of the Accountability and Transparency Review Team (ATRT) have occurred, in 2010 and 2013. The reports of these teams, on which NTIA actively has participated with a broad array of international stakeholders from industry, civil society, the Internet technical community, and other governments, have served as a key accountability tool for ICANN - evaluating progress and recommending improvements. Over time, ICANN has improved its performance by implementing key recommendations from the ATRT.

Throughout the various iterations of NTIA's relationship with ICANN, NTIA has played no role in the internal governance or day-to-day operations of ICANN. NTIA has never had the contractual authority to exercise traditional regulatory oversight over ICANN.

IV. Final Steps in the Privatization of the DNS

The multistakeholder model of Internet governance is the best mechanism for maintaining an open, resilient, and secure Internet because, among other things, it is informed by a broad foundation of interested parties and it is adaptable to innovation and changing conditions. This model includes all parties - including businesses, technical experts, civil society, and governments - arriving at consensus through a bottom-up process regarding policies affecting the underlying functioning of the Internet domain name system.

ICANN and several other technical organizations embrace this model and exemplify what is possible when all stakeholders are able to participate. Specifically, within ICANN's structure, governments work in partnership with businesses, organizations, and individuals to provide public policy input on deliberations related to ICANN's mission of technical coordination, and provide advice directly to the ICANN Board. ICANN holds meetings approximately three times a year, at which global stakeholders meet to develop policies that ensure the Internet's ongoing security and stability. ICANN policy development originates in the three Supporting Organizations (SOs), which work with Advisory Committees composed of governments, individual user organizations, and technical communities in the policy development process. Over one hundred governments, including the United States, and observers from more than 30 international organizations directly advise the ICANN Board of Directors via the Governmental Advisory Committee (GAC).[8]

The 112th U.S. Congress affirmed its support for the multistakeholder model in unanimous resolutions to "preserve and advance the successful multi-stakeholder model that governs the Internet."[9] More recently, a bipartisan group of Congressional leaders reiterated this position in stating that "[t]he multi-stakeholder model for Internet governance must prevail for more countries around the world to realize the transformative benefits of Internet connectivity."[10] I am also pleased to note the recent unanimous passage of S. Res. 71, which stated that "the United States remains committed to the multistakeholder model of Internet governance" and that "the [IANA] transition process demonstrates that the United States supports and is committed to the multistakeholder model of Internet governance."[11]

Demonstrating its commitment to the multistakeholder approach, on March 14, 2014, NTIA announced its intent to complete the privatization of the domain name system first outlined in 1998. NTIA called upon ICANN to convene a multistakeholder process to develop the transition plan.[12] While looking to stakeholders and those most directly served by the IANA functions to work through the technical details, NTIA established a clear framework to guide the discussion. Specifically, NTIA communicated to ICANN that the transition proposal must have broad community support and address four principles.

First, the transition proposal must support and enhance the multistakeholder model. Specifically, the process used to develop the proposal should be open, transparent, bottom-up, and garner broad, international stakeholder support. In addition, the proposal should include measures to ensure that changes made to any of the three IANA administered databases are consistent with the publicly documented IANA functions customer and partner accepted procedures, which are developed through the multistakeholder model.

Second, the transition proposal must maintain the security, stability, and resiliency of the Internet DNS. For example, the decentralized distributed authority structure of the DNS needs to be preserved so as to avoid single points of failure, manipulation, or capture. In addition, integrity, transparency, and accountability in performing the functions must be preserved. The IANA services also need to be resistant to attacks and data corruption, be able to fully recover from degradation, if it occurs, and be performed in a stable legal environment.

Third, the transition proposal must meet the needs and expectations of the global customers and partners of the IANA services. For example, mechanisms for the adherence to and development of customer service levels, including timeliness and reliability, should be clear, as should processes for transparency, accountability, and auditability. Consistent with the current system, the separation of policy development and operational activities should continue.

Fourth, the transition proposal must maintain the openness of the Internet. The neutral and judgment-free administration of the technical DNS and IANA functions has created an environment in which the technical architecture has not been used to interfere with the exercise of free expression or the free flow of information. Any transition of the NTIA role must maintain this neutral and judgment-free administration, thereby maintaining the global interoperability of the Internet.

In addition, NTIA explicitly stated that it would not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution.

While the current IANA functions contract expires on September 30, 2015, the contract can be extended for up to four years. Before any transition takes place, the businesses, civil society, and technical experts of the Internet must present a plan that has broad multistakeholder support and reflects the four key principles NTIA outlined in the announcement.

By transitioning its very limited current role in the IANA functions to the global multistakeholder community, the United States is fulfilling objectives outlined more than 17 years ago, demonstrating its commitment to the multistakeholder model, and strengthening the engagement of all stakeholders. For years, countries such as Russia, Iran, and China have opposed the multistakeholder model and sought to increase governmental control over the Internet through bodies such as the International Telecommunication Union (ITU) and the United Nations. The United States and likeminded countries, however, have firmly demonstrated our support for the multistakeholder community, and we continue to advocate for broader worldwide acceptance of and participation in the multistakeholder model to ensure that the Internet remains open and interoperable.

The world has witnessed significant progress in its collective efforts to expand support for multistakeholder Internet governance since the division that surfaced in December 2012 at the ITU World Conference on International Telecommunications (WCIT). We believe this is due in part to the transition and our support for the multistakeholder model. In April 2014, Brazil hosted the successful NetMundial conference at which a wide range of participants supported a statement reaffirming that Internet governance should be built on democratic multistakeholder processes.[13] Following NetMundial, a High-Level Panel headed by the president of Estonia released a report once again affirming the power of multistakeholder policy development. The panel said it "recognizes, fully supports, and adopts the IG [Internet governance] Principles produced in the NetMundial Statement. . . ."[14] In the fall of 2014, nations assembled at the ITU Plenipotentiary Conference in Busan, South Korea, rejected all efforts to expand the ITU's role in DNS issues handled by ICANN.[15]

V. Stakeholder Response

Following the March 2014 announcement, a broad array of Internet stakeholders issued public statements that demonstrate the importance of the transition:

AT&T: "This is an important step in the ongoing evolution of the global Internet. NTIA is to be commended for its historical stewardship, its current thoughtful and pro-active approach, and its global leadership throughout. The U.S. is looking to the future, promoting leadership and ideas from the global multi-stakeholder community, and establishing clear criteria to ensure the stability and security of a remarkably well-functioning system. We expect that other governments and stakeholders will join with the U.S. in committing to this vision."[16]

