# UNDERSTANDING THE ROLE OF CONNECTED DEVICES IN RECENT CYBERATTACKS

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

AND THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

NOVEMBER 16, 2016

**Serial No. 114–175**

Printed for the use of the Committee on Energy and Commerce
*energycommerce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
23–438 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
*Chairman*

JOE BARTON, Texas
*Chairman Emeritus*
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
*Vice Chairman*
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, JR., New Jersey
*Ranking Member*
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California

## SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon
*Chairman*

ROBERT E. LATTA, Ohio
*Vice Chairman*
JOHN SHIMKUS, Illinois
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

ANNA G. ESHOO, California
*Ranking Member*
MICHAEL F. DOYLE, Pennsylvania
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
BOBBY L. RUSH, Illinois
DIANA DEGETTE, Colorado
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
JERRY McNERNEY, California
BEN RAY LUJÁN, New Mexico
FRANK PALLONE, JR., New Jersey *(ex officio)*

## SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas
*Chairman*

LEONARD LANCE, New Jersey
*Vice Chairman*
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
FRED UPTON, Michigan *(ex officio)*

JANICE D. SCHAKOWSKY, Illinois
*Ranking Member*
YVETTE D. CLARKE, New York
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
BOBBY L. RUSH, Illinois
G.K. BUTTERFIELD, North Carolina
PETER WELCH, Vermont
FRANK PALLONE, JR., New Jersey *(ex officio)*

# CONTENTS

Page

Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement ..... 2
Prepared statement ..... 3
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement ..... 3
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement ..... 4
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement ..... 5
Prepared statement ..... 6
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement ..... 7
Hon. Fred Upton, a Representative in Congress from the State of Michigan, prepared statement ..... 80
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, prepared statement ..... 81

## WITNESSES

Dale Crew, Senior Vice President and Chief Security Officer, Level 3 Communications ..... 9
Prepared statement ..... 12
Bruce Schneier, Fellow, Berkman-Klein Center at Harvard University, and Lecturer and Fellow, Harvard Kennedy School of Government ..... 17
Prepared statement ..... 20
Kevin Fu, Ph.D., Chief Executive Officer, Virta Laboratories, Inc., and Associate Professor, Department of Electrical Engineering and Computer Science, University of Michigan ..... 26
Prepared statement ..... 28

## SUBMITTED MATERIAL

Statement of Craig Spiezle, Executive Director and President, Online Trust Alliance, November 16, 2016, submitted by Mr. Burgess ..... 83
Letter of November 15, 2016, from Kyle Pitsor, Vice President, Government Relations, National Electrical Manufacturers Association, to Mr. Walden, et al., submitted by Mr. Burgess ..... 92
Statement of the College of Healthcare Information Management Executives and the Association for Executives in Healthcare Information Security, November 16, 2016, submitted by Mr. Burgess ..... 121
Statement of the Advanced Medical Technology Association, November 16, 2016, submitted by Mr. Burgess ..... 125
Statement of Gary Shapiro, President and Chief Executive Officer, Consumer Technology Association, November 16, 2016, submitted by Mr. Burgess ..... 126

# UNDERSTANDING THE ROLE OF CONNECTED DEVICES IN RECENT CYBERATTACKS

**WEDNESDAY, NOVEMBER 16, 2016**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
JOINT WITH THE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
*Washington, DC.*

The subcommittees met, pursuant to notice, at 10:05 a.m., in Room 2175, Rayburn House Office Building, Hon. Greg Walden (chairman of the Subcommittee on Communications and Technology) presiding.

Members present: Representatives Walden, Burgess, Lance, Latta, Barton, Shimkus, Blackburn, Guthrie, Olson, Kinzinger, Bilirakis, Johnson, Long, Ellmers, Brooks, Mullin, Collins, Pallone (ex officio), Schakowsky, Eshoo, Rush, DeGette, Matsui, McNerney, Welch, Luján, Loebsack, and Kennedy.

Staff present: Grace Appelbe, Staff Assistant; James Decker, Policy Coordinator, Commerce, Manufacturing and Trade; Paige Decker, Executive Assistant; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Blair Ellis, Digital Coordinator/Press Secretary; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Gene Fullano, Detailee, Communications and Technology; Giulia Giannangeli, Legislative Clerk, Commerce, Manufacturing, and Trade, and Environment and the Economy; A.T. Johnston, Senior Policy Advisor; Grace Koh, Counsel, Communications and Technology; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Dan Schneider, Press Secretary; Olivia Trusty, Professional Staff Member, Commerce, Manufacturing, and Trade; Gregory Watson, Legislative Clerk, Communications and Technology; Jessica Wilkerson, Professional Staff Member, Oversight and Investigations; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Jeff Carroll, Democratic Staff Director; David Goldman, Democratic Chief Counsel, Communications and Technology; Lisa Goldman, Democratic Counsel; Elizabeth Letter, Democratic Professional Staff Member; Jerry Leverich, Democratic Counsel; Lori Maarbjerg, Democratic FCC Detailee; Dan Miller, Democratic Staff Assistant; Caroline Paris-Behr, Democratic Policy Analyst; Matt Schumacher, Democratic Press Assistant; and Ryan Skukowski, Democratic Senior Policy Analyst.

## OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. I will call to order the Subcommittee on Communications and Technology in our joint committee hearing with the Subcommittee on Commerce, Manufacturing, and Trade.

Good morning, everyone. I will start with opening statements for our side and for our subcommittee, and then I think we go back and forth. So we will work this out.

I want to thank the two subcommittees for coming together on this very important topic that I think we all share a deep concern about.

We live in a world that is increasingly connected. Our smartphones are now capable of locking and unlocking our front doors at home, turning on lights, checking the camera for packages left on the doorstep. We are able to measure our steps, check our baby monitors, record our favorite programs from wherever we have connectivity. We will soon be able to communicate—or, excuse me, we can communicate with our offices, too—but commute to our offices in driverless cars, trains, buses, have our child's blood sugar checked remotely, and divert important energy resources from town to town efficiently.

These are incredible potentially life-saving benefits that our society is learning to embrace, but we are also learning that these innovations do not come without a cost. In fact, recently we encountered a denial of service attack on a scale never before seen. This attack effectively blocked access to popular sites like Netflix and Twitter by weaponizing unsecured network connected devices like cameras and DVRs. Once these devices came under the command and control of bad actors, they were used to send a flood of DNS requests that ultimately rendered the DNS servers ineffective. As I understand it, at the beginning of this attack it was virtually impossible to distinguish malicious traffic from other normal traffic, making it particularly difficult to mitigate against attack.

So how do we make ourselves more secure without sacrificing the benefits of innovation and technological advances? A knee-jerk reaction might be to regulate the Internet of Things. And while I am not taking a certain level of regulation off the table, the question is whether we need a more holistic approach. The United States cannot regulate the world. Standards applied to American-designed, American-manufactured, American-sold devices won't necessarily capture the millions of devices purchased by the billions of people around the world, so the vulnerabilities might remain.

Any sustainable and effective solution will require input from all members of the ecosystem of the so-called Internet of Things. We will need a concerted effort to improve not only device security, but also coordinate network security and improve the relationships between industry and security researchers. We are all in this thing together and industry, Government, researchers, and consumers will need to take responsibility for securing this Internet of Things.

So today we will hear from a very distinguished panel of witnesses on some of the approaches that can be brought to bear on this challenge. My hope is that this hearing will help to sustain and accelerate conversations on our collective security and foster the innovation that makes the Internet the greatest engine of communications and commerce the world has ever seen.

So I thank our witnesses for being here. We appreciate your willingness to come and share your expertise. It is very helpful in our endeavors, and I look forward to your testimony.

[The prepared statement of Mr. Walden follows:]

## PREPARED STATEMENT OF HON. GREG WALDEN

Good morning. We live in a world that is increasingly connected. Our smart phones are now capable of locking and unlocking our front doors at home; turning on lights; and checking the camera for packages left on the doorstep. We are able to measure our steps; check our baby monitors; and record our favorite programs from wherever we have connectivity. We'll soon be able to commute to our offices in driverless cars, trains, and buses; have our child's blood sugar checked remotely; and divert import energy resources from town to town efficiently.

These are incredible, potentially life-saving benefits that our society is learning to embrace, but we are also learning that these innovations do not come without cost. This past month, we encountered a Denial of Service attack on a scale never before seen. This attack effectively blocked access to popular sites like Netflix and Twitter by weaponizing unsecured network-connected devices like cameras and DVRs. Once these devices came under the command and control of bad actors, they were used to send a flood of DNS requests that ultimately rendered the DNS servers ineffective. As I understand it, at the beginning of this attack it was virtually impossible to distinguish malicious traffic from other normal traffic, making it particularly difficult to mitigate against the attack.

How do we make ourselves more secure without sacrificing the benefits of innovation and technological advances? The knee-jerk reaction might be to regulate the Internet of Things, and while I am not taking that off the table, the question is whether we need a more holistic solution. The United States can't regulate the world. Standards applied to American-designed, American-manufactured, or American-sold devices won't capture the millions of devices purchased by the billions of people around the world.

Any sustainable and effective solution will require input from all members of the ecosystem for the so-called "Internet of Things." We'll need a concerted effort to improve not only device security, but also coordinate network security and improve the relationship between industry and security researchers. We're all in this together and industry, Government, researchers, and consumers will need to take responsibility for securing the Internet of Things.

Today we'll hear from a panel of distinguished witnesses on some of the approaches that can be brought to bear on this challenge. My hope is that this hearing will help to sustain and accelerate conversations on our collective security and fostering the innovation that makes the Internet the greatest engine of communcations and commerce the world has known. I thank the witnesses for their willingness to come and share their expertise. I'm looking forward to your testimony.

Mr. WALDEN. At this time, I would yield to Mrs. Blackburn for an opening statement.

## OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman.

And I also want to welcome our witnesses, and we appreciate your time. You know, we did an Internet of Things hearing in March 2015, and at that point I talked a lot about the convenience that this brings to us in our daily lives and about the opportunities that it will open for us. I think now as we look at it, as the chairman said, you look at the cost, you look at the maximized use that exists. I think that by 2020, the expectation is 3.4 billion devices that would be in this universe of connected. That means we have vulnerabilities that exist, entry points, and we will want to discuss some of those vulnerabilities with you today, get your insight, and see how we as policymakers work with this wonderfully exciting, innovative area in order to make certain that Americans have access, but they also know that there is, as the chairman said, security as we approach this.

And with that, Mr. Chairman, I yield back.

Mr. WALDEN. The gentlelady yields back the balance of her time. I will yield back the balance of my time as well.

We will now turn to my friend from California, the gentlelady Ms. Eshoo, for opening comments.

## OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman.

First of all, I want to express our collective thanks from this side of the aisle to you for responding to our request to have this hearing. Mr. Pallone, Mr. McNerney, Ms. Schakowsky, Ms. DeGette, and myself all made the request, and we are grateful to you for holding the hearing, because we think that this is, obviously, a very large issue and something that concerns the American people.

In fact, Americans are connecting more devices to the Internet than ever before. Most of us carry at least one in our pocket, but as technology evolves, we are seeing a proliferation of everyday items and appliances that connect online. This is good. Today, everything from washing machines to light bulbs are now capable of connecting to the Internet. The business world also relies more and more on the Internet, in fact, Internet-enabled objects, to drive their efficiencies to produce lower cost.

There are as many as 6.4 billion—billion with a B—Internet of Things products in use worldwide just this year. The growth in this market is expected to be significant, including estimates of over 20 billion Internet-enabled products connected worldwide by 2020. So this is not a small market. It makes it a very large issue. It is an economic one, and we don't want to damage that, but it is something that needs our attention.

There is great potential for innovation as more devices become connected, but there is also the potential for serious risk if they are not properly secured. That is really what we are pursuing here. We need to look no further than the major attack on October 21st that crippled some of the most popular Web sites and services in our country. The distributed denial of service attack against Dynamic Network Services, known as Dyn, was made possible by unsecure Internet of Things devices that attackers were able to infect with malware. This army of devices was then harnessed by the attackers to bring down Dyn's servers. Similar attacks in October targeted a journalist and a French cloud services provider.

These attacks raise troubling questions about the security of Internet-enabled devices and their potential to be used as weapons by cyberattackers. For example, it has been reported that some devices used in these attacks may have lacked the functionality to allow users to change the default username and password. We already know that an important way to prevent cyberattacks is to practice good cyberhygiene, which includes changing default usernames and passwords. When products lacking the commonsense functionality are manufactured, shipped, and eventually connected, they put users and the Internet as a whole at risk. So it seems to me that this is an area that we need to explore with our witnesses.

There is also the issue of how long these unsecured devices can remain in use. The Dyn attack reportedly used infected devices that were first manufactured as early as 2004. Manufacturers may no longer update products that have been in use for so long, further exposing users and the Internet to security risks.

Finally, we have to recognize that this is a global issue. Level 3 Communications estimates that a little more than a quarter of these devices infected with the malware that was used in the Dyn attacks are located in the United States. One of the major manufacturer of products that appear to be particularly vulnerable is based in China. This is important to keep in mind as we explore how to address this problem going forward.

So this hearing, I think, is a very important step in helping us, first of all, to all understand what lessons we should take away from these recent attacks. The Internet of Things offers exciting possibilities for innovation, but we can't afford to ignore the risks that come when devices are designed without security.

Whatever the ultimate solution is, I think industry must play a central role in the effort to address these issues, and I look forward to hearing from our witnesses today. You play a very important role in this.

So, with that, thank you again, Mr. Chairman, for allowing this hearing to take place, and I yield back the balance of my time.

Mr. WALDEN. The gentlelady yields back the balance of her time.

The Chair now recognizes the gentleman from Texas, Dr. Chairman Burgess.

## OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. Thank you, Mr. Chairman. And good morning to our witness panel today. Thank you, Mr. Chairman, for holding the hearing and allowing us to have this discussion about the recent cyberattacks.

Several popular Web sites were knocked offline for several hours on October 21 of this year. Hackers used malware to create a botnet, sort of a gargantuan, amorphous mass of connected devices, to flood a domain server with terabytes of traffic, overwhelming the system and preventing legitimate traffic from accessing those devices.

In this case, the result was brief, but the outages were on consumer-facing Web sites. The incident is unique in that it wasn't someone's desktop or laptop, but it was the armies of compromised devices that launched these attacks without the knowledge of the device owners. Many of the devices are regular household items, such as baby monitors, DVRs, Web cams. And many consumers do not realize they do need strong cyberprotections on even these everyday devices.

But that is exactly why this attack and others like it has been so successful. The malware that created this botnet spread to vulnerable devices by continuously scanning the Internet for Internet of Things systems protected only by the factory default manually generated usernames and passwords.

The balance between functionality and security is not going to be resolved in the near term. Consumers want the newest and fastest device, they want it as soon as possible, and they have not employed adequate security protections. In fact, the most common password is the word “password.” The culture surrounding personal cybersecurity must change to ensure that the Internet of Things is not vulnerable to a single insecure device.

The Subcommittee on Commerce, Manufacturing, and Trade has explored cybersecurity through a number of hearings, including our Disrupter Series. Cybersecurity, the issue of cybersecurity has been raised and discussed at each of these hearings. The Government is never going to be big enough to have the manpower and the resources to address all of these challenges as they come up, which is why it is so important and why I am grateful that we have industry here today to discuss this with us, because they must take the lead.

Recent attacks present a unique opportunity to examine the scope of the threats and the vulnerabilities presented by connected devices and to learn how stakeholders are considering these risks throughout the supply chain, as well as how consumers are responding in the market. We have learned about a number of best practices and the standard-setting projects that are ongoing with various groups.

It is an exciting time. And the growth of interconnected device, the growth of the Internet of Things, it is really going to be life-changing in so many industries, but we also need to see meaningful leadership from industry about how to address these real challenges.

Again, I want to welcome our witnesses, and then I am pleased to yield the balance of my time to the gentleman from Ohio, Mr. Latta.

[The prepared statement of Mr. Burgess follows:]

## PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Good morning and welcome to our joint hearing examining recent cyber-attacks. Several popular Web sites were knocked offline for a couple of hours on October 21, 2016. Hackers used malware to create a botnet, or massive group of compromised connected devices, to flood a domain server system with terabytes of traffic, overwhelming the system and preventing the server from responding to legitimate traffic.

In this case, the result was brief outages on consumer facing Web sites. However, the incident is unique in that it utilized armies of compromised devices, rather than computers and laptops, to launch attacks without the knowledge of device owners. Many of these devices are everyday household items—such as baby monitors, DVRs, and webcams—that many consumers do not realize need strong cyberprotections.

But that is exactly why this attack, and others like it, has been successful. The malware that created this botnet spread to vulnerable devices by continuously scanning the Internet for Internet of Things systems protected only by factory default or manually generated usernames and passwords.