Microsoft: "The U.S. Department of Commerce National Telecommunications and Information Administration's recent announcement of its intent to transition key Internet domain name functions to the global multi-stakeholder community is a significant and welcome development."[17]

Human Rights Organizations: "[W]e write to express our support for the Department of Commerce's National Telecommunications and Information Administration (NTIA) announcement of its intent to transition key Internet domain name functions to the global multi-stakeholder community...This move would alleviate international pressure on explicit terms, deter government overreach on the issue of Internet governance, and facilitate the exercise of human rights online."[18]

The Internet Association (representing Amazon, Facebook, Google, Netflix, Yahoo!, Twitter, Airbnb, and other Internet economy firms): ". . .we support the recent announcement regarding the National Telecommunications and Information Administration's (NTIA) oversight authority over important technical Internet functions .... For our companies to continue to innovate, to foster development and change, and ultimately to succeed as businesses globally, we need the continuation of the current bottom-up, multi-stakeholder model of Internet governance. However, as the Internet continues to evolve, so too must the models that govern it .... [I]t was always envisaged that this oversight role held by the United States would eventually transition to the private sector. The announcement by NTIA is simply the fulfillment of this vision. . . . For these reasons we encourage you to allow this process to continue toward a successful conclusion."[19]

U.S. Chamber of Commerce: "NTIA has steadfastly opposed a transition to any mechanism that would deviate from the current multi-stakeholder model of Internet governance and should be allowed to take any needed steps to achieve the cautiousness and transparency that we agree is essential for a safe and smooth transition of the technical functions. Any hindering of NTIA's ability to conduct the proper levels of due diligence through the use of currently available resources could result in harm to U.S. businesses and Internet users as a whole."[20]

Verizon: "We applaud NTIA for recognizing the global relevance of the Internet Assigned Numbers Authority (IANA) functions and the current maturity of multi-stakeholder frameworks."[21]

Ambassador David Gross, former United States Coordinator for International Communications and Information Policy (George W. Bush Administration): "We believe that NTIA's decision to initiate a process leading to the possible transition of the IANA functions contract to a multi-stakeholder entity is a critical step.... By allowing for the careful transition of the IANA to a bottom-up multi-stakeholder entity, the United States has affirmed its commitment to the multi-stakeholder model."[22]

Cisco: "This is a significant milestone in the transition of Internet governance to a global multi-stakeholder model, and Cisco welcomes this development. We applaud the NTIA for seeking to complete the final phase of the privatization of DNS management, as outlined by the U.S. Government in 1997. Cisco has long supported an open and innovative multi-stakeholder Internet governance process and this next step in its evolution."[23]

USTelecom: "We applaud NTIA for its responsible stewardship of the Internet's Domain Name System (DNS) over the years and are supportive of its proposal to transition the Internet Assigned Numbers Authority (IANA) functions to the global multi-stakeholder community."[24]

Center for Democracy and Technology: "CDT believes that this transition is an important part of the evolution and strengthening of multi-stakeholder governance of the Internet."[25]

Internet Technical Organizations: "The leaders of the Internet technical organizations responsible for coordination of the Internet infrastructure (IETF, IAB, RIRs, ccTLD ROs, ICANN, ISOC, and W3C), welcome the US Government's announcement of the suggested changes related to the IANA functions contract."[26]

Computer and Communications Industry Association: "The technology industry welcomes the news that the U.S. Commerce Department intends to complete the transition of relinquishing its control over key Internet addressing functions to the global multi-stakeholder community. This was a necessary next step in the evolution of the Internet and supports the current multi-stakeholder model of global Internet governance where all stakeholders concerned with the well being and functioning of the Internet help to shape the policies that make a bright online future for everyone possible."[27]

VI. Status of Multistakeholder Process to Develop Transition Proposal

Since NTIA's March 2014 announcement, interested stakeholders have responded with great energy and participation to develop a transition plan. An IANA Stewardship Transition Coordination Group (ICG), representing more than a dozen Internet stakeholder communities, was established as a convener of the process to develop a transition proposal that will ensure the stability, security, and openness of the Internet. As set forth in its charter, the ICG is "conduct[ing] itself transparently, consult[ing] with a broad range of stakeholders, and ensur[ing] that its proposals support the security and stability of the IANA functions."[28] On September 8, 2014, the ICG issued a Request for Transition Proposals to the multistakeholder community, with a proposal submission deadline of January 15, 2015.[29] The ICG requested one proposal for each of the three primary functions, i.e., the protocol parameters, numbering, and domain name-related functions, to be developed by the communities and parties most directly affected by each of the primary functions. Proposal development has to date been open and multistakeholder in participation.

As of February 2015, two of the three community groups have submitted their draft proposals, including the IETF, which is shepherding the protocol parameter proposal, and the five RIRs, which worked collaboratively in developing a draft numbering proposal. The third group, the ICANN Cross Community Working Group (CWG) on the naming related functions, continues to deliberate on how best to assure effective and accountable oversight of these naming functions in NTIA's absence. Upon receipt of the community proposals, the ICG will then work to develop a single consolidated proposal, which will go through various iterations of community review and comment.[30]

On January 27, 2015, I delivered remarks at the State of the Net Conference, where I posed several questions for stakeholders to consider as they continue to develop the naming related proposal, to ensure that it appropriately addresses the principles NTIA established for the transition. I indicated that these questions need to be resolved prior to approval of any transition plan.[31] At the ICANN meeting held in Singapore two weeks ago, I reiterated these remarks and questions. The subsequent community discussions in Singapore give me confidence that the domain name community (through the CWG) is working diligently to develop a proposal that not only considers appropriate accountability, but also what is necessary for the directly affected parties (registry operators) in terms of service levels and processes that preserve and maintain stable DNS root zone management that the community currently enjoys.

ICANN has also launched a parallel process to enhance its accountability to the global Internet community and to strengthen its accountability mechanisms in the absence of a contractual relationship with NTIA.[32] A Cross Community Working Group (CCWG) on Accountability, composed of appointed representatives from ICANN's Supporting Organizations (SOs) and Advisory Committees (ACs) and open to all interested parties as participants, is examining accountability mechanisms regarding the entirety of ICANN operations.[33] The CCWG charter identifies two work streams: the first is to identify accountability measures that need to be in place before the IANA transition; and the second to address accountability measures that should be adopted and implemented by ICANN in the longer term. The CCWG identified four distinct work areas: (1) overview of existing accountability mechanisms; (2) review of public comments filed in response to ICANN's proposed accountability process to categorize them as either Work Stream 1 or Work Stream 2 items; (3) review of accountability issues identified by the CWG; and (4) identification of contingencies or threat scenarios.[34] The CCWG adopted an intensive work plan to address the near-term, IANA-specific measures involving weekly meetings in order to progress its work.[35] While it got off to a slower start than the IANA transition process, the CCWG on Accountability is now making considerable progress, as evident at the ICANN Singapore meeting at which the group conducted numerous productive working sessions and meetings with stakeholders. The CCWG on Accountability is also cooperating and coordinating with the CWG working on the domain names transition proposal. This is a good and constructive development as it allows the CWG to return some of its focus on the domain name related functions and a little less on ICANN accountability. NTIA believes that this accountability process needs to include the "stress testing" of solutions to safeguard against future contingencies such as attempts to influence or take over ICANN functions that are not currently possible with the IANA functions contract in place.

These two multistakeholder processes - the IANA stewardship transition and enhancing ICANN accountability - are directly linked, and NTIA has repeatedly said that both issues must be addressed before any transition takes place. ICANN has indicated that it expects to receive both the ICG transition and CCWG accountability proposals at roughly the same time and that it will forward them promptly and without modification to NTIA.[36]

On the subject of timing, NTIA has not set a deadline for the transition. September 2015 has been a target date because that is when the base period of our contract with ICANN expires. However, we have the flexibility to extend the contract if the community needs more time to develop the best plan possible. It is up to the community to determine a timeline that works best for stakeholders as they develop a proposal that meets NTIA's conditions, but also a proposal that works.

The Internet community is undertaking truly historic work. NTIA is confident that engaging the global Internet community to work out these important issues will strengthen the multistakeholder process and will result in ICANN's becoming even more directly accountable to the customers of the IANA functions and to the broader Internet community.

VII. Next Steps

NTIA is committed to continuing to work closely with the stakeholder community as it develops a proposal that fully achieves the goals NTIA established, as well as continue our overarching commitment to strengthening the current multistakeholder model.

In the year ahead, it will be absolutely critical to the interests of the United States that NTIA continue to monitor the discussions within the multistakeholder community as it develops a transition plan and provide feedback where appropriate. Specifically, NTIA will:

- participate in meetings and discussions with other governments, the global stakeholder community, ICANN, and VeriSign with respect to the transition or planning the transition;
- if appropriate, amend the IANA functions contract to modify the length of contract renewal option periods; and

continue to represent the United States at the GAC meetings held at ICANN meetings and intersessionally throughout the year.

Once the community develops and ICANN submits the consolidated proposal, we will ensure that the March 2014 criteria are fully addressed and that the proposal has been adequately "stress tested" to ensure the continued stability and security of the DNS. The community processes used to develop their proposal might also influence the work NTIA will need to undertake. For example, if the community conducts "stress tests" as well as tests and validates any new process or structures included in the proposal prior to submission, well-documented results may facilitate NTIA's review. This will also give confidence that any process, procedure or structure proposed actually works. In addition, NTIA will review and assess the changes made or proposed to enhance ICANN's accountability required in advance of initiating the transition.

VIII. Conclusion

NTIA is cognizant of and appreciates the directive from Congress to inform the relevant Committees in advance of any decision related to the transition. As the proposal continues to take shape, we will update Congress accordingly. NTIA appreciates interest in this important topic and thanks Congress for its continued support for the multistakeholder model of Internet governance.

References

[1] The White House, "Memorandum for the Heads of Executive Departments and Agencies," (July 1, 1997), available at: http://clinton4.nara.gov/WH/New/Commerce/directive.html.
[2] NTIA, "Statement of Policy, Management of Internet Names and Addresses," (DNS White Paper), 63 Fed. Reg. 31741 (1998), available at: http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses.
[3] The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. See, https://www.ietf.org/ (link is external).
[4] Regional Internet Registries (RIRs) manage, distribute, and register Internet number resources (IPv4 and IPv6 addresses and Autonomous System Numbers) within their respective regions. See, https://www.nro.net/about-the-nro/regional-internet-registries (link is external).
[5] For further information on the NTIA role in root zone management and the IANA functions, see http://www.ntia.doc.gov/other-publication/2014/ntia-s-role-root-zone-management.
[6] DNS White Paper, supra n. 2.
[7] "Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers" (September 30, 2009), available at http://www.ntia.doc.gov/files/ntia/publications/affirmation_of_commitments_2009.pdf