The balance between functionality and security is not going to be resolved in the near term. Consumers want the newest and fastest device as soon as possible, but they have not employed adequate security protections. In fact, the most common password is the word password. The culture surrounding personal cybersecurity must change to ensure the Internet of Things is not vulnerable to a single insecure device.

The Subcommittee on Commerce, Manufacturing, and Trade has explored cybersecurity throughout a number of hearings, including our Disrupter Series.

Cybersecurity has been raised and discussed at each of these hearings. Government is never going to have the man power or resources to address all of these challenges as they come up-which is why we need industry to take the lead.

Recent attacks present a unique opportunity to examine the scope of the threats and vulnerabilities presented by connected devices and learn how stakeholders are considering these risks throughout the supply chain, as well as how consumers are responding in the market.

We have learned about a number of best practices, and standards-setting projects are on-going with various groups.

We are facing exciting growth in the connected device industry, but we also need to see meaningful leadership from industry about how to address these challenges.

Mr. LATTA. Thank you very much, and I appreciate the gentleman for yielding. And I also appreciate both chairmen of both subcommittees for holding this very important subcommittee hearing today on the cybersecurity risks associated with connected devices.

As has been mentioned, that last month we witnessed one of the largest distributed denial of service attacks caused by devices connected to the Internet or the Internet of Things. The attack against Dyn revealed the impact that a lack of adequate security measures in these devices can have on the broader Internet community. By simply exploiting weak security features, such as default usernames and passwords, hackers could easily leverage hundreds of thousands of networked devices and compromise several major Web sites.

That is why it is essential, under the Internet of Things, device manufacturers build in security by design and have the ability to deploy patches or upgrades. Additionally, consumers must be vigilant in securing devices through good cyberhygiene practices in order to guard data and fully experience the benefit of the Internet of Things.

As the co-chair of the committee on the Internet of Things Working Group, I am all too familiar with this issue. Cybersecurity is among one of the most common things that is mentioned in all of our working group briefings. No matter what type of IoT, from health to energy applications, securing devices and protecting consumer data is a top priority.

Today, we are reminded again that there is a need for IoT security guidelines that keep pace with rapidly evolving technologies. However, there is a delicate balance between oversight and regulatory flexibility, and we must encourage the industry to establish best practices that will not hinder innovation and protect consumer privacy and security.

And, with that, I appreciate the gentleman for yielding, and I yield back.

Mr. WALDEN. The gentlemen yield back their time.

We will now turn to the gentlelady from Illinois, Ms. Schakowsky, for opening comments.

## OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

With each report of a new cyberattack, Americans increasingly realize how vulnerable their devices are. On October 21, Americans lost access to sites such as Twitter, Amazon, and Spotify because of a massive distribution denial of service, or DDoS, attack against Dyn, a domain naming system company.

In the wake of that cyberattack, I joined with Representatives Pallone, Eshoo, DeGette, and McNerney in requesting a hearing like this—and I appreciate it very much that we are having it—on this important issue. We need to better understand our vulnerabilities and update Federal policy to stop such attacks in the future.

The motivations of hackers vary from identity theft to actually undermining public trust. They go after consumers, businesses, and even Presidential elections.

The U.S. intelligence community found that hackers supported by the Russian Government put their thumb on the scale in 2016. I strongly believe that use of cyberattacks by a foreign actor to manipulate our democracy should be troubling to everyone. This problem does not go away now that the 2016 election is over.

The day after the election, a Wired article reported, quote, "That Russia perceives those operations as successful, experts say, will only encourage similar hacks aimed at shifting elections and sowing distrust of the political processes in Western democracies," unquote. Everyone, whether your candidate won or lost last week, must grapple with this threat, and I hope that we will work on a bipartisan basis to protect our democracy from foreign interference.

Russian hackers exploited holes in security on computers and servers. The hackers that carried out the October 21 DDoS attack directed their attack through the Internet of Things.

The Internet of Things is uniquely vulnerable to cyberattacks. IoT devices often have less protection from malware and manufacturers are often slower to install security patches. Manufacturers put consumers at further risk by using default passwords or hardcoded credentials. Once hackers find out what those passwords are, they can hack hundreds, thousands, or even millions of devices. That is what happened in the Dyn attack.

Hackers accessed an army of IoT devices by exploiting default passwords. They then used that army to attack Dyn. Traffic from the IoT devices overwhelmed the service and shut it down, which, in turn, cut off Americans' access to many popular Web sites. You don't have to be a tech expert to see the terrifying potential for future cyberattacks. So it is time now for action.

Two weeks ago, Ranking Member Pallone and I called on the Federal Trade Commission to work with IoT manufacturers to patch vulnerabilities on their devices and require the changing of default passwords. We also called on the FTC to alert consumers about potential security risks. We need stronger cybersecurity standards for all devices that could be attacked or used to launch a cyberattack.

Given the nature of cyberattacks, we cannot count on IoT manufacturers to do the right thing on their own. They have little financial incentive to improve security, and their customers may not even realize when their devices are being used to harm others. Consumer watchdogs, like the FTC, must take a leading role in promoting cybersecurity and holding companies accountable when they fail to provide adequate protections.

Unfortunately, at the same time that the threat to consumers from cyberattacks are rising, the Republican majority is pushing legislation to reduce the FTC's authority and cripple its enforcement capabilities. Stopping irresponsible behavior by companies requires strong consent orders and the ability to pursue privacy cases. The so-called, quote, "process reform," unquote, bill that Republicans reported out of committee would threaten the FTC's ability in those areas. Instead of rolling back consumer protections, we need to face today's cyberthreats head on. Consumers can't afford to be left vulnerable. And in the long run, manufacturers can't survive a pattern of high-profile cyberattacks that undermine consumer trust in their products.

In Mr. Schneier's written testimony, he called the Dyn attack, quote, "as much a failure of market policy as it was of technology," unquote. We should not be content with failure any longer.

I want to thank the chairman for listening to our request for a hearing, and we have to continue our work on this issue in the months and years to come.

Mr. WALDEN. The gentlelady yields back her time. We thank you very much for your request. We share in this concern, obviously. It is a bipartisan issue.

We look forward now to the testimony from our expert witnesses. We are glad you are all here, and we will start with Mr. Dale Drew, who is the senior vice president/chief security officer for Level 3 Communications.

Mr. Drew, welcome. Thank you very much. Turn on your microphone and have at it.

**STATEMENTS OF DALE DREW, SENIOR VICE PRESIDENT, CHIEF SECURITY OFFICER, LEVEL 3 COMMUNICATIONS; BRUCE SCHNEIER, FELLOW, BERKMAN–KLEIN CENTER AT HARVARD UNIVERSITY, AND LECTURER AND FELLOW, HARVARD KENNEDY SCHOOL OF GOVERNMENT; AND KEVIN FU, PH.D., CEO, VIRTA LABORATORIES, INC., AND ASSOCIATE PROFESSOR, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF MICHIGAN**

## STATEMENT OF DALE DREW

Mr. DREW. Chairmen Walden and Burgess and Ranking Members Eshoo and Schakowsky, thank you for the opportunity to testify on behalf of Level 3 Communications regarding the recent cyberattacks on our Nation's communications landscape and the risks posed by vulnerabilities found in IoT devices.

Level 3 is a global communications company serving customers in more than 500 markets in over 60 countries. Given our significant network footprint and the amount of traffic we handle on a daily basis, Level 3 has a unique perspective on threats facing our communications landscape. Several years ago, Level 3 established the Threat Research Labs to actively monitor communications for malicious activity, helping to detect and mitigate threats on our networks, our customers, and the broader Internet. Every day our security team monitors more than 48 billion security events, detecting over 1 billion unusual or suspicious pieces of traffic.

The proliferation of IoT devices represents tremendous opportunities and benefits for consumers by connecting devices such as cameras, light bulbs, appliances, and other everyday items to the Internet. However, the lack of adequate security measures in these devices also poses significant risks to users in the broader Internet community.

Vulnerabilities in IoT devices stem from several sources. Some devices utilize default and easily identifiable passwords that hackers can exploit. Others utilize hard-coded credentials that users are not able to change. Many devices also lack the capability of updating their firmware, forcing consumers to monitor for and install the updates themselves.

The global nature of the IoT device marketplace means many products are manufactured in and shipped to foreign countries that have yet to embrace sound and mature cybersecurity practices. IoT devices are also particularly attractive targets because users often have very little way to know when they have been compromised. Unlike your personal computer or phone, which have endpoint protection capabilities and the user is more likely to notice when they perform improperly, compromised IoT devices may go unnoticed for longer periods of time.

In September of 2016, Level 3's Threat Research Labs began tracking a family of malware targeting IoT devices. The bad actors were leveraging the infected devices to create DDoS botnets, impacting not just those devices but potentially anyone on the Internet. The new malware, known as Mirai and its predecessor BASHLITE has affected nearly 2 million devices on the Internet. Mirai resulted in multiple major Web sites going offline, and the new attacks are alarming for their scope, impact, and the ease in which the attackers have employed them.

Also worrisome is that these attackers relied on just a fraction of the total available compromised IoT nodes in order to attack their victims, demonstrating the potential for significantly greater havoc for these new threats. Level 3 detected, for example, approximately 150,000 IoT devices were used to generate more than 500 gigabits per second of traffic, a significant amount of bandwidth that threatens the fabric of the global Internet.

The primary motivation for these attacks appear to be financial. Hackers utilize DDoS to overwhelm businesses, threatening to take their business offline unless they pay a ransom for the attacker. In other cases, attackers are simply out to create mischief.

Although Level 3 has not been a direct victim of these attacks, we are proactively taking steps to address these. We have contacted manufacturers of compromised devices to inform them of the problem and for them to take appropriate action, such as firmware updates or recalls. We have engaged in a public awareness campaign to educate consumers and businesses about the risk of IoT botnets and steps they can take to protect themselves. We are also working collaboratively with our industry partners to monitor this evolving threat and implementation of mitigation techniques.

With the exploding proliferation of IoT devices, so too will the threats they pose continue to expand and evolve. It will be imperative for all relevant stakeholders to continue to work collaboratively and address and mitigate IoT security risks so that we can reap the benefits of this exciting and transformative technology.

Thank you again very much for the opportunity to testify, and I look forward to taking your questions.

[The prepared statement of Mr. Drew follows:]

**Testimony of Dale Drew**
**Chief Security Officer**
**Level 3 Communications**

**Before the**

**U.S. House of Representatives**
**Committee on Energy and Commerce**
**Subcommittee on Communications and Technology, and the**
**Subcommittee on Commerce, Manufacturing, and Trade**

**Joint Hearing Entitled**
**"Understanding the Role of Connected Devices in Recent Cyber Attacks"**

**November 16, 2016**

Chairmen Walden and Burgess, and Ranking Members Eshoo and Schakowsky, thank you for the opportunity to testify on behalf of Level 3 Communications regarding the recent cyberattacks on our nation's communications landscape and the risks posed by vulnerabilities found in Internet of Things (IoT) devices.

Level 3 Communications is a Fortune 500 company that provides local, national and global communications services to enterprise, government and carrier customers. Level 3's comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; data center and cloud-based solutions. Level 3 serves customers in more than 500 markets in over 60 countries across a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities.

Given our significant network footprint and the amount of traffic we handle on a daily basis, Level 3 has a unique perspective on the threats facing our communications landscape. To address the growing extent of cybersecurity risks, several years ago Level 3 established the Threat Research Labs to actively monitor communications for malicious activity, helping to detect and mitigate threats to our networks, our customers, and the broader internet. Every day, our security team monitors more than 48 billion security events, detecting more than 1 billion unusual or suspicious pieces of traffic.

The proliferation of IoT devices represents tremendous opportunities and benefits for consumers by connecting devices such as cameras, lightbulbs, appliances and other everyday items to the internet. Estimates suggest there are already billions of IoT devices in operation and their use is growing dramatically. However, the lack of adequate security measures in these devices also poses significant risks to users and the broader internet community.

Vulnerabilities in IoT devices stem from several sources. Some devices utilize default and easily-identifiable passwords that hackers can exploit. Others utilize hard-coded credentials that users are not able to change. Many devices also lack the capability of updating their firmware, forcing consumers to monitor for and install updates themselves. The global nature of the IoT device marketplace means many products are manufactured in and shipped to foreign countries that have yet to embrace sound cybersecurity practices. IoT devices also are particularly attractive targets because users often have little way to know when they have been compromised. Unlike a personal computer or phone, which has endpoint protection capabilities and the user is more likely to notice when it performs improperly, compromised IoT devices may go unnoticed for longer periods of time.

In September 2016, Level 3's Threat Research Labs began tracking a family of malware targeting IoT devices. The bad actors were leveraging the infected devices to create Distributed Denial of Service (DDoS) botnets impacting not just those devices, but potentially anyone on the internet. The new malware known as Mirai and its predecessor BASHLITE has affected nearly 2 million devices on the internet. Mirai was used to attack the website KrebsOnSecurity.com as well as the Domain Naming System (DNS) company Dyn that compromised multiple major websites. These new attacks are alarming for their scope, impact, and the ease with which attackers employed them. Also worrisome is that these attackers relied on just a fraction of the total available compromised IoT nodes in order to attack their victims, demonstrating the potential for significantly greater havoc from these new threats. Level 3 detected approximately 150,000 IoT devices were used to generate more than 500 gigabits per second of traffic, a significant amount of bandwidth use that threatens the fabric of the global internet.

The primary motivation for these attacks appears to be financial. Hackers utilize DDoS to overwhelm a business, threatening to take their business offline unless they pay a ransom to the attacker. According to one estimate, the total costs of ransomware to U.S. businesses are expected to total $1 billion in 2016. In other cases, attackers are simply out to create mischief. We believe that in the case of Dyn, the relatively unsophisticated attacker sought to take offline a gaming site with which it had a personal grudge and rented time on the IoT botnet to accomplish this.

Level 3 is taking a number of steps to address these threats. In these recent IoT botnet attacks, Level 3 was not a direct victim of the attacks, but we see the devastating potential of what these unprotected IoT devices can bring, and we have decided to be proactive about protecting our backbone, our customers, and the global internet as a whole. We have contacted manufacturers of compromised devices to inform them of the problem and take appropriate action, such as firmware updates or recalls. We have engaged in a public awareness campaign to educate consumers and businesses about the risks of IoT botnets and steps they can take to protect themselves, such as updating the default passwords and downloading patches. We are working collaboratively with our industry partners to monitor this evolving threat and mitigation techniques. We also have actively been blocking critical elements of the IoT botnets in an effort to disrupt their communication.

With the exploding proliferation of IoT devices, so too will the threats they pose continue to expand and evolve. Bad actors are increasingly attracted to IoT devices since they can use those devices without being detected for long periods of time, they know most devices will not be monitored or updated, and they know there are no endpoint protection capabilities on IoT devices that can detect and remove the threats. Network operators, device manufacturers and users will need to remain vigilant to the security risks these devices present. The current lack of any security standards for IoT devices is certainly part of the problem that ought to be addressed. In particular, IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet. In this context, there may be a role for the government to provide appropriate guidance. It will be imperative for all relevant stakeholders to continue to work collaboratively to address and mitigate IoT security risks so that we can reap the benefits of this exciting and transformative technology.

Thank you again for the opportunity to testify and I look forward to taking your questions.

###

Mr. WALDEN. Mr. Drew, thank you for taking time out of your schedule to be here as well. We greatly appreciate it.

I now turn to Mr. Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University; lecturer and fellow, Harvard Kennedy School of Government; and special adviser to IBM Security.

Mr. Schneier, thank you for being here. We look forward to your testimony, sir.

## STATEMENT OF BRUCE SCHNEIER

Mr. SCHNEIER. Thank you, Chairman Walden, Chairman Burgess, Ranking Members Eshoo and Schakowsky. Committee members, thank you for having me and thank you for having this, I think, very important hearing.

I am Bruce Schneier. I am a security technologist. And while I have an affiliation with both Harvard and IBM, I am not speaking for any of them and I am not sure they know I am here.

Mr. WALDEN. It is a secret. Nobody on the Internet knows either.

Mr. SCHNEIER. As the chairman pointed out, there are now computers in everything, but I want to suggest another way of thinking about it, in that everything is now a computer. This is not a phone, this is a computer that makes phone calls; or a refrigerator is a computer that keeps things cold; an ATM machine is a computer with money inside. Your car is not a mechanical device with computers, but a computer with four wheels and an engine, actually, a hundred-computer distributed system with four wheels and an engine. And this is the Internet of Things, and this is what caused the DDoS attack we are talking about.

I come from the world of computer security, and that is now everything security. So I want to give you four truths from my world that now apply to everything.

First, attack is easier than defense for a whole bunch of reasons. The one that matters here is that complexity is the worst enemy of security. Complex systems are hard to secure for an hour's worth of reasons, and this is especially true for computers and the Internet. The Internet is the most complex machine mankind has ever built by a lot and it is hard to secure. Attackers have the advantage.

Two, there are new vulnerabilities in the interconnections. The more we connect things to each other, the more vulnerabilities in one thing affect other things. We are talking about vulnerabilities in digital video recorders and Web cams that allowed hackers to take down Web sites. There are stories of vulnerabilities in a particular account.

One story. A vulnerability in an Amazon account allowed hackers to get to an Apple account, which allowed them to get to a Gmail account, which allowed them to get to a Twitter account. Target Corporation, you remember that attack. That was a vulnerability in their HVAC contractor that allowed attackers to get into Target. And vulnerabilities like these are hard to fix because no one system might be at fault. There might be two secure things come together and create insecurity.

Truism three: The Internet empowers attackers, attack scale. The Internet is a massive tool for making things more efficient, and that is also true for attacking. The Internet allows attacks to scale to a degree impossible otherwise. We are talking about millions of devices harnessed to attack Dyn, and that code, which somebody smart-wrote, has been made public. Now anybody can use it. It is in a couple of dozen botnets right now. Any of you can rent time on one on the dark Web to attack somebody else. I don't recommend it, but it can be done. And this is more dangerous as our systems get more critical.

The Dyn attack was benign, a couple of Web sites went down. The Internet of Things affects the world in a direct and physical manner: Cars, appliances, thermostats, airplanes. There are real risks to life and property and there are real catastrophic risks.

The fourth truism: The economics don't trickle down. Our computers are secure for a bunch of reasons. The engineers at Google, at Apple, at Microsoft spent a lot of time at this, but that doesn't happen for these cheaper devices. Ms. Eshoo has talked about this. These devices are lower profit margin, they are offshore, there are no teams, and a lot of them cannot be patched. Those DVRs, they are going to be vulnerable until someone throws them away, and that takes a while. We get security, because I get a new one of these every 18 months. Your DVR lasts for 5 years, your car for 10, your refrigerator 25. I am going to replace my thermostat approximately never.

So the market really can't fix this. The buyer and seller don't care. And Mr. Burgess pointed this out. The buyer and seller want a device that works. This is an economic externality. They don't know about it and it is not part of the decision. So I argue that Government has to get involved, that this is a market failure, and what I need are some good regulations. And there is a list of them, and Dr. Fu is going to talk about some of them, but this is not something the market can fix.

And to speak to Mr. Walden's point, I mean, yes, I am saying that a U.S.-only regulatory system will affect the products in the world, because this is software. Companies will make one software and sell it everywhere, just like, you know, automobile emissions control laws in California affect the rest of the country. It makes no sense for anybody to come up with two versions. And I think this is going to be important, because for the first time, the Internet affects the world in a direct and physical manner.

And the second point I want to make very quickly is we need to resist the FBI's calls to weaken these devices in their attempt to solve crimes. We have to prioritize security over surveillance. It was OK when it was fun and games, but now, you know, already this stuff on this device that monitors my medical condition, controls my thermostat, talks to my car, I mean, I have just crossed four regulatory agencies and it is not even 11 o'clock.

This is going to be something that we are going to need to do something new about. And like many new technologies in the 20th century, new agencies were created: Trains, cars, airplanes, radio, nuclear power. My guess is this is going to be one of them, and that is because this is different. This is all coming. Whether we like it or not, the technology is coming. It is coming faster than we think. I think Government involvement is coming, and I would like to get ahead of it. I would like to start thinking about what this would look like. And we are now at the point, I think, where we need to start making moral and ethical and political decisions about how these things worked.

When it didn't matter, when it was Facebook, when it was Twitter, when it was email, it was OK to let programmers, to give them the special right to code the world as they saw fit. We were able to do that. But now that it is the world of dangerous things, that is, cars and planes and medical devices and everything else, that maybe we can't do that anymore. And I don't like this. I like the world where the Internet can do whatever it wants whenever it wants at all times. It is fun. This is a fun device. But I am not sure we can do that anymore.

So thank you very much, and I look forward to questions.

[The prepared statement of Mr. Schneier follows:]

**Testimony of Bruce Schneier**
**Fellow, Berkman-Klein Center at Harvard University**
**Lecturer and Fellow, Harvard Kennedy School of Government**
**Special Advisor to IBM Security and CTO of Resilient: An IBM Company**

**Before the**

**U.S. House of Representatives**
**Committee on Energy and Commerce**
**Subcommittee on Communications and Technology, and the**
**Subcommittee on Commerce, Manufacturing, and Trade**

**Joint Hearing Entitled**
**"Understanding the Role of Connected Devices in Recent Cyber Attacks"**

**November 16, 2016**
**10:00 AM**

Good morning. Chairmen Walden and Burgess, Ranking Members Eshoo and Schakowsky, members of the committee: thank you for the opportunity to testify on this matter. Although I have an affiliation with both Harvard University and IBM, I am testifying in my personal capacity as a cybersecurity expert and nothing I say should be construed as the official position of either of those organizations.

I have worked in Internet security since the mid-1990s. I write books, articles, essays, and academic papers. I teach at the Harvard Kennedy School of Government. I give talks all over the world. I have testified before Congress before, and have served on several national and international committees on these topics.

Last month, popular websites like Twitter, Pinterest, Reddit and PayPal went down for most of a day. The distributed denial-of-service attack that caused the outages, and the vulnerabilities that made the attack possible, was as much a failure of market and policy as it was of technology. If we want to secure our increasingly computerized and connected world, we need more government involvement in the security of the "Internet of Things" and increased regulation of what are now critical and life-threatening technologies. It's no longer a question of if, it's a question of when.

First, the facts. Those websites went down because their domain name provider — a company named Dyn — was forced offline. We don't know who perpetrated that attack, but it could have easily been a lone hacker. Whoever it was launched a distributed denial-of-service attack against Dyn by exploiting a vulnerability in large numbers — possibly millions — of Internet-of-Things devices like webcams and digital video recorders, then recruiting them all into a single botnet. The botnet bombarded Dyn with traffic, so much that it went down. And when it went down, so did dozens of websites.

DDoS attacks are neither new nor sophisticated. The attacker sends a massive amount of traffic, causing the victim's system to slow to a crawl and eventually crash. There are more or less clever variants, but basically, it's a datapipe-size battle between attacker and victim. If the defender has a larger capacity to receive and process data, he or she will win. If the attacker can throw more data than the victim can process, he or she will win.

The attacker can build a giant data cannon, but that's expensive. It is much smarter to recruit millions of innocent computers on the internet. This is the "distributed" part of the DDoS attack, and pretty much how it's worked for decades. Cybercriminals infect innocent computers around the internet and recruit them into a botnet. They then target that botnet against a single victim.

You can imagine how it might work in the real world. If I can trick tens of thousands of others to order pizzas to be delivered to your house at the same time, I can clog up your street and prevent any legitimate traffic from getting through. If I can trick many millions, I might be able to crush your house from the weight. That's a DDoS attack — it's simple brute force.

Because of these attacks, your security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you've never heard of to consumers who don't care about your security.

I want to focus on the particulars of this attack, but the general vulnerabilities from these Internet-of-Things devices. In many ways, the Dyn attack was benign. Some websites went offline for a while. No one was killed. No property was destroyed. But computers have permeated our lives. The Internet now affects the world in a direct physical manner. The Internet of Things is bringing computerization and connectivity to many tens of millions of devices worldwide. We are connecting cars, drones, medical devices, and home thermostats. What was once benign is now dangerous.

Insecurities abound. It is no longer surprising when security researchers demonstrate that cars can be disabled remotely over the Internet. We have seen ransomare against Internet-enabled thermostats, and hacks against computerized medical devices. We know that our computerized election machines are insecure, and that we can be eavesdropped on through our Internet-enabled televisions. These devices are proliferating, and they're vulnerable.

The technical reasons that Internet-of-Things computers are insecure is complicated, but there is a fundamental market failure at work. Basically, the market has prioritized features and cost over security. Many of these devices are low-cost, designed and built offshore, then rebranded and resold. The teams building these devices don't have the security expertise we've come to expect from the major computer and smartphone manufacturers, simply because the market won't stand for the additional costs that would require. Unlike your computer and smartphone, these devices don't get security updates, and many don't even have a way to be patched. And, unlike our computers and phones, they stay around. DVRs and cars last a decade. Refrigerators, twenty-five years. We expect to replace our home thermostats approximately never.

This is important. The vulnerability exploited in the Dyn attack was made public, and is now in over a dozen different botnets. There is no way to patch the CCTV cameras and DVRs that are being exploited, and those devices will remain on the Internet for years if not decades.

They'll remain in use because of an additional market failure: neither the seller nor the buyer of those devices cares about fixing the vulnerability. The owners of those devices don't care. They wanted a webcam — or thermostat, or refrigerator — with nice features at a good price. Even after they were recruited into this botnet, they still work fine — you can't even tell they were used in the attack. The sellers of those devices don't care: They've already moved on to selling newer and better models. There is no market solution because the insecurity primarily affects other people. It's a form of invisible pollution.

And, like pollution, the only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers, allowing companies like Dyn to sue them if their devices are used in DDoS attacks. The details would need to be carefully scoped, but either of these options would raise the cost of insecurity and give companies incentives to spend money making their devices secure.

Most importantly, the government needs to resist the urge to deliberately weaken the security of any computing devices at the request of the FBI. Devices like smart phones are becoming the de facto digital hub where we control many of our Internet-of-Things devices.

Attempts to weaken encryption will make these attacks easier and more damaging, and will harm our society far more than their benefit to FBI investigations. Invest in FBI cybersecurity expertise, not back doors.

It's true that this is a domestic solution to an international problem and that there's no U.S. regulation that will affect, say, an Asian-made product sold in South America, even though that product could still be used to take down U.S. websites. But the main costs in making software come from development. If the United States and perhaps a few other major markets implement strong Internet-security regulations on IoT devices, manufacturers will be forced to upgrade their security if they want to sell to those markets. And any improvements they make in their software will be available in their products wherever they are sold, simply because it makes no sense to maintain two different versions of the software. This is truly an area where the actions of a few countries can drive worldwide change.

Regardless of what you think about regulation vs. market solutions, I believe there is no choice. Governments will get involved in the IoT, because the risks are too great and the stakes are too high. Computers are now able to affect our world in a direct and physical manner.

Security researchers have demonstrated the ability to remotely take control of Internet-enabled cars. They've demonstrated ransomware against home thermostats and exposed vulnerabilities in implanted medical devices. They've hacked voting machines and power plants. In one recent paper, researchers showed how a vulnerability in smart lightbulbs could be used to start a chain reaction, resulting in them *all* being controlled by the attackers — that's every one in a city. Security flaws in these things could mean people dying and property being destroyed.

Nothing motivates the U.S. government like fear. In 2001, a small-government Republican president created the Department of Homeland Security. A fatal IoT disaster will similarly spur our government into action, and it's unlikely to be well-considered and thoughtful action. Our choice isn't between government involvement and no government involvement. Our choice is between smarter government involvement and stupider government involvement. We have to start thinking about this now. Regulations are necessary, important and complex — and they're coming. We can't afford to ignore these issues until it's too late.

Letting the market figure out optimal security levels was okay when software didn't matter. But it is fundamentally different when a spreadsheet crashes and you lose your data and when your car crashes and you lose your life. The security vulnerabilities in the Internet of Things are deep and pervasive, and they won't get fixed if the market is left to sort it out for itself. We need to proactively discuss good regulatory solutions; otherwise, a disaster will impose bad ones on us.

Mr. WALDEN. Mr. Schneier, thank you very much. I appreciate your comments.

We will now go to Dr. Kevin Fu, CEO of Virta Labs and associate professor, Department of Electrical Engineering and Computer Science, at the University of Michigan.

Dr. Fu, thank you for joining us. Please go ahead.

## STATEMENT OF KEVIN FU

Dr. FU. Good morning, Chairmen Walden, Burgess, Ranking Member Eshoo and Schakowsky, and distinguished members of the joint committee.

My name is Kevin Fu. I represent the academic cybersecurity research community. I am at the University of Michigan, where I conduct research on embedded security. My laboratory discovers how to protect computers built into everyday objects, ranging from mobile phones and smart thermostats to pacemakers and automotive airbags. I am also CEO and cofounder of the healthcare cybersecurity startup Virta Labs.

I am testifying before you today on the insecurity of the Internet of Things as related to the recent attacks on Dyn. I will provide a perspective on the evolving cybersecurity risks framed in the broader societal context. In short, IoT security remains woefully inadequate. None of these attacks are new. None of these attacks are fundamentally new, but the sophistication, the scale of disruption, and the impact on infrastructure is unprecedented.

Let me make some observations. We are in this sorry and deteriorating state because there is almost no cost to a manufacturer for deploying products with poor cybersecurity to consumers. Has a consensus body or Federal agency issued a meaningful IoT security standard? Not yet. Is there a national testing lab to verify and assess the premarket security of IoT devices? No. Is there tangible cost to any company that puts an insecure IoT device into the market? I don't think so.

So I would like to highlight eight observations about this IoT insecurity.

Number one, security needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an IoT device, it is too late for effective risk control.

Two, good security and bad security look the same at the surface.

Three, the healthcare community does not issue different advice for flu transmitted by cough versus flu transmitted by sneeze. Similarly, both connected and disconnected IoT devices carry significant cybersecurity risks, so it is important to consider both conditions.

Four, the millions of insecure IoT devices are just a small fraction of what the IoT market will resemble in 2020, and it will get much worse if these security problems remain unchecked.

Five, unlike inconvenient security problems for your tablets or notebook computers, IoT's insecurity puts human safety at risk, and innovative systems will not remain safe if they are not secure.

Six, I consider security a solution, not a problem. Better cybersecurity will enable new markets, promote innovation, and give consumers the confidence to use new technologies that improve the quality of life.

Seven, it may be surprising, but there are over 209,000 unfilled cybersecurity jobs in the USA, and that is just this country.

And eight, the Nation lacks an independent testing facility at the scale of a federally funded research and development center as a proving ground for testing premarket IoT cybersecurity crashworthiness and for testing embedded cybersecurity defenses.

Let me conclude with five recommendations to protect our national infrastructure.

Number one, incentivize built-in basic cybersecurity hygiene by establishing meaningful milestones encouraging use of strong cryptography in these products.

Two, support agencies such as the National Science Foundation, the National Institute of Standards and Technology, to advance our understanding of IoT security and to train the hundreds of thousands of students necessary for a robust cybersecurity workforce.

Three, study the feasibility of standing up an independent national embedded cybersecurity testing facility modeled after, for instance, post-incident initiatives, such as the National Transportation Safety Board; incident prevention initiatives, such as the National Highway Traffic Safety Administration, NHTSA; and then more unusual places like the survivability and destruction testing at the Nevada National Security Site.

Number four, I recommend leveraging the existing cybersecurity expertise with an agency such as NIST, NSF, DHS, and DARPA.

And finally, five, I believe that universities, industry, and the Government must find the strength and the resolve for protecting our national infrastructure through partnerships, and that investments in embedded cybersecurity will pay great dividends to our society and our economy.

I would like to close, just thank you for the invitation to testify on what I think is a very important subject for our country. The committee can also find photos of illustrative IoT problems in water treatment facilities, hospitals and more in the appendix of my written testimony. And I would be happy to take your questions. Thank you.

[The prepared statement of Dr. Fu follows:]

STATEMENT OF PROF. KEVIN FU, PH.D.

DEPARTMENT OF
ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI

CEO, VIRTA LABORATORIES, INC
ANN ARBOR, MI

# INFRASTRUCTURE DISRUPTION:
# INTERNET OF THINGS SECURITY

SUBMITTED TO THE
U.S. HOUSE ENERGY AND COMMERCE COMMITTEE

SUBCOMMITTEE ON COMMUNICATIONS AND
TECHNOLOGY & SUBCOMMITTEE ON COMMERCE,
MANUFACTURING, AND TRADE
JOINT HEARING ON

UNDERSTANDING THE ROLE OF CONNECTED DEVICES
IN RECENT CYBER ATTACKS

WEDNESDAY, NOVEMBER 16, 2016

## 1 Introduction

Good morning, Chairman Walden, Chairman Burgess, Ranking Member Eshoo, Ranking Member Schakowsky, and distinguished members of the Committee. I am testifying before you today on the insecurity of the Internet of Things (IoT) as related the recent attacks on Dyn. I will provide a perspective on the evolving cybersecurity risks and frame the issues in broader societal context. In the appendix of my written testimony, you can also find photographs and stories of problematic IoT devices where I invite your questions. In short, IoT security remains woefully inadequate, and the Dyn attack is a sign of worse pains to come. None of these attacks are new, but the sophistication, scale of disruption, and impact on infrastructure is unprecedented[1]. Cybersecurity needs to be built into IoT devices, not bolted on after the fact. I will close with a summary and recommendations on what can be done to improve IoT security and innovation.