[8] See ICANN, "Beginner's Guide to Participating in ICANN," available at: https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf (link is external). See also, ICANN Groups, available at: https://www.icann.org/resources/pages/groups-2012-02-06-en (link is external).
[9] See H.Con.Res. 127 and S.Con.Res. 50.
[10] Reps. Upton (R-MI), Waxman (D-CA), Royce (R-CA), Engel (D-NY), Re/code, "Protecting the Internet From Government Control" (Dec. 18, 2014), available at: http://recode.net/2014/12/18/protecting-the-internet-from-government-control/.
[11] S. Res. 71 (2015)
[12] "NTIA Announces Intent to Transition Key Internet Domain Name Functions" (Mar. 14, 2014), available at: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.
[13] Michael Daniel, Lawrence E. Strickling, Daniel Sepulveda, Christopher Painter and Scott Busby, "A Major Win for the Open Internet" (Apr. 30, 2014), available at: http://www.ntia.doc.gov/blog/2014/major-win-open-internet.
[14] See Panel on Global Internet Cooperation and Governance Mechanisms, "Towards a Collaborative, Decentralized Internet Governance Ecosystem" (May 2014), available at: http://internetgovernancepanel.org/sites/default/files/ipdf/XPL_ICAN1403_Internet%20Governance%20iPDF_06.pdf (link is external).
[15] U.S. Department of State, "Outcomes from the International Telecommunication Union 2014 Plenipotentiary Conference in Busan, Republic of Korea" (Nov. 10, 2014), available at: http://www.state.gov/r/pa/prs/ps/2014/11/233914.htm.
[16] AT&T Public Policy Blog, "The Continuing Evolution of the Global Internet" (Mar. 14, 2014) (emphasis added), available at: http://www.attpublicpolicy.com/international/the-continuing-evolution-of-the-global-internet/ (link is external).
[17] David Tennenhouse, Microsoft on the Issues, "Microsoft Applauds US NTIA's Transition of Key Internet Domain Name Functions" (Mar. 17, 2014) (emphasis added), available at: https://blogs.microsoft.com/on-the-issues/2014/03/17/microsoft-applauds-us-ntias-transition-of-key-internet-domain-name-functions/#sm.0013wreg145pf9w11vp2eo8zc5o47 (link is external).
[18] Access, Center for Democracy & Technology, Freedom House, Human Rights Watch, The Open Technology Institute at New America Foundation, Public Knowledge, "Congress Should Support U.S. Plan to Alter Administration of Internet" (Apr. 1, 2014) (emphasis added), available at: https://freedomhouse.org/article/congress-should-support-us-plan-alter-administration-internet#.VJmLdl4AFA (link is external).
[19] Michael Beckerman, The Internet Association, Letter to Rep. Hal Rogers and Rep. Nita Lowey (May 8, 2014) (emphasis added), available at: http://internetassociation.org/wp-content/uploads/2014/05/Internet-Association-Letter-on-Future-of-Internet-Governance-Approps-.pdf (link is external).
[20] R. Bruce Josten, U.S. Chamber of Commerce, Letter to U.S. House of Representatives (May 27, 2014) (emphasis added), available at: https://www.uschamber.com/sites/default/files/140527_hr4660_commercejusticescienceappropriationsact2015_house.pdf (link is external).
21] Verizon Policy Blog, "Verizon Supports Global Multi-stakeholder Process for Domain Names" (Mar. 14, 2014), available at: http://publicpolicy.verizon.com/blog/entry/verizon-supports-global-multi-stakeholder-process-for-domain-names (link is external).
[22] Ambassador David A. Gross, Testimony Before the U.S. House Committee on Energy and Commerce (Apr. 2, 2014) (emphasis added), available at: http://docs.house.gov/meetings/IF/IF16/20140402/102044/HHRG-113-IF16-Wstate-GrossD-20140402.pdf.
[23] Robert Pepper, "Cisco Supports U.S. Department of Commerce Decision to Transition Internet Management Functions" (Mar. 15, 2014) (emphasis added), available at: http://blogs.cisco.com/gov/cisco-supports-u-s-department-of-commerce-decision-to-transition-internet-management-functions/ (link is external).
[24] Glenn Reynolds, "USTelecom Statement on Global Internet Transition" (Apr. 2, 2014), was available at: http://www.ustelecom.org/news/press-release/ustelecom-statement-global-internet-transition.

[25] Emma Llanso, Center for Democracy and Technology, "Don't Let Domestic Politics Derail the NTIA Transition" (Apr. 2, 2014) (emphasis added), available at: https://cdt.org/blog/dont-let-domestic-politics-derail-the-ntia-transition/ (link is external).
[26] Internet Society, "Internet Technical Leaders Welcome IANA Globalization Progress" (Mar. 14, 2014), available at: http://www.internetsociety.org/news/internet-technical-leaders-welcome-iana-globalization-progress (link is external).
[27] Computer and Communications Industry Association, "Tech Industry Praises Liberation Of Internet Governance Functions From U.S.G." (Mar. 17, 2014), available at: https://www.ccianet.org/2014/03/tech-industry-praises-liberation-internet-governance-functions-u-s-g/ (link is external).
[28] Charter for the IANA Stewardship Transition Coordination Group (Aug. 27, 2014), available at: https://www.icann.org/en/system/files/files/charter-icg-27aug14-en.pdf (link is external).
[29] IANA Stewardship Transition Coordination Group, "Request for Proposals" (Sept. 8, 2014), available at: https://www.icann.org/en/system/files/files/rfp-iana-stewardship-08sep14-en.pdf (link is external).
[30] See IANA Stewardship Transition Coordination Group, "Process Timeline," (Dec. 2014), available at: https://www.icann.org/en/system/files/files/icg-process-timeline-07jan15-en.pdf (link is external).
[31] Remarks by Lawrence E. Strickling, State of the Net Conference, Washington, DC, (Jan. 27, 2015), available at: http://www.ntia.doc.gov/speechtestimony/2015/remarks-assistant-secretary-strickling-state-net-conference-1272015.
[32] See Enhancing ICANN Accountability, "Opportunity for public dialogue and community feedback" (May 6, 2014), available at: https://www.icann.org/resources/pages/enhancing-accountability-2014-05-06-en (link is external); see also, Enhancing ICANN Accountability: Process and Next Steps (Revised Oct. 10, 2104), available at: https://www.icann.org/resources/pages/process-next-steps-2014-10-10-en (link is external).
[33] See ICANN Announcements, "Proposed Charter for Enhancing ICANN Accountability Cross Community Working Group (CCWG) Submitted for Consideration" (Nov. 5, 2014), available at: https://www.icann.org/news/announcement-2014-11-05-en (link is external).
[34] Cross Community Working Group on Enhancing ICANN Accountability, "Charter" (Last Modified Dec. 11, 2014)(Adopted by 5 organizations), available at: https://community.icann.org/display/acctcrosscomm/Charter (link is external).
[35] See CCWG on Enhancing ICANN Accountability, "Meetings," (last modified Jan. 6, 2015), available at: https://community.icann.org/display/acctcrosscomm/Meetings (link is external).
[36] ICANN, "ICANN 52 Board Statement on ICANN Sending IANA Stewardship Transition and Enhancing ICANN Accountability Proposals to NTIA" (Feb. 12, 2015), available at: https://www.icann.org/news/announcement-3-2015-02-12-en (link is external)
Source: https://www.ntia.doc.gov/speechtestimony/2015/testimony-assistant-secretary-strickling-senate-committee-commerce-science-and-

The GAO Findings on IOT

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD GAO-17-668: Published: Jul 27, 2017. Publicly Released: Jul 27, 2017.