**Credentials and experience.** My name is Dr. Kevin Fu. I represent the academic cybersecurity research community. I am Associate Professor of Electrical Engineering & Computer Science at the University of Michigan where I conduct research on embedded security, the discipline of protecting computers built into every day objects ranging from mobile phones and smart thermostats to pacemakers and automotive airbags. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from M.I.T.'s Department of Electrical Engineering and Computer Science. Michigan teaches programming to over 1,300 undergraduates each year, and we teach a rigorous course in computer security to 440 undergraduates each year. I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of any of my past or present sponsors or employers.

[1] The earliest prediction of IoT problems I have found is from 1995 on page 22 of the MIT Voodoo Humor Magazine on Internet-enabled lightbulbs. `http://web.mit.edu/voodoo/www/archive/pdfs/1995-Fall.pdf`

## 2 Observations and Recommendations

In this testimony, I'd like to make the following observations and recommendations.

1. Security needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an IoT device, it's too late for effective risk control.

2. Good security and bad security look the same at the surface. Default passwords are pervasive and harmful. Testing is an essential part of security, but a complete security development lifecycle is necessary to effectively defend against increasingly sophisticated threats.

3. Focus on *exposure* to cybersecurity risks rather than merely "connectedness."

4. For IoT devices already deployed, take joy that the millions of insecure IoT devices are just a small fraction of what the IoT market will resemble in 2020.

5. Unlike inconvenient security problems for your tablet or notebook computer, IoT insecurity puts human safety at risk. Innovative systems will not be safe if they are not secure. Human factors may impact IoT security more so than the technology. For instance, poor user interfaces may encourage consumers to make unwise security decisions.

6. Security is a solution, not a problem. Better cybersecurity will enable new markets, promote innovation, and give consumers confidence to use new technologies that improve the quality of life. Poor security will likely cause the IoT market to eventually collapse on itself as consumers begin to lose trust in technology from compilations of horror stories.

7. There are tens of thousands of unfilled cybersecurity jobs in the USA. Existing approaches are insufficient to train a large enough work force to counter growing cybersecurity threats against IoT devices, our economy, and infrastructure.

8. The nation lacks independent, FFRDC-scale testing facilities akin to the NTSB (postmarket), automotive crash safety testing (premarket), or NNSS (destruction and survivability testing) to provide a proving ground for embedded cybersecurity defenses needed by IoT.

My recommendations aim to ensure that insecure IoT technology does not put our national infrastructure, hospitals, and homes at risk.

1. Incentivize built-in, basic cybersecurity hygiene for IoT devices by establishing meaningful security milestones and encouraging use of strong cryptography.
2. Support agencies such as NIST and NSF to advance our understanding of how to protect IoT devices and to establish a cybersecurity workforce that meets industry needs.
3. Study the feasibility of standing up an independent, national embedded cybersecurity testing facility modeled after the NTSB, automotive crash safety testing, or the Nevada National Security Site.
4. Leverage the existing cybersecurity expertise within NIST's National Cybersecurity Center of Excellence (CCoE) and Information Security and Privacy Advisory Board (ISPAB).
5. To meet national cybersecurity workforce shortfalls and protect our national infrastructure, universities, industry, and government must find the strength and resolve to invest in embedded cybersecurity with interdisciplinary science and engineering, industrial partnerships for research and education, and service to the nation.

## 3 Why All the Fuss about Internet of Things Security?

None of these risks are new. Researchers have known about these flaws for decades. What's new is the scale and ease of attack because of the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers.

To put the Dyn attack in perspective, think back to the 1980s when a person might dial the operator to ask, "Please connect me to Alice." The operator looks in a directory, finds the phone number, then connects the caller to Alice. If only a few people call the operator in a period of time, there is no problem. If 100,000 compromised IoT devices make this simple query simultaneously, the operator will be overwhelmed. Legitimate callers will likely receive a busy tone. That is essentially what happened to Dyn. An overwhelming number of insecure IoT devices were tricked into making directory queries to Dyn.

**Think exposure, not connectedness.** The term "networked" and "connected" are red herrings in the long term because both terms hint at a perimeter-based security model. There are no effective network perimeters because IoT devices are notorious for piercing perimeters. Moreover, a device can be partially connected. The healthcare community does not issue different guidance for flu transmitted by cough versus flu transmitted by sneeze. Therefore, the cybersecurity community should not limit its thinking to just networks and connectivity. A network is not necessary for a cybersecurity exploit; malware gets in just fine by unhygienic USB drives carried by unwitting personnel. Hackers continue to use social engineering by telephone to trick personnel into giving out unauthorized remote access. Rather than focus on *connected* devices, a more comprehensive approach would examine *exposed* devices. Focus on outcomes, not modalities. I recommend using language such as "exposed to cybersecurity risk" instead of "networked" or "connected" when discussing overall objectives because cybersecurity threats are constantly evolving.

**Complexity breads insecurity.** In my role as a member of the Computing Community Consortium (CCC) Council, I recognize the painful challenges of IoT security. One of the core problems with the increasing number of IoT devices is the increased complexity that is required to operate them safely and securely. This increased complexity creates new safety, security, privacy, and usability challenges far beyond the difficult challenges individuals face just securing a single device.

## 4 Examples of IoT Security Problems

Many of the security problems in IoT devices are attributable to lack of proper security engineering during early design, but IoT devices also pose risks quite different in nature from traditional computing. While both traditional computing and IoT devices suffer from poor cyberhygiene such as the use of factory-set default passwords, IoT devices tend to have safety consequences or involve physical manipulation of the world that could more easily lead to harm.

**National Vulnerability Database.** The NVD now includes a category for IoT devices. NIST quantifies risks of IoT vulnerabilities, and some of the results appear in the Common Vulnerabilities and Exposures (CVE) database. Relevant to the Dyn attack, a DDoS vulnerability was scored in 2009 for a connected coffee pot (CVE-2008-7174), vehicle vulnerabilities, (CVE-2015-5611, Jeep Chrysler vehicle) and medical devices (CVE-2011-3386, Medtronic insulin pump).

**Internet-connected home security cameras.** The irony is not lost on me that security cameras have created an unwitting army of network bandwidth weaponry. I built my own home security system and implanted home-made wirelessly powered sensors in the concrete foundation of my house because I found that most security cameras have unverified or weak security. For instance, one foreign manufacturer is a common OEM that supplies software to a number of popular security camera products sold in the USA. This particular software was vulnerable to a remote root exploit, which means an attacker can take total control of the system via the Internet. When the software manufacturer issued a patch to fix the security problem, the software malfunctioned and consumers were forced to undo the patch. The manufacturer has since removed the patch, and provides no mitigating security solution. Consumers are stuck with insecure security cameras.

**Hospitals and healthcare delivery.** The number one cybersecurity problem for hospitals is how to ensure continuity of clinical operations to deliver safe and timely patient care. Note that security is a means to an end: delivery of care. The healthcare community dodged the bullet on the Dyn attack. Hospitals survived not by design, but by luck. The adversary did not target healthcare. This time. Dyn represents a single point of failure for resolving Internet names, but hospitals have other kinds of single points of failure. For instance, heating and ventilation now resembles IoT with unpatched computers controlling negative pressure in units with highly infectious diseases. Elevators systems run on embedded computers, where there is little understanding of defensive technology. A number of hospitals expressed concern about IoT devices, and no one has been able to provide assurance that a future Dyn-like attack will not cause a massive, nation-wide healthcare outage.

The best known approach is to maintain a more accurate, risk-based inventory of devices, software, and cyberexposure such that when a new vulnerability is discovered, hospitals can more quickly identify affected devices to triage and remediate. However, hospitals simply do not have accurate inventories of software in actual use. In my experience, we usually find "shadow IT" on hospital networks. That is, contraband computing enters hospital infrastructure in unusual ways.

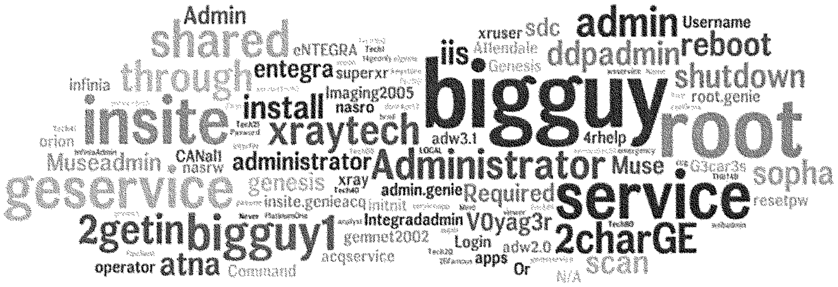


Figure 1: One medical device manufacturer had 35 CVEs and 125+ sets of exposed credentials. This word cloud, courtesy of Scott Erven, describes common default passwords from a single medical device manufacturer. Default passwords on cameras and other IoT devices enabled attackers to direct a tsunami of network traffic at Dyn. Similar default password risks exist for medical devices.

**Medical device security.** Default passwords and the inability to tolerate intrinsically hostile networks are two common problems in medical IoT devices. Another unusual problem with medical devices is that traditional cryptography does not work as easily on battery-powered, implantable devices because of the risks of cryptographic computations draining the battery. When an implant's battery runs low, it requires surgical replacement. For this reason, NIST's effort on lightweight cryptography is especially important. More information about medical device security appears at `medicalsecurity101.org` and `secure-medicine.org`.

**No Fire and Forget.** There is no fire and forget for IoT security. Threats and vulnerabilities constantly change. Therefore, any solution based solely on manufacturing is doomed to failure. Software effectively ages because of shifting threats, and there will always be a need for vigilance and updates/maintenance. NIST produced a cybersecurity framework for industrial control systems that may apply well to IoT security. NIST recommends to first (1) assess cybersecurity risks of inventory, (2) deploy compensating controls that address specific risks, and (3) continuously monitor the effectiveness of the controls as threats change.

## 5 Why IoT Needs Embedded Cybersecurity

Embedded cybersecurity represents a rapidly growing area in terms of educational opportunities, research questions, talent demand, and federal policy for science and engineering. Safety critical systems such as automobiles, airplanes, and medical devices depend on embedded cybersecurity. The market size for securing the Internet of Things is predicted to reach $37B by 2021. While there are pockets of cybersecurity research and education programs across the country, the nation lacks an independent testing facility that can begin to model complex behavior of interoperable devices in homes, hospitals, transportation, etc. Moreover, industries will require a highly skilled workforce for embedded security as they discover that security solutions are needed before consumers will gain confidence in innovative new technologies like self-driving cars and sensors that wirelessly command medical devices to delivery therapy.

**Assessing medical IoT security.** The Mayo Clinic reportedly spends roughly $300K per medical device to perform security assessment, and they have thousands of models of devices. It makes little economic sense to have individual hospitals testing the security of devices that ought to remain secure for all 6,000 hospitals in the USA. Cybersecurity ought to be a public good much like automobile safety. Imagine if every car dealer were individually responsible for crash testing automobiles: costs would skyrocket and the public would have little confidence. A facility for embedded cybersecurity at the scale of a hospital could provide testing to both government and industry, while allowing students to conduct innovative research during surplus time.

**National embedded cybersecurity testing facility.** Neither industry nor government have the capability to safely conduct thorough security testing and assessment on IoT devices spanning healthcare to transportation. The cost to establish a realistic test facility for healthcare IoT cybersecurity, for instance, is likely to exceed $1.1 billion because of the sheer complexity and specialized equipment. But that is much cheaper and more effective than having 6,000 hospitals across 50 states each attempting to establish tiny facilities.

## 6 National Activities on IoT Security

Federal agencies such as NIST and NSF have a number of initiatives aimed at improving IoT security. The Computing Research Association's CCC Council has also produced a number of IoT security recommendations on behalf of the computing community. Below I provide references to such documents at various stages of maturity to improve IoT security.

- The Computing Research Association primer on IoT policy and its role in innovation. `http://cra.org/govaffairs/wp-content/uploads/sites/6/2016/02/IoT-Policy-Document.pdf`

- *Systems Computing Challenges in the Internet of Things* by the CCC Council explains that existing best practices in building robust and secure systems are insufficient to address the new security challenges that IoT systems will present.
  `http://cra.org/ccc/wp-content/uploads/sites/2/2015/09/IoTSystemsChallenges.pdf`

- NIST published a widely cited document on cybersecurity for industrial control systems, and one of the draft standards on lightweight cryptography is designed for the especially constrained environment of IoT devices.
  `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf`
  `http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf`

- NIST published *Special Publication 800-183: Networks of "Things"* as a framework to guide engineers responsible for securing IoT technology.
  `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf`

- NIST has created a small number of projects to solve security problems in certain high priority IoT technologies such as smart home devices, medical infusion pumps, and manu-

facturing industrial control systems. http://tinyurl.com/zlhl653
https://nccoe.nist.gov/projects/use_cases/medical_devices
https://nccoe.nist.gov/projects/use_cases/manufacturing

- NSF highlighted a number of projects related to IoT security with application to cars, medical devices, and voting machines.
  https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=136601

Thank you. I would be happy to respond to any questions you may have, especially on how IoT security impacts hospitals and medical devices.

## Biography

Dr. Kevin Fu, Ph.D., is Associate Professor of Electrical Engineering and Computer Science at the University of Michigan and CEO and co-founder of healthcare cybersecurity startup Virta Laboratories, Inc. His research investigates how to achieve trustworthy computing on embedded devices with application to health care, commerce, and communication. He teaches computer science courses in security and privacy. Virta Labs provides hospitals a managed cybersecurity service called BlueFlow to assure continuity of clinical operations despite medical device security risks.

Fu received his Ph.D. in EECS from MIT where his research pertained to secure storage and how web authentication fails. His participation in the provocative 2008 research paper [12] analyzing the security of a pacemaker/defibrillator led to a wake-up call for cybersecurity in medical device manufacturing.

Fu has given nearly 100 invited talks on medical device security to industry, government, and academia—including Senate and House hearings, the Institute of Medicine, and National Academy of Engineering events. He directs the Archimedes Center for Medical Device Security at the University of Michigan. He co-chaired the AAMI Working Group on Medical Device Security, which led to the the AAMI TIR57 document that advises medical device manufacturers on how to incorporate security engineering into medical device product development. Fu co-authored the NIST Information Security and Privacy Advisory Board recommendations [16] to HHS on how the federal government must adapt to risks of medical device security. His medical device security efforts were recognized with a Fed100 Award, Sloan Research Fellowship, NSF CAREER Award, MIT TR35 Innovator of the Year award, and best paper awards on medical device security by organizations such as IEEE and ACM [2, 13, 10, 6, 7, 3, 15, 14, 5, 4, 11, 1, 9, 17, 8].

Fu served as a visiting scientist on cybersecurity research at the U.S. Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. He was a member the NIST Information Security and Privacy Advisory Board. ISPAB is a Federal Advisory Committee that identifies emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in Federal Government information systems.

## References

[1] W. P. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proceedings of the 49th Design Automation Conference*, DAC '12, June 2012. Invited paper `https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf`.

[2] S. S. Clark and K. Fu. Recent results in computer security for medical devices. In *International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth), Special Session on Advances in Wireless Implanted Devices*, Oct. 2011. `https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf`.

[3] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), Jan. 2008. `https://web.eecs.umich.edu/~kevinfu/papers/whitepaper-protecting_global_medical.pdf`.

[4] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proceedings of USENIX Workshop on Hot Topics in Security (HotSec)*, July 2008. `https://spqr.eecs.umich.edu/papers/watchdog-hotsec08.pdf`.

[5] K. Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009. `http://www.csl.sri.com/users/neumann/insiderisks08.html#218`.

[6] K. Fu. Software issues for the medical device approval process, Apr. 2011. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011 `https://spqr.eecs.umich.edu/papers/fu-senate-comm-aging-med-dev-sw-apr-2011.pdf`.

[7] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, Washington, DC, July 2011. IOM (Institute of Medicine), National Academies Press `https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf`.

[8] K. Fu. On the technical debt of medical device security. Technical report, National Academy of Engineering FOE, Sept. 2015. `http://www.naefrontiers.org/File.aspx?id=50750`. A version appeared in the National Academy of Engineering's *The Bridge*, Winter 2016.

[9] K. Fu and J. Blum. Inside risks: Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10):21–23, Oct. 2013. http://www.csl.sri.com/users/neumann/cacm231.pdf.

[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, Aug. 2011. https://spqr.eecs.umich.edu/papers/gollakota-SIGCOMM11-IMD.pdf.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1):30–39, Jan. 2008. https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf.

[12] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, pages 129–142, May 2008. https://www.secure-medicine.org/public/publications/icd-study.pdf.

[13] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, Aug. 2011. https://spqr.eecs.umich.edu/papers/hanna-aed-healthsec11.pdf.