The Internet of Things (IoT) is the set of Internet-capable devices, such as wearable fitness devices and smartphones, that interact with the physical environment and typically contain elements for sensing, communicating, processing, and actuating. Even as the IoT creates many benefits, it is important to acknowledge its emerging security implications. The Department of Defense (DOD) has identified numerous security risks with IoT devices and conducted some assessments that examined such security risks, such as infrastructure-related and intelligence assessments. Risks with IoT devices can generally be divided into risks with the devices themselves and risks with how they are used. For example, risks with the devices include limited encryption and a limited ability to patch or upgrade devices. Risks with how they are used—operational risks—include insider threats and unauthorized communication of information to third parties. DOD has developed IoT threat scenarios involving intelligence collection and the endangerment of senior DOD leadership—scenarios that incorporate IoT security risks (see figure). Although DOD has begun to examine security risks of IoT devices through its infrastructure-related and intelligence assessments, the department has not conducted required assessments related to the security of its operations.

DOD has issued policies and guidance for IoT devices, including personal wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices associated with industrial control systems. However, GAO found that these policies and guidance do not clearly address some security risks relating to IoT devices. First, current DOD policies and guidance are insufficient for certain DOD-acquired IoT devices, such as smart televisions in unsecure areas, and IOT device applications. Secondly, DOD policies and guidance on cybersecurity, operations security, information security, and physical security do not address IoT devices. Lastly, DOD does not have a policy directing its components to implement existing security procedures on industrial control systems—including IoT devices. Updates to DOD policies and guidance would likely enhance the safeguarding and securing of DOD information from IoT devices.

Why GAO Did This Study

Congress included provisions in reports associated with two separate statutes for GAO to assess the IoT-associated security challenges faced by DOD. This report (1) addresses the extent to which DOD has identified and assessed security risks related to IoT devices, (2) assesses the extent to which DOD has developed policies and guidance related to IoT devices, and (3) describes other actions DOD has taken to address security risks related to IoT devices.

GAO reviewed reports and interviewed DOD officials to identify risks and threats of IoT devices faced by DOD. GAO also interviewed DOD officials to identify risk assessments that may address IoT devices and examined their focus areas. GAO further reviewed current policies and guidance DOD uses for IoT devices and interviewed officials to identify any gaps in policies and guidance where security risks may not be addressed.

What GAO Recommends

GAO recommends that DOD (1) conduct operations security surveys that could address IoT security risks or address operations security risks posed by IoT devices through other DOD risk assessments; and (2) review and assess its security policies and guidance affecting IoT devices and identify areas, if any, where new DOD policies may be needed or where guidance should be updated. DOD reviewed a draft of this report and concurs with GAO's recommendations.

Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available GAO-18-71: Published: Nov 16, 2017. Publicly Released: Nov 27, 2017.

What GAO Found

The stakeholders GAO spoke with identified two primary spectrum-related challenges for the internet of things (IoT)—the availability of spectrum and managing interference. Although not considered an immediate concern, Federal Communications Commission (FCC) staff and some stakeholders noted that rapid increases in IoT devices that use large amounts of spectrum—called high-bandwidth devices—could quickly overwhelm networks, as happened with smart phones. Stakeholders and FCC staff also indicated that managing interference is becoming more challenging as the number of IoT and other wireless devices grows, particularly in bands that do not require a spectrum license. The figure below illustrates the uses of radio frequency spectrum, including unlicensed use.

FCC plans for IoT's spectrum needs by broadly tracking spectrum demand and making additional spectrum available as needed. Ensuring sufficient spectrum to support commercial demand is one way FCC pursues its strategic goal of promoting economic growth. FCC has made additional spectrum publicly available at least four times since 2015 by repurposing over 11 gigahertz of spectrum. However, FCC does not track the growth of IoT devices in two areas that pose the greatest risk to IoT's growth—high bandwidth and unlicensed-spectrum devices. In 2014, FCC's Technical Advisory Council (TAC) recommended that FCC monitor high-bandwidth IoT devices and make sufficient unlicensed spectrum available. FCC officials said that FCC monitors spectrum use broadly and makes spectrum available as needed. However, since the process of reallocating spectrum is lengthy, FCC may not have adequate time to take actions to avoid a shortage, possibly hindering IoT's growth and associated economic growth.

Spectrum planners in four leading countries—France, Germany, the Netherlands, and South Korea—have taken steps similar to those taken by the United States in preparation for IoT's expansion, including taking a technology-neutral approach that stakeholders believe encourages innovation. Unlike the United States, officials from two leading countries said they are concerned about spectrum congestion from the growth of IoT devices, but only one is actively monitoring congestion. In addition, three leading countries have developed nationwide low power wide-area networks that use unlicensed spectrum with potential benefits including low costs and low barriers to entry.

Why GAO Did This Study

IoT generally refers to devices (or "things"), such as vehicles and appliances, that use a network to communicate and share data with each other. The increasing popularity of wireless IoT devices that use spectrum has created questions about spectrum needs. GAO was asked to examine issues related to spectrum and IoT. This report discusses, among other things, (1)

spectrum challenges related to IoT, (2) how the federal government plans for IoT's spectrum needs, and (3) how selected leading countries prepare for IoT's spectrum needs.

GAO reviewed documents and interviewed officials from FCC and the National Telecommunications and Information Administration as well as 24 officials from a variety of sectors, including government, commercial, and manufacturing. Stakeholders were selected based on a literature review, among other factors. GAO interviewed government and commercial representatives from four leading countries regarding IoT planning and development and reviewed associated documents. These countries were selected based on criteria that included level of economic development among other criteria.

What GAO Recommends

FCC should track the growth in (1) high-bandwidth IoT devices and (2) IoT devices that rely on unlicensed spectrum. FCC did not believe these actions are necessary but noted that it would ask its TAC to periodically review and report on IoT's growth. GAO continues to believe the recommendations are valid.

Internet of Things: Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise GAO-17-570: Published: Jul 26, 2017. Publicly Released: Jul 26, 2017.

What GAO Found

The internet of things (IoT) generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things." Federal agencies that GAO reviewed are undertaking two kinds of efforts that support IoT in communities:

Broad federal research and oversight of IoT-related technologies and issues: For example, 8 of the 11 agencies GAO reviewed are involved in broad research efforts, often on communication systems—both wired and wireless network systems. In addition, nine agencies have oversight efforts that include providing IoT-related guidance, often on data security and privacy.