[14] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart Rhythm Journal*, 6(10):1432–1436, Oct. 2009. http://bit.ly/1NEk3dR or http://download.journals.elsevierhealth.com/pdfs/journals/1547-5271/PIIS1547527109007401.pdf.

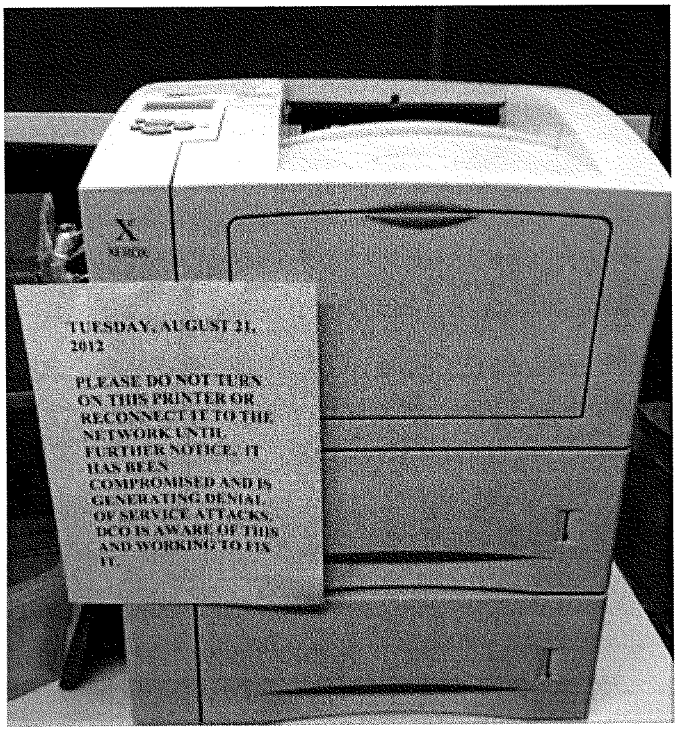
[15] A. D. Molina, M. Salajegheh, and K. Fu. HICCUPS: Health information collaborative collection using privacy and security. In *Proceedings of the Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 21–30. ACM Press, Nov. 2009.

[16] NIST ISPAB federal advisory commmittee recommendations on improving medical device cybersecurity, 2012. Sent to OMB Director, HHS Secretary, NSC, DHS, NIST, March 30, 2012 http://1.usa.gov/1qlnh0X or http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf.

[17] M. Salajegheh, A. Molina, and K. Fu. Privacy of home telemedicine: Encryption is not enough. *Journal of Medical Devices*, 3(2), Apr. 2009. Design of Medical Devices Conference Abstracts https://spqr.eecs.umich.edu/papers/salajegheh-DMD09-abstract.pdf.

## Appendix: Photographs of IoT Failures

In my travels, it disturbs me to find so many everyday devices as well as safety-critical devices without adequate cybersecurity controls.



TUESDAY, AUGUST 21, 2012

PLEASE DO NOT TURN ON THIS PRINTER OR RECONNECT IT TO THE NETWORK UNTIL FURTHER NOTICE. IT HAS BEEN COMPROMISED AND IS GENERATING DENIAL OF SERVICE ATTACKS. DCO IS AWARE OF THIS AND WORKING TO FIX IT.

Figure 2: A smaller scale precursor to the Dyn DDoS attack, this printer at the University of Michigan was infected by network-based malware and began to generate denial of service attacks against other institutions.

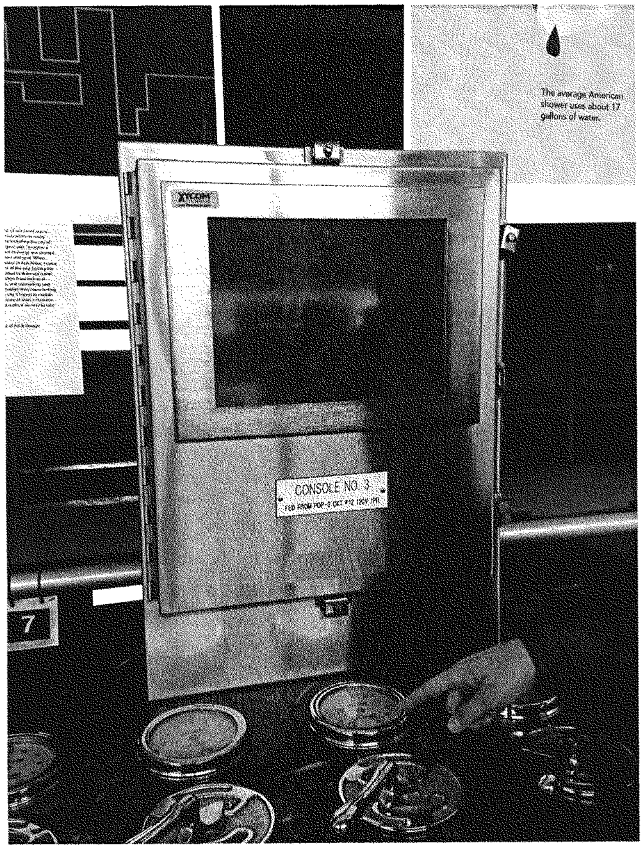
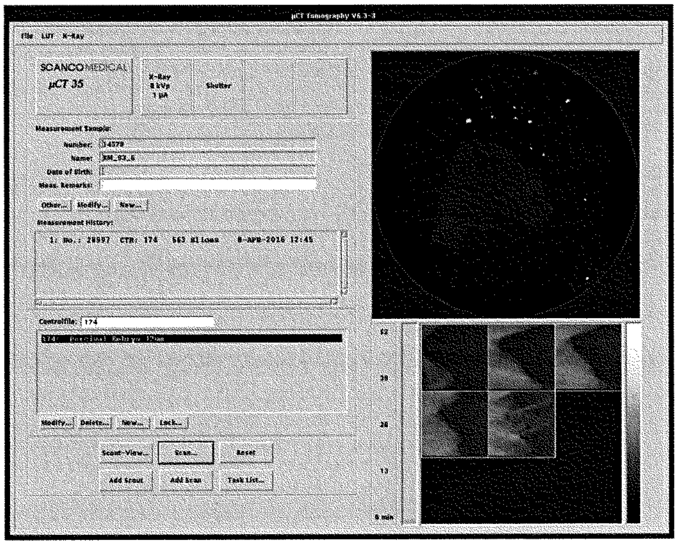


Figure 3: This water treatment facility in Michigan depends on insecure Windows XP for its water pump controls. In my photograph, you can see the Windows XP logo. Note that Windows XP ended security patch maintenance several years ago, and customers were advised of the expiration date before making purchases of the software. Windows XP machines are trivially compromised because there are no security fixes available and perimeter-based security provides little assurance.



X-Ray
8 kVp
1 µA

Measurement Sample:

Number: 14578

Name: XM_83_6

Date of Birth:

Meas. Remarks:

Measurement History:

```
1: No.: 28997  CTR: 174   563 Slices   8-APR-2016 12:45
```

Controlfile: 174

174: [illegible]

Figure 4: A researcher on Twitter claims to have discovered a tomography machine on the Internet by using the Shodan IoT vulnerability search engine. I have insufficient information to verify, however, but it is quite plausible. IoT medical devices can be both victims and sources of DDoS attacks.

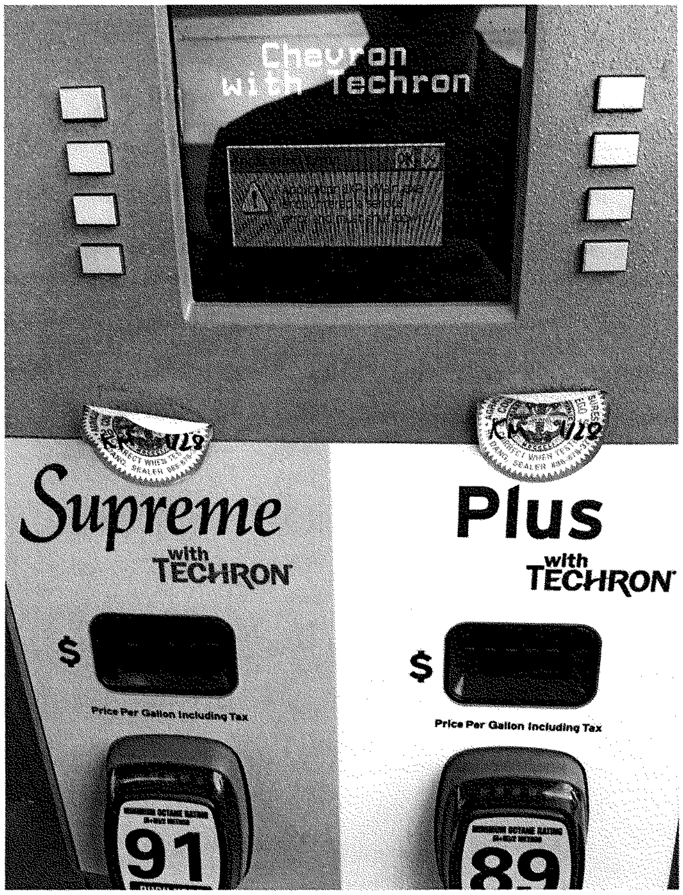
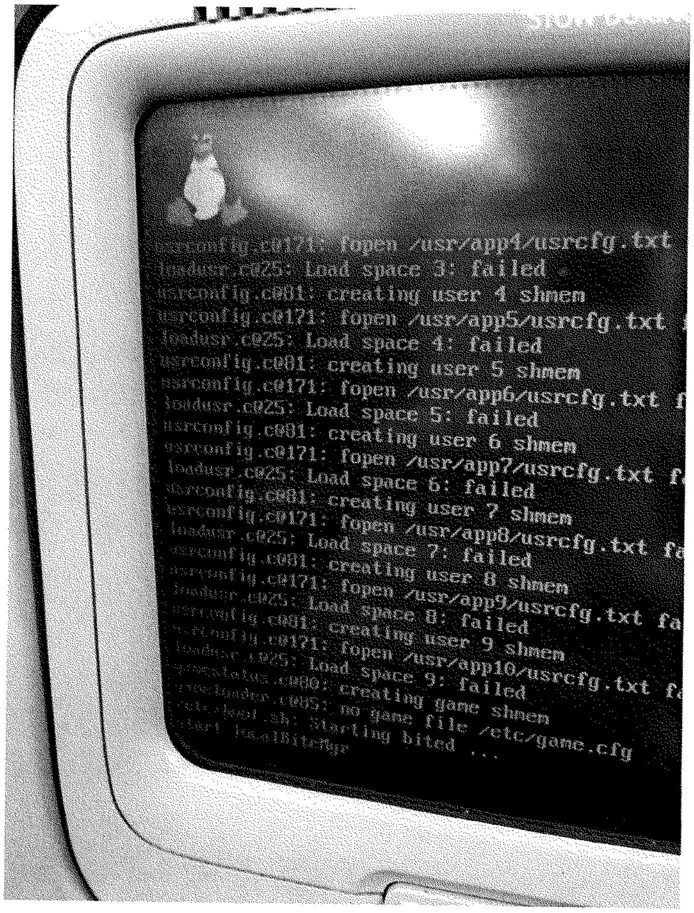

Chevron
with Techron
Supreme
with
TECHRON
Plus
with
TECHRON
$
Price Per Gallon Including Tax
$
Price Per Gallon Including Tax
91
89

Figure 5: I found this gas pump had crashed, and was unable to pay at the pump. Imagine if a virus knocked out every gas pump simultaneously in the nation, or if a chorus of infected gas pumps began to unwittingly mount DDoS attacks on critical infrastructure.



```
usrconfig.c@171: fopen /usr/app4/usrcfg.txt
loadusr.c@25: Load space 3: failed
usrconfig.c@81: creating user 4 shmem
usrconfig.c@171: fopen /usr/app5/usrcfg.txt
loadusr.c@25: Load space 4: failed
usrconfig.c@81: creating user 5 shmem
usrconfig.c@171: fopen /usr/app6/usrcfg.txt f
loadusr.c@25: Load space 5: failed
usrconfig.c@81: creating user 6 shmem
usrconfig.c@171: fopen /usr/app7/usrcfg.txt f
loadusr.c@25: Load space 6: failed
usrconfig.c@81: creating user 7 shmem
usrconfig.c@171: fopen /usr/app8/usrcfg.txt fa
loadusr.c@25: Load space 7: failed
usrconfig.c@81: creating user 8 shmem
usrconfig.c@171: fopen /usr/app9/usrcfg.txt fa
loadusr.c@25: Load space 8: failed
usrconfig.c@81: creating user 9 shmem
usrconfig.c@171: fopen /usr/app10/usrcfg.txt fa
loadusr.c@25: Load space 9: failed
gamestatus.c@80: creating game shmem
gameloader.c@85: no game file /etc/game.cfg
/etc/boot.sh: Starting bited ...
start localBiteMgr
```

Figure 6: This airplane entertainment system running Linux crashed on my plane. While entertainment is not safety critical, imagine if flight control systems accidentally had a pathway to the entertainment software. Automobiles used to separate entertainment systems from engine control. However, a programmer eventually mixed the two systems unwittingly, enabling hackers to take control of an automobile by infecting the entertainment system.

DEPARTURES
San Diego International Airport
ARRIVALS
ARRIVALS
Thursday July 16, 2015 6:56 AM
Thursday July 16, 2015 6:56 AM

Figure 7: Crashed flight display consoles are a common occurence in airports. Imagine if every smart TV in the world were simultaneously infected with a virus, sourcing a massive DDoS attack against a victim like Dyn.

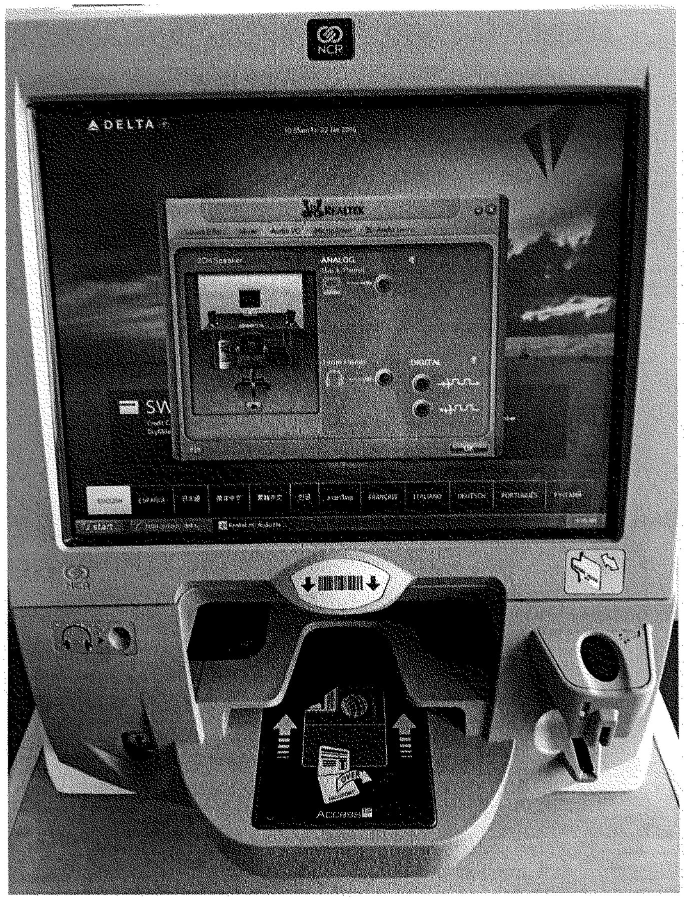


Figure 8: When checking in for a flight, I had difficulty because the boarding pass kiosk gave me a Windows GUI. Computing is everywhere, and we often forget how much we depend on hard-to-maintain software.