More direct efforts to support communities, including funding community IoT projects (see figure) and fostering collaboration among the agencies and communities: For example, DOT recently awarded $40 million in federal funds to a community for a suite of "smart" projects related to improving surface transportation performance, and EPA awarded $40,000 each to two communities to develop strategies for deploying air quality sensors and managing the data collected from them. To foster such collaboration, in July 2016, the White House formed an interagency task force that has developed a draft Smart Cities and Communities Federal Strategic Plan . A final plan will be released in summer of 2017, according to federal officials.

All four of the communities that GAO reviewed are using federal funds in combination with other resources, both financial and non-financial, to plan and deploy IoT projects. For example, one community used the $40 million DOT award to leverage, from community partners, more than $100 million in additional direct and in-kind contributions, such as research or equipment contributions. Communities discussed four main challenges to deploying IoT, including community sectors (e.g., transportation, energy, and public safety) that are siloed and proprietary systems that are not interoperable with one another.

Why GAO Did This Study

Communities are increasingly deploying IoT devices generally with a goal of improving livability, management, service delivery, or competitiveness. GAO was asked to examine federal support for IoT and the use of IoT in communities. This report describes: (1) the kinds of efforts that selected federal agencies have undertaken to support IoT in communities and (2) how selected communities are using federal funds to deploy IoT projects.

GAO reviewed documents and interviewed officials from 11 federal agencies identified as having a key role in supporting IoT in communities, including agencies that support research or community IoT efforts or that have direct authority over IoT issues. GAO interviewed a non-

generalizeable sample of representatives from multiple stakeholder groups in four communities, selected to include a range of community sizes and locations and communities with projects that used federal support. GAO also reviewed relevant literature since 2013 and discussed federal efforts and community challenges with 11 stakeholders from academia and the private sector, selected to reflect a range of perspectives on IoT issues.

GAO requested comments on a draft of this product from 11 federal agencies. Five agencies provided technical comments, which GAO incorporated as appropriate. Six agencies did not provide comments.

Technology Assessment: Internet of Things: Status and implications of an increasingly connected world GAO-17-75: Published: May 15, 2017. Publicly Released: May 15, 2017.

What GAO Found

The Internet of Things (IoT) refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. These "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and respond automatically to improve industrial processes, public services, and the well-being of individual consumers. For example, a "connected" fitness tracker can monitor a user's vital statistics, and store the information on a smartphone. A "smart" tractor can use GPS-based driving guidance to maximize crop planting or harvesting.

Electronic processors and sensors have become smaller and less costly, which makes it easier to equip devices with IoT capabilities. This is fueling the global proliferation of connected devices, allowing new technologies to be embedded in millions of everyday products. The IoT's rapid emergence brings the promise of important new benefits, but also presents potential challenges such as the following:

Information security. The IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet.

Privacy. Smart devices that monitor public spaces may collect information about individuals without their knowledge or consent. For example, fitness trackers link the data they collect to online user accounts, which generally include personally identifiable information, such as names, email addresses, and dates of birth. Such information could be used in ways that the consumer did not anticipate. For example, that data could be sold to companies to target consumers with advertising or to determine insurance rates.

Safety. Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners. For example, in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission.

Standards. IoT devices and systems must be able to communicate easily. Technical standards to enable this communication will need to be developed and implemented effectively.

Economic issues. While impacts such as positive growth for industries that can use the IoT to reduce costs and provide better services to customers are likely, economic disruptions are also

possible, such as reducing the need for certain types of businesses and jobs that rely on individual interventions, including assembly line work or commercial vehicle deliveries.

Why GAO Did This Study

The rapid, global proliferation of IoT devices has generated significant interest. In light of the current and potential effects of the IoT on consumers, businesses, and policy makers, GAO was asked to conduct a technology assessment of the IoT.

This report provides an introduction to the IoT and describes what is known about current and emerging IoT technologies, and the implications of their use.

To conduct this assessment, GAO reviewed key reports and scientific literature; convened two expert meetings with the assistance of the National Academies; and interviewed officials from two agencies to obtain their views on specific implications of the IoT.

Ten federal agencies and twelve experts reviewed the draft report and some provided technical comments, which were incorporated as appropriate.

Federal Buildings: GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program GAO-18-200: Published: Jan 30, 2018. Publicly Released: Jan 30, 2018.

What GAO Found

Limited quantified information exists on the costs and benefits of the General Services Administration's (GSA) smart buildings program's key technologies. GSA officials stated that the approximate cost of equipping a building with these technologies ranged between about $48,000 to $155,000. However, they stated that accurately calculating installation costs is challenging because GSA typically installs these technologies in selected buildings incrementally and sometimes as part of other capital improvement projects. Additionally, GSA officials identified perceived operational benefits of the smart buildings program's key technologies, including that these technologies enable officials to more precisely identify building system problems and more closely monitor contractors. However, existing data on the smart buildings program are of limited usefulness in quantifying the program's benefits. For example, according to GSA officials, while data from an application within GSAlink that estimates avoided costs from addressing each fault that GSAlink identifies are useful for prioritizing maintenance actions, the imprecise estimates preclude their use as a measure of actual avoided costs in quantifying program benefits.

GSA does not have documented, clearly defined goals for the smart buildings program, nor has GSA developed performance measures that would allow it to assess the program's progress. These omissions are contrary to leading practices of results-oriented organizations identified in previous GAO work. GSA officials verbally described broad goals for the smart buildings program to GAO, but the agency has not documented these goals. Further, because GSA has not clearly defined its verbally expressed goals, it cannot demonstrate progress in achieving them. For example, GSA officials said that the agency cannot measure progress for the stated goal of improving tenant productivity and comfort because of the subjective nature of individual tenant preferences, such as for office temperatures. Additionally, GSA has not developed performance measures to assess the program, and GSA's lack of data that can be used to quantify benefits of the program impedes its ability to measure the success of the program. Without clearly defined goals, related performance measures, and data that can be used to measure its progress, GSA is limited in its ability to make informed decisions about the smart buildings program.