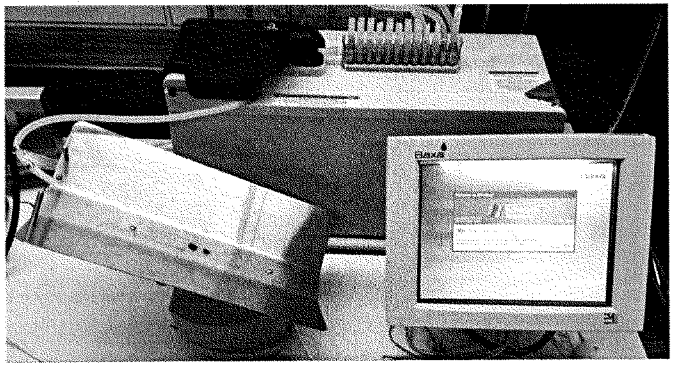
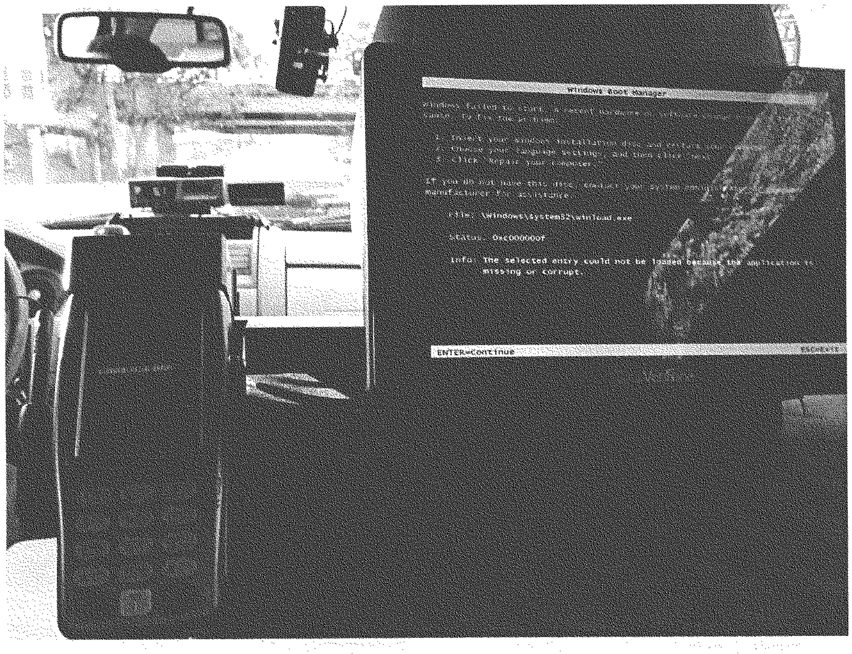


Figure 9: This is a pharmaceutical compounder from my lab at the University of Michigan. Hospitals use this device to mix custom, liquid drugs for IV delivery. FDA received a complaint that this model of compounder was infected with a virus. We found the machine to be running Windows XP, an insecure operating system. It was trivial to infect. A former employee of the company further explained that when the compounder was brought in for repair, the malware was accidentally spread to other compounders under repair.



```
                    Windows Boot Manager
Windows failed to start. A recent hardware or software change
cause. To fix the problem:

  1. Insert your Windows installation disc and restart your
  2. Choose your language settings, and then click "Next."
  3. Click "Repair your computer."

If you do not have this disc, contact your system administrator
manufacturer for assistance.

    File: \Windows\system32\winload.exe

    Status: 0xc000000f

    Info: The selected entry could not be loaded because the application is
          missing or corrupt.

ENTER=Continue                                                 ESC=Exit
```

Figure 10: Even taxi cabs run on Windows. For the moment, the payments systems are separate from the engine control unit. But history shows that engineering mistakes happen, and one could imagine a vulnerability in an IoT payment system that causes massive disruption of transportation.

Mr. WALDEN. Dr. Fu, thank you.

And thank you to all of our witnesses. This has been very enlightening. We greatly appreciate your testimony and your recommendations for our consideration.

I guess I will start with a couple of questions as we try and wrestle this issue. Over the last 6 years, we have done multiple hearings on cybersecurity threats to the United States. We have had multiple panels come before us and testify. And I think almost entirely they said, first, do no harm. Be careful when you lock things into statute because you can misallocate our resources and our opponents will know what we have to go do and we can't get out of it and they will just go do a workaround.

So how do we establish a framework that would both be appropriate here but have an effect internationally, because we don't make all the devices and we may have market power, but we are not the biggest market anymore? But how do we create a national framework where the stakeholders really are driving this in realtime and we don't do something stupid like lock certain requirements into statute?

Mr. Drew, can I start with you, and we will just work down the panel?

Mr. DREW. I think the best place to start is with standards. I think the best place to start is for us to define how we intend on solving this problem on the devices themselves. Industries have a number of standards with regards to how they operate these platforms once they purchase them, but they don't have standards on how they are supposed to be manufactured to be secure premarket.

So I believe if we were to start with standards and then apply pressure—so as an industry, I am under pressure to implement standards in order to be able to serve businesses and serve the consumers. I think if we start with that standard, then we are able to apply that pressure. And to the extent that pressure can be applied globally, I think that we can get some traction and some momentum before we have to start regulating.

Mr. WALDEN. All right.

Mr. Schneier?

Mr. SCHNEIER. I am also a fan of standards. And I think your question is a really important one, how do you do it properly as to not stifle innovation?

Mr. WALDEN. Right.

Mr. SCHNEIER. And I think the answer is to make them technologically invariant. And I tend to look at the pollution model as something—what works and what doesn't. And what works is, you know, here is the result we want. Figure out how to do it in the most cost-effective way possible, rather than legislate here's the process, here's the technology. The standard has to be technologically invariant.

And I heard, you know, you had a driverless car hearing yesterday, and I think it is somewhat similar. We are going to make standards on the driverless car manufacturers to do things properly, but we are going to assume an environment where there exists, you know, malicious cars out to get you. So we will have to deal with the rogue devices. We can't assume that everything on the Internet, or everything on the roads, is going to be benign and secure. But standards will raise the tide, but yes, we have to do them properly, because you do them wrong and it will stifle innovation. Do them right, I think it will help innovation.

Mr. WALDEN. All right.

Dr. Fu?

Dr. FU. Yes. I think there are ways you can do this effectively without stifling innovation. In fact, I believe that a well-designed cybersecurity framework will actually promote innovation. I will try to avoid the technical side, but I will just say, you know, of course, encoding mechanism would be unwise. For instance, if you decide to encode that all forms must be signed in blue ink, that didn't, you know, assume the existence of e-signatures in the future. So you should be very careful of encoding mechanism.

However, principles I think you can encode. I would actually say that NIST has done a relatively good job at encoding principles. There is no perfect standard. But it will be very difficult to build in security if we don't have these principles set in place. And it needs to have buy-in from industry. It needs to have Government leadership as well. But it is all about setting those principles, which many of which are already known for over 30 years in the cybersecurity community.

Mr. WALDEN. All right. Most helpful. The extent to which you all can think about this some more and give us kind of your ideas on how to actually get it to the right place. Because this is my concern, that if we are not careful, we lock something in, it is so hard to change statute.

And we don't want this to be an innovation killer in America. We actually want to lead on this and get it right. But, you know, I don't think I want my refrigerator talking to, you know, some food police somewhere, you know. It just is what it is. So we need to get this thing right. So thank you for being here.

At this point, I will return the balance of my time and turn to my friend and colleague who has been very involved in this, Ms. Eshoo, from California.

Ms. ESHOO. Thank you, Mr. Chairman.

And thank you to each one of you, the witnesses. I think you were absolutely terrific.

I have legislation that I introduced that speaks to this issue. It hasn't really gained much traction. But what you said today I think puts some wheels on it, because it is about security without damaging innovation.

We talk a lot about the attacks that take place, but we don't really focus on prevention. Throughout the Valley, Silicon Valley, no matter who I have met with, I have asked them the same question: What would you do about this? And to a person, they have spoken about hygiene, the lack of hygiene in systems, number one; and number two, the lack of good solid security management.

I don't think—let me put it in a positive. I think we need a Good Housekeeping Seal of Approval on this, and I think that—and my bill called for NIST to set the standards, not the Congress, because we really don't know anything about that. And we miss the mark, we will miss it by a wide mile. Exactly.

So I also think in listening to you, especially Mr. Schneier, that this is an issue that should be included in national infrastructure legislation, because this is part of our national infrastructure. And it deserves the kind of protection that you spoke to, because, as you said, everything is a computer, everything. It is not just the computers over at the DOD. We are carrying them around in our pockets, we are driving them, et cetera, et cetera.

So given that, what is the framework for it? How would both—Mr. Schneier and Dr. Fu and Mr. Drew, what would it look like? What would it look like? I am giving you a blank slate. What would you write on that slate to be placed in a national infrastructure bill? So whomever wants to start.

Mr. Schneier.

Mr. SCHNEIER. I actually think we need a new agency. The problem we are going to have is that we can't have different rules if the computer has wheels or propellers or makes phone calls or is in your body. That is just not going to work, that these are all computers and we are going to have to figure out rules that are central.

Ms. ESHOO. We have a continuing new new majority. So I don't think they want to create an agency, honestly, but this thing needs to get done.

Mr. WALDEN. For every one we create, we delete two.

Ms. ESHOO. They don't like that stuff.

Mr. SCHNEIER. I think you are right.

Ms. ESHOO. You know, new agencies, new regulations, we are dead in the water. But we can't leave this issue to be dead in the water. Our country deserves much better. And so I am really not joking. I mean, it is a little bit of fun, but, you know.

Mr. SCHNEIER. I understand. But I actually think it is not going to go that way. I mean——

Ms. ESHOO. Oh, good.

Mr. SCHNEIER [continuing]. Because I think the Government is getting involved here regardless. The risks are too great and the stakes are too high. And, you know, nothing motivates a Government into action like security and fear.

In 2001, we had another small-Government, no-regulation administration produce a new Federal agency 44 days after the terrorist attacks. Something similar happens in the Internet of Things, and there is no cybersecurity expert that will say, well, sure, that could happen. I think you are going to have a similar response.

So I see the choice is not between Government involvement and no Government involvement, but between smart Government involvement and stupid Government involvement. I would rather think about it now, even if you say you don't want this, because when something happens and the public says something must be done, what do you mean, a thousand people just died, that we have something more than a, "I don't know, let's figure it out fast." So I agree with you. I am not a regulatory fan, but this is the world of dangerous things. We regulate dangerous things. So——

Ms. ESHOO. Dr. Fu, can you do something, in 5 seconds? Thank you.

Dr. FU. I would say just we are going to have some serious trouble if we don't answer these questions. I fear for the day where every hospital system is down, for instance, because an IoT attack brings down the entire healthcare system.

I do think you need to spend more time on the premarket. I know from my working with manufacturers that the engineers there are brilliant, but they often are not given the time of day from their executives. They are often not given the resources to do their jobs. What you need to do is give those people who can do a good job at those companies the ability to do so and incentivize their executives.

Ms. ESHOO. Thank you very much. Most helpful.

Thank you, Mr. Chairman.

Mr. WALDEN. Thank you. I would just point out we are all engaged in this on both sides. My friend and I have some back-and-forths from time to time. She likes to characterize what we are for or against, which we may or may not be, but we are all committed to trying to figure out how to find a solution, and this is bipartisan.

So we appreciate your testimony. We scheduled this hearing back in October right after the attack, and as soon as we were back in town we are having it, and we will continue to march forward.

With that, I would turn to the gentleman from Texas, Mr. Burgess.

Mr. BURGESS. Thank you, Chairman Walden.

And it has been a fascinating discussion back and forth. Many years ago before I knew about the Internet of Things, I was invited up to Microsoft in Washington and they showed me the house they had. In fact, the house was named Grace. And, you know, you walk up to the door and Grace knew you were coming to the door. Grace turned the lights on, set the thermostat for the temperature that you wanted. As you came into the kitchen, Grace might suggest a meal for you. Like Mr. Walden, I worried that Grace's refrigerator would communicate with the bathroom scale and lock down the Blue Bell ice cream on me. So it is an interesting world in which we have arrived.

Mr. Drew, I am really fascinated by your comment in your written testimony about the incentive for someone to do this in the first place. And we have all heard, since 9/11, that sometimes you have got to think like a criminal or think like a terrorist in order to outsmart them. And you referenced the monetization. I don't even see—I mean, I get on ransomware when you lock down a hospital and you have got to come up with so many thousands of dollars in bitcoins to some dark Web site, but how do you monetize that your doorbell is conversing with Twitter? I mean, I don't know how that works.

Mr. DREW. What we are seeing in these botnets is the botnet operators are operating, you know, hundreds of thousands of nodes and then renting out a small portion of those nodes to people to be able to attack Web sites and hold those Web sites for ransom. So if you don't pay me $20,000, your Web site will be offline for the next 3 days. So a very successful enterprise. It is 40 to 45 attacks a day at 16 grand an attack. So——

Mr. BURGESS. That is happening right now?

Mr. DREW. It is happening right now.

Mr. BURGESS. I know you are not in law enforcement. What is the response of our law enforcement agencies that are supposed to be enforcing the laws?

Mr. DREW. They are working very diligently to identify the operators of the botnet as well as the renters of the botnet, as well as making some arrests in those cases to be able to curtail this. But what we have seen is the IoT of Things has changed the nature of the game of this to where it is much easier to break into those devices and they go unnoticed for longer periods of time.

Mr. BURGESS. This is one of the things that bothers me about this, because until we had this headline-grabbing attack because it was just so massive, you don't hear about someone being busted for holding someone hostage for $17,000 so you unlock their hospital records or whatever was going on.

I mean, one of the things that is talked about is making the public aware. You got to change, you got to practice good hygiene, you can't have your password as password or 1234. But you also—there needs to be a societal understanding of reporting the crimes when they occur and, to some degree, these need to be publicized much more than they are.

I mean, I have heard from folks in the FBI that, yes, there is a risk that a hospital that gets stuck with one of these things, they are just simply embarrassed and they don't want to go public with the fact that they were hacked. Pay the $17,000. You are given instructions on how to get the bitcoins and where to deliver them. So that is actually easier than going to law enforcement and dealing with all of the things that would happen with law enforcement. But that is absolutely critical.

And then never in any of the discussion of this, that I have seen so far, has there been really the discussion of what happens to people who are caught who perpetrate this, and it should be swift and severe and public. I suggested at another hearing, shot at sunrise. And I am not trying to be overly dramatic, but if you lock down an ICU's medical records and an ICU's worth of patients die as a consequence, I mean, that is a capital crime.

So anyway, I know we are not going to solve all of the problems today, but I just wanted to put those concepts out there. This is relatively new for most of us.

I think one of the things that I like about—you know, Mr. Chairman, one of the things I like about what the Commerce, Manufacturing, and Trade Subcommittee did on data breach notification was, we will set the standard, but we don't prescribe the technology, because the technology changes much faster than the Congress.

Yes, I am nervous too about creating new Federal agencies. The concept that we could delete two Federal agencies for every one we create, I have got two to recommend to leave very quickly. They deal with health care. But I know the standards need to be there.

And the other thing is we have got a massive job as far as informing the public, and that is part of this hearing today and I hope we all carry that forward quite seriously.

Thank you, Mr. Chairman. I will yield back.

Mr. WALDEN. The gentleman yields back.

The Chair recognizes the gentlelady from Illinois, Ms. Schakowsky.

Ms. SCHAKOWSKY. So let me ask actually all of you, but let me start with Mr. Schneier. You talked about how markets have failed us and that Government has to play a role. But I am wondering, from you and from anyone, given that computers are ubiquitous—and your example that got into Target through the HVAC system is just shocking to me. But is there a role for consumers, for consumer education, for consumer action, or is this beyond us now for individuals to actually play a role in security?

Mr. SCHNEIER. Yes. I think there is a role for some, but, really, we are asking consumers to shore up lousy products. It shouldn't be that there are default passwords. It shouldn't be that you have to worry about what links you click on. Links are for clicking on. I mean, these devices are low profit margin. They are made offshore. The teams that—after they make them disband. And the buyer and seller don't care. I mean, so this—I might own this DVR, you might own it. You don't know if it was used. You don't know if it is secure or not. You can't test it. And you fundamentally don't care. You bought it because of the features and the price. It was sold to you because of the features and the price.

And this is an externality. The fact that it was used by this third party, not him but, you know, by the third party to attack this other site, and it is something that the market can't solve because the market isn't involved in that. So I don't think I can educate the consumer. It is putting a sticker on that says, you know, this device costs $20 more and is 30 percent less likely to annoy people you don't know. I am not sure I am going to get a lot of sales.

Ms. SCHAKOWSKY. So in 2015, the Federal Trade Commission suggested best practices for device manufacturers to address security vulnerabilities. For example, device manufacturers should test security measures before releasing their products, minimizing the data they collect and retain.

And, frankly, it seems surprising to me that manufacturers are not already taking these steps. But you are saying that right now there are no real incentives. So is that what we need to focus on?

Mr. SCHNEIER. I think we should. I think if we get the incentives right, the technologists will figure this out. I mean, this isn't—some of it is rocket science, most of it isn't. But these are solvable problems. The incentives just aren't there to build the security in. We incentivize price. We incentivize time to market. We incentivize features. I mean, that is what we buy, that is what we want, because that is what we can see.

I don't think I can get consumers to pry open the hood and look at the details. It is beyond the consumers I know and it shouldn't be their problem. It shouldn't be something they have to worry about.

Ms. SCHAKOWSKY. So let me ask Mr. Drew and Dr. Fu if you want to comment on that.

Mr. DREW. I would largely agree with my colleague here. I would say that, from a business perspective, there is a lot of incentive for me to make sure that the products that I buy, the software that I buy follow specific standards, have been manufactured correctly before I put them in the network.

I would like to see more in that area. I would like to see more responsibility put on the manufacturer than there is today, but I do provide that incentive to those manufacturers.

Consumers, on the other hand, don't have that incentive. What they do have is the incentive of public events, right, and the Internet has been very adaptable and very flexible to that, that when there is a large sort of trip over—or a mistake over security that they become more aware, and then they push those requirements and those demands back to the manufacturers by purchasing products they feel more comfortable with.

So I am going back to standards. I am going back to certifications and standards. You see that seal of approval on the device and you know that is a device that is going to be more protected than another device, because you don't want your refrigerator talking to your scale or you don't want your thermostat talking to your doorbell. And so I think——

Ms. SCHAKOWSKY. Let me just interrupt you because my time is running out, but I would like Dr. Fu to be able to join in.

Dr. FU. Sure. I would just paint a darker picture. Even if a consumer wants to have—so not many consumers are aware they need security, but when they even want security, it is hard to get. Let me take the example of the hospitals, asking questions about why ransomware gets into hospitals. It is not because they are not clueful about it. They can't get the manufacturers to provide them with these IoT medical devices that can withstand the threats of malware.

And it comes down to plain old economics. The question is, well, how much will you pay for it? Well, we think it should be built in. We think it is a public good. Well, how much are you going to pay for it? So everything is going to be driven by the economic factors. And I think the problem is, you know, the consumer group thinks that, you know, it ought to be a public good. And then from the manufacturing standpoint the question is, well, how much are you going to pay for it? And that is a question that needs to be resolved.

Ms. SCHAKOWSKY. Thank you.

Thank you. I yield back.

Mr. LATTA [presiding]. The gentlelady yields back.

And the Chair now recognizes the gentlelady from Tennessee for 5 minutes.

Mrs. BLACKBURN. Thank you so much, Mr. Chairman.

I want to go back. I mentioned the Cisco stats, and I think they rolled out of my mouth the wrong way. I want to clarify that for the record.

We are currently at 3.4 IoT devices per person, and by 2020, we are going to be at 50 billion IoT devices. And that is the magnitude of this vulnerability that we have, because we are seeing it across our entire economy as we move from a physical application in so many arenas to the virtual space.

And, Professor Fu, I want to come to you. And Ms. Schakowsky just mentioned hospitals. Let's stay with that medical device component, because of the area that I represent, Nashville area, there is a lot of healthcare informatics and work that is done utilizing IoT devices in the medical field. And as you look at the security, of course, that is a concern. You look at information share, you know, you get vulnerabilities.

But you mentioned in your testimony, going back on pages 5 and 6, IoT devices tend to have safety consequences or involve physical manipulation of the world that could easily lead to harm. And then you go on to say a number of hospitals expressed concern about the IoT devices.

So talk to me about mitigation strategies and what you see with these devices, and then what special considerations must be given to healthcare technology and to the medical devices, and how should we go about addressing that?

Dr. FU. Thanks for the question. Unfortunately, I don't think I will be able to give a satisfying answer, because at the moment, if you were to be a fly on the wall in the boardroom when the hospitals are discussing the topic of how does IoT security affect their assurance of the clinical operations being continuous, at the moment, it is—they don't have a plan. It is more, well, we need to get a plan, what can we do. And it is usually some of the security officers saying, well, the problem is we don't really know what devices we have in our hospital, we don't have a very good inventory, we get a lot of contraband coming in. This contraband is known as shadow IT. It has got a great acronym. But the shadow IT that comes in, typically it is a clinician who accidentally connects a device to a very important network, but maybe it is a music player that is simply providing comfort to the patients during surgery, and they don't realize it is introducing new safety and security risks, because they don't have the security baked into these devices.

So the IoT risk is more about having unvetted assets coming in to a very safety critical arena. They don't have a good answer right now and that is because it is not built in.

Mrs. BLACKBURN. OK. Well, then let me go to Mr. Drew. And the article in the New York Times yesterday that I am sure you all saw and are aware of, "Secret Backdoor in Some U.S. Phones Sent Data to China."

Mr. SCHNEIER. Yes.

Mrs. BLACKBURN. And, Mr. Schneier, I assume you read that. Looks like you did. But this is the kind of thing where consumers are unaware. And if you take a device like that and then you have the concerns if it does get into an environment such as a hospital or a medical facility with patient information, things of that nature.

So these malicious actors are out there, and with the vulnerability of these IoT devices, you have some of these concerns that are going to manifest themselves. So how do we make sure that the consumers and the users are alerted to the vulnerabilities in the software and in these devices when they purchase them so that if they get something like this, they know to get rid of it? So, Mr. Drew?

Mr. DREW. I would say that the biggest sort of benefit of IoT devices—the reason IoT devices can get compromised so quickly is because they all look the same. So at a device manufacturer, all the devices look the same, the users are not really configuring the operating system at all, that is why devices can get compromised very, very quickly, very wide scale.

Having those devices ability to auto patch so when a new exposure comes out, that that device can call home, get a new software update and automatically update, that—that is getting the thing that keeps that infrastructure healthy.

Mrs. BLACKBURN. Thank you. I yield back.

Mr. LATTA. The gentlelady, the vice chair of the full committee, yields back.

The Chair now recognizes the gentleman from New Jersey, the ranking member, for 5 minutes.

Mr. PALLONE. Thank you, Mr. Chairman.

I wanted to ask Mr. Schneier a couple of questions. Looking at the attack on Dyn 3 weeks ago, I am concerned some people may dismiss it as only a few Web sites going down for a few hours. But in your view, what does the attack on Dyn expose about cybersecurity generally and why are these attacks moving from benign to dangerous?

Mr. SCHNEIER. It is really what I talked about the world moving. The Internet is becoming something that affects the world in a direct physical manner. And the computers are the same. When we are talking about these computers in our phones, in our computers, it is the same computers that are in these cheaper and smaller devices. But while the software is the same, the engineering is the same, there is a fundamental difference between your spreadsheet crashes and you lose your data and your car crashes and you lose your life. The computer is the same, the software is the same, but the effects are night and day different.

And as these computers start—I live in Minnesota. I have a thermostat I can control from my phone and, you know, if someone hacks it, they can—well, not this weekend, but in the middle of winter, they can burst my pipes when I am here, and that is real property damage. And that is different than a few Web sites going down. Which I agree, I mean, Dyn was benign. It annoyed some people for a while. It didn't hurt anybody. We are talking about hospitals, we have seen DDoS attacks against 911 services. We are looking at our critical infrastructure, our power grid, our telecommunications network. These are systems that are being controlled by computers.

We had hackers break into a dam a couple of years ago. They didn't do anything, but, you know, next time you might not get lucky. We had Russia attack Ukraine's power grid. These are now tools of war and of national aggression. I mean, even the attacks against our election system, which in the scheme of things are pretty benign, might not be next time. I had a piece in the New York Times a couple days ago that talked about, we need to think about this now, because election machines are computers you vote on.

Mr. PALLONE. Sure. Well, let me get to—that kind of leads me to the next question, because you and others have said that the insecurity of devices connected to the Internet stems from market failure, and you even compare the problem to invisible pollution. Being an environmentalist, I would like to better understand what you mean. Can you expand on the market failure at play here, and how are these insecure devices like traditional environmental pollution?

Mr. SCHNEIER. It is because the insecure effects are often not borne by the buyer and the seller. The person who bought that DVR who is still using it, will use it for the next 5, 10 years, will not bear any of the costs of the insecurity. So the manufacturer and the buyer too reap the benefit. The device was cheaper. It was easier to make because it is insecure. And there is a societal cost that it can be used to attack others, to cause other vulnerabilities, to be used in conjunction to cause other insecurities.

So like pollution, it is something in the environment that neither the buyer nor the seller, when they enter their market agreement to purchase the product, will fix. So I think the solutions are along those lines. We have to think about what is the risk to us as a group; you know, what is the national security risk of this, for example. I mean, there is one, but it is not going to be borne by, you know, the person who bought that. It will be borne by all of us.

So it is incumbent on all of us to secure our critical infrastructure against this risk, and that is—so I think the solutions are very similar in conception. The tech is very different.

Mr. PALLONE. All right. Let me ask you one last question. You seem to believe that regulation of some kind might be part of the solution, but I have heard some at the FCC argue that regulation of devices connected to the Internet will constrain innovation. Would you agree with that?

Mr. SCHNEIER. Yes, it will. I mean, I don't like that, but in the world of dangerous things, we constrain innovation. You cannot just build a plane and fly it, you can't, because it could fall on somebody's house. And you might not care, I mean, it might be a drone, but we societally care. True for medical devices, true for dangerous things. And it might be that the Internet era of fun and games is over, because the Internet is now dangerous.

I mean, we haven't even started talking about actual robots, but, you know, a robot is just a computer with arms and legs that can do stuff. And I personally don't like killer robots. I think they are a mistake and we should regulate them.

So, yes, this is going to constrain innovation. It is not going to be good, I am not going to like it, but this is what we do when innovation can cause catastrophic risk. And it is catastrophic risk here. It is crashing all the cars, it is shutting down all the power plants. I mean, the Internet makes this possible because of the way it scales, and these are real risks.

Mr. PALLONE. Thank you.

Thank you, Mr. Chairman.

Mr. LATTA. Thank you. The gentleman yields back.

The Chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. LANCE. Thank you. Good morning to the distinguished panel. And I certainly agree with Congresswoman Eshoo that this is one of the more interesting panels that we have had on this extremely important topic.

Professor Fu, of your observations and recommendations, the eight of them you have given to us, I would like to concentrate on three of them.

Number one, you state that security needs to be built into the Internet of Things, devices, not bolted on. Could you expand on that as to how you think that might occur, that the security occurs before the device has been manufactured?

Dr. FU. Right. Thank you. So often when we talk about security problems in the media or the news, you think, oh, this was a poorly implemented product, where, in fact, it was a poorly designed product, and there is a subtle difference. If you don't get security built in to the early design of these IoT devices, it doesn't matter how smart the engineers are, they will never be able to succeed at creating a secure device, and so that is why you really need to build it in.

If you have this residual risk that you then hand off to the consumer, there are some sweet spots where you can try to mitigate the risk after the fact, but it is extremely rare, extremely hard, and extremely——

Mr. LANCE. So how do we do that? How do we build it in initially?

Dr. FU. Right. There is actually quite a bit of—this is going to get deep into engineering, but let me just say it in one sentence. It is about hazard analysis. It is all about understanding and enumerating those risks and having the manufacturer choose which risks to accept, which risks to mitigate, which risks to pass on to the consumer.

Mr. LANCE. And can that be done through the consumer market or would it require some sort of governmental control? We have mandated, of course, airbags in automobiles, seatbelts in automobiles to be built into the automobile initially and not to be added to the automobile. Is it your recommendation that this will require some sort of governmental mandate or not?

Dr. FU. I do believe in the long-term, this will likely require some kind of governmental mandate only because, in my experience working with the industry, even though they mean well, even the people who can do it don't have the authority to do the right thing, because they don't have the economic drivers. You often have different constituencies within each company.

And let me just cite an example from the medical world. We didn't think about the safety of over-the-counter drugs until 1982 with the cyanide poisonings in Chicago. Until that day, consumers had quite a bit of faith in those pharmaceuticals. We haven't seen that moment for IoT, but we know that that is there and we know that it can cause harm.

Mr. LANCE. Thank you. Moving on, number 4 of your observations for devices already deployed, we should take some comfort that millions of insecure devices are just a small fraction of what the market will resemble in 2020. I suppose you mean by that that this is just at the beginning and there will be many, many more by 2020.

Dr. FU. That is correct. I would say, on a positive side, it means if we take an action now, we could actually win this, we could actually have a very secure ecosystem. So even though there are terrible, terrible problems today, we can fix it, so we shouldn't give up hope.

Mr. LANCE. And can you give us a rough estimate, if we have X number of devices now, how many devices will we have in 2020?

Dr. FU. Well, I have heard the number double in the last 62 minutes from 20 billion to 50 billion, so somewhere between 20- to 50 billion, I think, is a reasonable estimate.

Mr. LANCE. I see. And then number 7 of your observations, there are tens of thousands of unfilled cybersecurity jobs in this country. Existing approaches are insufficient to train a large number in the workforce for what we need in this area.

Based upon your experience first at MIT and more recently in Ann Arbor, what do the great universities need to do in this regard and what do we need to do at the level of community colleges, for example?

Dr. FU. That is a very good question. I think community colleges play a very important role as we develop the different kinds of skill sets. So actually, in fact, there are 209,000 unfilled cybersecurity positions as of a year ago in the U.S., over a million unfilled positions globally.

The problem is, I think, universities need to shift and adapt to the changing marketplace. Right now we are overrun with students. We cannot teach the number of students who want to take our security courses, and yet we are still not meeting the needs. In Michigan, for instance, we have the automotive companies talking about they have 30 unfilled FTE positions for cybersecurity and they are wondering why no one applies.

Mr. LANCE. Well, thank you. My time has expired. I hope to continue the discussion with all on the distinguished panel and particularly with you, Dr. Fu. Thank you very much.

Mr. LATTA. Thank you. The gentleman's time has expired. The Chair now recognizes the gentleman from California for 5 minutes.

Mr. MCNERNEY. Well, I thank the Chair and I thank the panel. This is why I love this subcommittee and this committee. Great stuff happening. I am going to start with Mr. Drew.

In your testimony, you noted that about 2 million of these IoT devices have been affected by this bot, botnet, and only 150,000 were used in the attack. That means there are, what, 1.85 million left. Are they still capable of carrying out new attacks, or have they been neutralized in any way?

Mr. DREW. We have taken—the Internet as a whole has taken steps to try to neuter portions of it, but it is still a 1.5- or 1.6-million-strong-node botnet.

Mr. MCNERNEY. And they can attack not just Dyn servers, but they can attack real physical devices. Is that right?

Mr. DREW. Yes, correct. I mean, the one fear about a botnet like this or a botnet of this size is that they are capable of doing something called a shaped attack, meaning that the operators of that botnet are able to generate any protocol, any application they want from those machines to be able to direct attacks of very specific nature to their targets.

Mr. MCNERNEY. So we have sort of a Damocles sword hanging over us right now?

Mr. DREW. Yes. I think the saving grace we have had so far is that no one has been able to afford to rent all 1.7 million nodes. They have been renting them at 80 to 150,000 nodes at a time. Our biggest fear is that another adversary sees the power of this total force and begins to adopt attacks that follow a similar nature.

Mr. MCNERNEY. Mr. Fu, in your testimony, you recommended we should incentivize built-in security. I am kind of following up on Mr. Lance's question. What type of incentives do you believe would be effective to prevent the risks that you have outlined?

Dr. FU. I think that it all comes down to accountability, whether that be economic accountability or liability. Right now, there just isn't any kind of tangible cost to a manufacturer who deploys something with poor security. Also, there is no benefit if they deploy something with good security.

Mr. MCNERNEY. Well, thank you. This is a question to all witnesses. I want you to answer it with a yes or no.

IoT devices span a wide range of products. Would it be feasible to create one set of security standards for all IoT devices? Starting with Mr. Drew.

Mr. DREW. Yes.

Mr. MCNERNEY. Good.

Mr. SCHNEIER. No.

Mr. MCNERNEY. No?

Dr. FU. No.

Mr. MCNERNEY. No. Oh. OK.

In the alternative, the Federal Government could establish minimum security standards for IoT devices and then direct the relevant Federal agencies to provide additional sector-specific requirements. Would that be feasible, yes or no, please?

Mr. DREW. I am sorry. I missed the question.

Mr. MCNERNEY. Well, since there is a wide range of products, it might be feasible to ask the Federal Government to have the different agencies apply specific standards to those devices. Would that be feasible?

Mr. DREW. Oh, absolutely, because that allows people to apply specific requirements and regulations to the area in which those devices operate.

Mr. SCHNEIER. I think no, because devices do multiple things.

Dr. FU. I think it depends.

Mr. MCNERNEY. OK. Good. Or not.

Mr. Fu, several things. So many questions, so little time. You said that there is no cost to produce devices with poor security, that is pretty clear, but that IoT security is a solution—I mean, it should be a solution, not a problem. Could you expand on that a little bit——

Dr. FU. Right. So my fear is that consumers will not embrace technologies that will improve their quality of life in the future because they don't trust that it will be safe. It won't take too many more horror stories before people start to go back to their analog ways.

So I view security as a solution enabling innovation. In the short term, yes, I would agree with the other witnesses that you may see a short-term problem, because you are going to be interrupting the product development and lifecycle. But in the long-term, we are going to see, I think, this actually producing new innovation, just like what we saw with the car safety regulation many decades ago.

Mr. MCNERNEY. Very good. Now, you also mentioned that devices should incorporate strong crypto security, cryptography. Isn't that asking a lot for these cheap devices to incorporate strong cryptography?