GSA faces challenges in implementing the smart buildings program and has taken steps to mitigate these challenges. Since smart building technologies are Internet-connected, they are potentially vulnerable to cyberattacks that could compromise security or cause harm to facilities or their occupants. GSA has taken actions intended to mitigate cybersecurity challenges, such as instituting policies to address threats and known vulnerabilities and moving Internet-connected

building systems to GSA's secured network. Separately, according to GSA officials, GSA faces implementation challenges related to the limited technological proficiency of some GSA building managers and contractors or lack of buy-in from them. GSA is taking actions intended to address these challenges. For example, it has provided training to staff and contractors, and its central office monitors the extent to which staff address problems detected by the smart buildings program's key technologies.

Why GAO Did This Study

To help comply with federal policies aimed at improving federal building energy and environmental management, GSA has implemented a smart buildings program nationwide in federally owned buildings under its custody and control. Two key technologies included in the program are Internet-connected advanced utility meters and an analytical software application, GSAlink, which alerts staff to potential building system problems, such as equipment operating outside of normal hours.

GAO was asked to review GSA's smart buildings program. This report examines: (1) what is known about the costs and benefits of the program, (2) the extent to which GSA has developed performance goals and measures to help it manage the performance of the program, and (3) any challenges GSA faces in implementing the technologies used in the program and GSA's actions to mitigate those challenges. GAO reviewed relevant GSA documentation, interviewed officials at GSA's central and regional offices, and visited a sample of GSA smart buildings in San Francisco, California, and Washington, D.C. that were selected based on the high concentration of GSA smart buildings located in each city.

What GAO Recommends

GAO recommends that GSA establish clearly defined performance goals and related performance measures for the smart buildings program, and identify and develop data to measure progress. GSA concurred with GAO's recommendations.

FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices Contestants will compete for a top prize of $25,000 for best technical solution

January 4, 2017

Technology Bureau of Consumer Protection Consumer Protection Privacy and Security Consumer Privacy Data Security

The Federal Trade Commission announced today that it is challenging the public to create an innovative tool that will help protect consumers from security vulnerabilities in the software of home devices connected to the Internet of Things. The agency is offering a cash prize of up to $25,000 for the best technical solution, with up to $3,000 available for up to three honorable mention winner(s).

The FTC is asking IoT Home Inspector Challenge contestants to develop a tool that would address security vulnerabilities caused by out-of-date software in IoT devices. An ideal tool might be a physical device that the consumer can add to his or her home network that would check and install updates for other IoT devices on that home network, or it might be an app or cloud-based service, or a dashboard or other user interface. Contestants also have the option of adding features such as those that would address hard-coded, factory default or easy-to-guess passwords.

"Every day American consumers are offered innovative new products and services to make their homes smarter," said Jessica Rich. "Consumers want these devices to be secure, so we're asking for creativity from the public – the tinkerers, thinkers and entrepreneurs – to help them keep device software up-to-date."

The Internet of Things, an array of billions of everyday objects sending and receiving data over the internet, is expanding rapidly with the adoption of applications such as health and fitness monitors, home security devices, connected cars and household appliances. It holds many potential benefits for consumers, but also raises numerous privacy and security concerns that could undermine consumer confidence.

Submissions will be accepted as early as March 1, 2017 and are due May 22, 2017 at 12:00 p.m. EDT. Winners will be announced on or about July 27, 2017.

Up to 20 contestants will be selected in the first round, where judges will only assess the contestants' videos and abstracts without the detailed explanation. Qualifying contestants will then move on to the next and final round where the detailed explanations will be considered for a chance to win the top prize of $25,000 or $3,000 for honorable mention.

An expert panel of five judges will judge the contest.

This the FTC's fourth government contest under the America COMPETES Act, and the first one addressing IoT issues. In 2015, the FTC hosted robocall contests in partnership with Pindrop Security and the Canadian Radio-television and Telecommunications Commission.

Complete rules for the current contest are published in the Federal Register and available at: ftc.gov/IoTHomeInspector where you can find instructions and requirements regarding the registration and submission process. Contest information will also be posted on Challenge.gov, an online challenge platform administered by the U.S. General Services Administration.

FBI: Internet of Things Poses Opportunities for Cyber Crime

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

Automated devices which remotely or automatically adjust lighting or HVAC

Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings

Medical devices, such as wireless heart monitors or insulin dispensers

Thermostats

Wearables, such as fitness devices

Lighting modules which activate or deactivate lights

Smart appliances, such as smart refrigerators and TVs

Office equipment, such as printers

Entertainment devices to control music or television from a mobile device

Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT Risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other

systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety. The main IoT risks include:

An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. The UPnP describes the process when a device remotely connects and communicates on a network automatically without authentication. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping;

An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information;

Compromising the IoT device to cause physical harm;

Overloading the devices to render the device inoperable;

Interfering with business transactions.

What an IoT Risk Might Look Like to You?

Unsecured or weakly secured devices provide opportunities for cyber criminals to intrude upon private networks and gain access to other devices and information attached to these networks. Devices with default passwords or open Wi-Fi connections are an easy target for cyber actors to exploit.

Examples of such incidents:

Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers. Many devices have default passwords cyber actors are aware of and others broadcast their location to the Internet. Systems not properly secured can be located and breached by actors who wish to stream live feed on the Internet for anyone to see. Any default passwords should be changed as soon as possible, and the wireless network should have a strong password and firewall.

Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting. The exploits allow criminals to obtain administrative privileges on the automated device. Once the criminals have obtained the owner's privileges, the criminal can access the home or business network and collect personal information or remotely monitor the owner's habits and network traffic. If the owner did not change the default password or create a strong password, a cyber criminal could easily exploit

these devices to open doors, turn off security systems, record audio and video, and gain access to sensitive data.

E-mail spam attacks are not only sent from laptops, desktop computers, or mobile devices. Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail. Devices affected are usually vulnerable because the factory default password is still in use or the wireless network is not secured.

Criminals can also gain access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines. Once criminals have breached such devices, they have access to any personal or medical information stored on the devices and can possibly change the coding controlling the dispensing of medicines or health data collection. These devices may be at risk if they are capable of long-range connectivity.

Criminals can also attack business-critical devices connected to the Internet such as the monitoring systems on gas pumps. Using this connection, the criminals could cause the pump to register incorrect levels, creating either a false gas shortage or allowing a refueling vehicle to dangerously overfill the tanks, creating a fire hazard, or interrupt the connection to the point of sale system allowing fuel to be dispensed without registering a monetary transaction.

Consumer Protection and Defense Recommendations

Isolate IoT devices on their own protected networks;

Disable UPnP on routers;

Consider whether IoT devices are ideal for their intended purpose;

Purchase IoT devices from manufacturers with a track record of providing secure devices;

When available, update IoT devices with security patches;

Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it operate on a home network with a secured Wi-Fi router;

Use current best practices when connecting IoT devices to wireless networks, and when connecting remotely to an IoT device;

Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor;

Ensure all default passwords are changed to strong passwords. Do not use the default password determined by the device manufacturer. Many default passwords can be easily located on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets. If the device does not allow the capability to change the access password, ensure the device providing wireless Internet service has a strong password and uses strong encryption.

Source: https://www.ic3.gov/media/2015/150910.aspx

Glossary

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Availability: Ensuring timely and reliable access to and use of information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Capacity: The information carrying ability of a telecommunications facility. What the "facility" is determines the measurement (e.g., you might measure a data line's capacity in bits per second). (Newton's Telecom Dictionary)

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. (NIST Special Publication [SP] 800-145)

Communications: Modern network is the totality of users, devices, data and applications. (National Security Telecommunications Advisory Committee [NSTAC] Secure Government Communications [SGC] Subcommittee Definition)

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: (1) the development of a strategy to regularly evaluate selected IA controls/metrics; (2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events; (3) recording changes to IA controls, or changes that affect IA risks; and (4) publishing the current security status to enable information-sharing decisions involving the enterprise. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Critical Infrastructure and Key Resources (CIKR): Elements that support the essential functions and services that underpin American society. (DHS.gov) Data Aggregation: Compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Data Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Defense-in-Depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Fair Information Practice Principles: A set of eight principles that form the basis of the Department of Homeland Security's privacy compliance policies and procedures governing the use of personally identifiable information. (DHS.gov)

Government Emergency Telecommunications Service (GETS): Provides national security and emergency preparedness (NS/EP) personnel a high probability of completion for their phone calls when normal calling methods are unsuccessful. It is designed for periods of severe network congestion or disruption, and works through a series of enhancements to the public switched telephone network. GETS is in a constant state of readiness. Users receive a GETS "calling card" to access the service. This card provides access phone numbers, Personal Identification Number (PIN), and simple dialing instructions. (DHS.gov)

Identity Management: The structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices. (International Telecommunications Union Identity Correspondence Group)Identity Validation: Tests enabling an information system to authenticate users or resources. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Industrial Control Systems: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Information Security Architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Internet Protocol: Part of the Transmission Control Protocol/Internet Control family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and

recognizes incoming messages; used in gateways to connect networks at Open Systems Interconnection network Level 3 and above. (Newton's Telecom Dictionary)

Interoperability: The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together for mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility for use in services outside the direct control of the issuing assigner. International Organization for Standardization Technical Committee 46/Subcommittee 9)

Long Term Evolution (LTE): The access part of the Evolved Packet System. The main requirements for the new access network are high spectral efficiency, high peak data rates, short round trip time, and frequency flexibility. (3GPP.org) LTE is the standard created and adopted by 3GPP through its Release 8 regarding fourth generation (4G) cellular wireless telecommunications. 4G is based upon an all IP packet switched network that supports mobile broadband access as well as multi-media applications with high data rates and low latencies utilizing spectrum efficiency by smooth handoffs and seamless roaming across multiple networks. LTE has been accepted and adopted by national and international communities as the foundation for future mobile telecommunications. (http://transition.fcc.gov/pshs/docs/LTE_Info_Sheet_09082010.pdf)

Machine-to-Machine (M2M): Technologies that enable computers, embedded processors, smart sensors, actuators and mobile devices to communicate with one another, take measurements and make decisions - often without human intervention. (Machine to Machine Technology in Demand Responsive Commercial Buildings)

Network Priority Services: A National Communications System program to define and deploy priority voice communications in the next generation packet- switched network environment. (DHS.gov)

NS/EP Communications: Primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international); to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications also include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (National Security and Emergency Preparedness Communications Executive Committee definition based on Executive Order 13618)

Personally Identifiable Information: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or

biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Government Accountability Office Report 08-536)

Reliability: A measure of how dependable a system is once you actually use it. (Newton's Telecom Dictionary)

Resilience: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (PPD-8: National Preparedness)

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision

Security: A way of insuring data on a network is protected from unauthorized use. Network security measures can be software-based where passwords restrict users' access to certain data files or directories. This kind of security is usually implemented by the network operating system. Audit trails are another software-based security measure, where an ongoing journal of what users did what with what files is maintained. Security can also be hardware-based, using more traditional lock and key. (Newton's Telecom Dictionary)

Smart Device: A smart device is an electronic device that is cordless (unless while being charged), mobile (easily transportable), always connected (via WiFi, 3G, 4G etc.) and is capable of voice and video communication, internet browsing, geolocation (for search purposes and location-based services) and that can operate to some extent autonomously. (NSTAC SGC Subcommittee Definition)

Spectrum: A continuous range of frequencies, usually wide in extent within which waves have some specific common characteristics. (Newton's Telecom Dictionary)

Supervisory Control and Data Acquisition (SCADA Systems): A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (delays, data integrity, etc.) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Survivability: A property of a system, subsystem, equipment, process, or procedure, that provides a defined degree of assurance that the device or system will continue to work during

and after a natural or man-made disturbance (e.g., nuclear attack). This term must be qualified by specifying the range of conditions over which the entity will service, the minimum acceptable level of post-disturbance functionality, and the maximum acceptable outage duration. (Newton's Telecom Dictionary)

Telecommunications Service Priority (TSP): A regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of national security and emergency preparedness (NS/EP) telecommunications services. (DHS.gov)

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Wireless Priority Service (WPS): A priority communications service for improving call completion capabilities for authorized NS/EP cell phone users. In the event of congestion in the wireless network, an emergency call using WPS can queue for the next available channel. All WPS (and GETS) calls will receive priority during access, transport, and egress to a wireless mobile on a WPS carrier, even if the terminating mobile is not subscribed to WPS. WPS calls do not preempt calls in progress or deny the general public's use of the radio spectrum. (GETS/WPS

Source: https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf

CREATE EBOOKS IN 30 SECONDS WITHOUT WRITING A WORD

CLICK HERE TO SEE HOW