Dr. FU. Cryp-—stop leading me, Bruce.

Crypto—you can implement crypto on these devices. However, there are certain special cases, like medical devices, where it is more challenging. For instance, cryptography does draw more electrical power and it can actually reduce the battery, and so it does cause this sort of risk question. But in the general case, I think it is almost always the right answer to deploy the cryptography.

Mr. MCNERNEY. Well, I have one more important question, but my time has run out, so I yield back.

Mr. LATTA. Thank you. The gentleman's time has expired, and the Chair now recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. Thanks. I appreciate you all being here. And thanks, Mr. Chairman.

And this has been really informative to me. Usually when I get memorandums getting ready for a meeting and it uses words like bots and terabytes, it kind of—my eyes glaze over. But this is important and it is interesting and I have appreciated what you are moving forward.

One thing that—actually, Mr. Lance asked one of the questions I was going to ask. I was going to let Dr. Fu finish a thought, but one thing that you said earlier, that when we write the regulation or the law, that we are going to have to address this if and when we do, that we can't be too prescriptive, because the sign in blue ink, example you used, and I certainly understand that. And I think a lot of things that we have done in legislating has deferred a lot of that to the agencies and we say, well, everything is going to go in good faith, but we also have to be careful to make sure, as we have seen in a lot of other areas, not necessarily this area, that when an agency gets a little leeway, sometimes they go farther than Congress wants them to go, so that forces us to be more specific as we move forward. So we just have to find the right balance in that.

You were talking about—I am interested in auto industry, I am interested in computer science technology, and jobs available. And you were talking about the auto industry and 30 full-time equivalents, and then all of a sudden time ran out and you didn't finish your thought. Do you remember that thought, and can you finish, if you can.

Dr. FU. Sure, sure. So, I mean, Michigan is known as a State with quite a bit of manufacturing, and many of these industries are trying desperately to hire cybersecurity experts. I found one. Many of them have come to me from the automotive industry. They also tend to quit fairly often to go get other jobs. You have got to understand, at the career fair, you will see a line out the door for the Silicon Valley companies, the Googles, the Facebooks of the world. And for these other industries, it is very difficult for them to compete for this talent, not only because of the insufficient number of qualified skilled workers who are trained in appropriate security, but because just the competition is so great.

Mr. GUTHRIE. So hence, one of the major companies, industrial companies, General Electric's ads about—so when the kid—the young man going or woman going to work for General Electric say, I am going to go work for a high tech company, they go, well, you are going to work for General Electric. So maybe that is why they are pursuing that——

Dr. FU. It is a good marketing strategy.

Mr. GUTHRIE [continuing]. Marketing strategy to try to get people to come work for them, yes, absolutely, because they are—exactly proves the point we are saying here. As a matter of fact, they make refrigerators right outside of my district in Louisville, just so that—and they are very high tech. They are very high tech. As a matter of fact, they were showing me one, I couldn't figure out how to operate the refrigerator. It was automatic coffee, pods, and everything in it.

Dr. FU. My refrigerator tweets.

Mr. GUTHRIE. Yep. That is what they do there.

So let me ask you, in your testimony, you start with the basic premise that cybersecurity threats—this is Dr. Fu—are constantly evolving. This is a truism that we have heard reinforced many times. One of the issues is the identification of vulnerabilities. Can you tell us about how vulnerabilities are shared nowadays and if you have any recommendations moving forward on information sharing?

Dr. FU. Sure. So there are many different ways to share vulnerabilities. In the consumer world, for instance, there is the US–CERT, which is a coordinating agency, works in concert with DHS, works in concert with Idaho National Labs and other places to collect information from security researchers and then provide it to manufacturers. That is just one pathway.

Other pathways are things like bug bounties rewards directly between the researchers and the companies. And then the third way that is becoming a little more disturbingly popular is just to sort of drop it in the public before there is a chance to deploy any kind of mitigating control or evaluate whether or not the report is true.

Mr. GUTHRIE. OK. And you sort of talked about this earlier about that the hackers are going to look at the least secure device and then get into the system through that way, so—but I was going to ask you this again, what is the general level of security included in consumer grade Internet of Things devices, and have the recent attacks prompted any conversations that you are aware of about the security included in those devices with manufacturers?

Dr. FU. I have seen no good news about any security in any IoT device. Even in my own home, I have seen devices where I could trivially—anyone on the Internet could just break in and take complete control. This was a device I just picked up in one of those big box stores. I have no good news on the security built in to IoT devices today.

Mr. GUTHRIE. Well, thank you.

Mr. Chairman, that concludes my questions. I yield back.

Mr. LATTA. The gentleman yields back, and the Chair now recognizes the gentleman from New Mexico for 5 minutes.

Mr. LUJÁN. Thank you very much, Mr. Chairman. And thank you for holding this important hearing, to you and to our ranking member.

As we all know, this is an important discussion since the proliferation of cyberattacks represents a serious challenge to both our digital and to our physical space. We saw the proliferation of cyberattacks this year all across the country, including with foreign actors as well being called out by our national security teams.

Pertaining to the development of Internet of Things, which will provide a robust and important infrastructure for America, we also know that there is going to be more conflicts and dynamic networks that will result from that.

Dr. Fu, you talked about shadow devices. Currently, Los Alamos National Laboratory is looking at ways to use the data they collect from all devices connected to a network to monitor and protect against malicious attacks. The LANL work addresses the issue of dynamic and ill-defined networks with devices joining and leaving. It constantly monitors these ever-changing networks to detect and respond autonomously to malicious behavior.

Can you talk about the importance of us moving in that direction as well in developing this, maybe looking to national assets like our national laboratories and what we can learn there for tech transfer opportunities, whether it is in a secure space or an open space, to help us with these endeavors?

Dr. FU. Well, I think what I can do is I can say there is—NIST has a document that talks about how to do this kind of security well, and I hope LANL is implementing these. And one is you have to know your assets at risk, so you enumerate that, and it sounds like that is what you are referring to. The second is to deploy compensating controls that match those specific risks. And then the third one that we often forget as consumers and industry is to continuously monitor the effectiveness of those controls, and that is where it gets to the shifting threat landscape. You deploy a security product today, might be effective tomorrow, might not work at all.

Now, here is where I am a little skeptical of LANL and other agencies that claim they know all of their networks. I know as a fact that most hospitals refuse to look at the security of their most sensitive networks because they are afraid of tipping over things like linear accelerators, radiation therapy devices, very sensitive machines. They have actually rebooted from very simple security products. So if you are in a facility that has nuclear materials, fissile material, I would be very skeptical of a claim where they have thoroughly vetted the embedded systems to see how well they have survived, unless they have actually tipped something over.

Mr. LUJÁN. Is there a benefit, though, with working with these national assets to assist us in the private sector?

Dr. FU. I think there can be a benefit for safety-critical issues for places like LANL. I think there is quite a bit of expertise in what is called embedded security at many of the national labs. However, this is a very interdisciplinary problem, and I have seen this come up already in my vulnerability reports to different agencies. They will often tell me, I am sorry, we don't have an in-house expert on that particular subject of this healthcare situation, let me try to help you, and they usually have a difficult time finding a partner.

Mr. LUJÁN. Mr. Schneier, as more and more of our critical health, energy, and finance infrastructure is brought online, the things connected to the networks will need to be secured from inception to delivery. Are you able to speak specifically to what we can do with securing the technology foundations and supply chains through the Internet of Things, whether it be through semiconductor chips, secure IoT device operating systems, secure communication protocols, or secure device access management?

Mr. SCHNEIER. So this is actually, I think, you know, part of the big problem. Security has to go all the way down. So someone there, I think, who left talked about that phone that surreptitiously, unbeknownst to the consumer, would send copies of your text messages to China. Now, on the plus side, it was cheaper, but you are not going to know, and that could be the software. We are worried about switching equipment that we use in our country that comes from China, because we worry about the hardware, that there might be some hardware switch that will eavesdrop or turn off in the face of hostilities. And these are very complicated questions. And any place in the stack, we can cause an insecurity that affects the others. Lots of people are working on this, there is a lot of tech here, but this is, I think, an extreme worrisome issue when we deal with global manufacturing.

So this is an American device made, I believe, in China. And many of our devices are made in countries that might not be as friendly to us at all times as we would like. And while we have tech that will hopefully detect these things, it is an arms race, and right now there is an edge on the attacker. It is easier to hide a vulnerability in something like this than it is to detect it.

Now, we also use that, right? I mean, the NSA uses that to spy on our enemies, so there is some good here too, but I think by and large it is dangerous for us.

Mr. LUJÁN. And, Mr. Chairman, as my time runs out, I think, Dr. Schneier, I will maybe submit a question to you pertaining to maybe expanded use of trusted foundries pertaining to hardware, and then we can have an expanded conversation in that space.

Mr. SCHNEIER. I would be happy to.

Mr. LUJÁN. Thank you, Mr. Chairman.

Mr. LATTA. Well, thank you. The gentleman's time has expired, and the Chair now recognizes the gentleman from Texas for 5 minutes.

Mr. OLSON. I thank the Chair.

And welcome, Mr. Drew, Mr. Schneier, and Dr. Fu. I have to admit, last night I lost a little sleep preparing for this hearing all because we focused on September 21st of this year when a Mirai botnet launched a DDoS strike on the KrebsOnSecurity. Over 600 gigabits per second swarmed them. And then a month later, October 21st, the same bad actor went after Dyn.

I lost sleep because after 9 years in our Navy as a naval aviator, 8 years working with the Senate side as a senior staffer for two Texas senators, and four terms in the House, I know the biggest threat to our security and our prosperity is not bombs, it is not missiles; it is cyberattacks and cybersecurity, ones and zeros.

What bothers me most about what happened earlier this year is that the attacks—the execution was exactly what Coach McHugh told me when I was 9 years old on the football field. He got his little—drew a play in the sand: Here are the defenders, there are two over there. We will swarm them with four offensive people, score a touchdown. That is exactly what these guys did, nothing hard, nothing new, and yet they had the success of having 600 gigabits per second swarm KrebsOnSecurity.

And so in this environment, we can't be reactive. We have to be proactive. Our Government has to be proactive. Now, I said the word "Government" and said "proactive." Looking around the room here, some people shook their heads and smiled. They know those words don't go together, but somehow we have to come together to address this problem.

And, Dr. Fu, I love your term about we have to have it built in, not bolted on. I know Mr. Lance asked questions about that, but I want to further elaborate on it. Say you went crazy, you ran for Congress, you won, you are a member of this committee. How would you ask—what do you think we should do to help out our American economy to make sure we control these attacks and be proactive instead of reactive? What is our role here in DC?

Dr. FU. All right. Thank you. Let me first correct the build it in, not bolted on is actually a phrase my community has been using for many years, including Mr. Schneier is behind that quite a bit.

But I would say to really get out in front of this problem and be proactive, we haven't even done what I would consider—if I were talking with my students, I would say, you have to do your prelab first before you do the real work. And the prelab is actually going out and actually getting firsthand information from some of these constituents. I am doing that and that is where I am getting my firsthand information, from the executives themselves, from the engineers, and I am just picking up horror story after horror story. I can't relay that to you in this manner, because you haven't seen the people I have talked to. I think that needs to happen. I think there needs to be some congressional visits to these sites. I think they need to go to the universities, I think they need to see where the struggles are happening, what are the barriers.

I believe that likely after you see the same problems that I am seeing, you are probably going to start thinking about, we need to have incentive systems built in economically. I don't know what these are going to resemble. Could they be regulations? Maybe. Could they be more financial incentives or financial penalties? Maybe. Is it more about corporate liability? Perhaps. I don't know the answer on the mechanism, but I know that we need to get more people doing congressional visits to these sites to understand where the problems are borne.

Mr. OLSON. Thank you.

Congressman-elect Drew, your concerns about that how as we get involved in DC, how laws—if you could write laws, how would you write the laws to help your organization overcome this incredible challenge we have with these cyberattacks?

Mr. DREW. I agree entirely with regards to us having the right incentives to make sure that, whether I am a business buying technology or whether I am a consumer buying technology, that we have the right incentives, whether they are economic, liability, or regulation. I completely agree with that mind-set.

And I do think that there are a significant number of existing frameworks with regards to each of those ideals around health, safety, convenience, and use with regards to these threats, as well as with regards to these technologies.

Mr. OLSON. And very quickly, Congressman-elect Schneier, your comments about how would you approach this from a Federal Government role.

Mr. SCHNEIER. So I think you have a serious problem here, and I think we have in a lot of areas, that we are now at the point where the speed of technology exceeds the speed of law. And that has probably changed in the past decade or so. It used to be laws could lead technology and now it has reversed. And so we need to figure out a regulatory structure, an incentive structure, liability structure that is technologically invariant; that we can't focus on technology and rely on them, but focus on people and incentives, because that is what is invariant. Technology will change.

And you are right, these DDoS attacks are kindergarten stuff. It is basic, it is not sophisticated, and yet highly effective. The sophisticated stuff is worse.

Mr. OLSON. Thank you. I yield back the balance of my time.

Mr. LATTA. Thank you very much. The gentleman yields back, and the Chair now recognizes for 5 minutes the gentleman from Ohio.

Mr. JOHNSON. Thank you, Mr. Chairman. And thank you, gentlemen, for joining us today.

Having spent nearly 30 years of my professional career in information technology, I want to get a little bit more into the technical aspects of some of the things we are talking about this morning, particularly traditional DDoS attacks versus these connected device DDoS attacks.

Mr. Drew, as I understand it, these DDoS attacks have been around almost as long as the Internet itself has. They have certainly gotten worse over the last few years, but at least for traditional DDoS attacks, we know that—we know how to defend them against—using techniques like IP address blacklisting or white listing and IP packet inspection, among other techniques. Can you tell us a bit more about those defensive techniques, why they have been successful in defending against traditional DDoS attacks?

Mr. DREW. I would say about every 3 years or so we encounter an evolution of capability with regards to DoS attacks. Every 3 years or so, we have somewhat of a backbone impairment event on the global Internet that is resulting of adversaries developing new capability based on either new weaknesses or new technology and then directing that capability to the backbone. And so I would say that the community at large has been fairly proactive as well as reactive in investigating what those bad guys are doing, the techniques that they are evolving and shaping, and making sure that our capability to respond is built into the platform, or in some cases, bolted onto the platform by redirecting traffic and scrubbing it.

So what I would say is what scares us about IoT attacks is just the enormous potential scale, whereas, you know, the typical botnet that is involved in these attacks over the past handful of years to up to a decade has been in the tens of thousands. We now have the potential of devices in the millions. And network capability for filtering and scrubbing has not scaled at that sort of a factor. So it is something that we are taking with great notice and great pause to make sure that we can invest in our capability and technology to prepare for that.

Mr. JOHNSON. Is it safe to say that the majority of these defensive techniques have worked because they target the way that traditional DDoS attacks use spoofing and amplification?

Mr. DREW. I would say that with regards to what the traffic looks like itself, meaning how that traffic is executed upon the victim, there have been slight evolutions in the way that that traffic looks, but for the most part, that the definition that has an upper and lower control in it, that is fairly well understood. And so the technology is geared to be able to operate within that sort of control parameter. It is really—the big issue is the scale in which that the devices are coming at that victim and being able to launch those sorts of attacks.

Mr. JOHNSON. OK. So to get kind of to the heart of the matter of why we are here today, because from what we have been told, this Mirai botnet doesn't use spoofing or amplification. Is that accurate?

Mr. DREW. That is correct. It uses what is called a shaped attack where it can send any protocol or any packet that it wants to.

Mr. JOHNSON. OK. Instead, the botnet is built out of these individual connected devices, and you would say now there are potentially millions of them out there that are so numerous that spoofing and amplification aren't even necessary. It is the total—it is just a deluge of traffic from those connected devices, correct?

Mr. DREW. That is correct. If you wanted to send a large amount of traffic in the past, you would use an amplification attack.

Mr. JOHNSON. OK.

Mr. DREW. Now with devices like this, you don't need that.

Mr. JOHNSON. Well, you know, I think we need to dig into this a little more then, because when we were talking about defensive techniques before, most of those defensive techniques seem to rely on DDoS attacks that use spoofing and amplification. If a DDoS attack doesn't use spoofing or amplification, and you began to allude to it a little bit, how do techniques like IP address blacklisting or white listing or IP packet inspection work and how effective are they?

Mr. DREW. I would say, in fact, they are probably more effective on nonspoofed traffic. And so the overall capability to inspect and mitigate is more capable when the traffic is not spoofed. Again, I am going to go back to the scale issue, is that a lot of that technology is built for the, you know, hundreds of thousands of inspections at the same time as opposed to the millions of inspections at the same time.

Mr. JOHNSON. My time has expired, but I guess it is safe to say we have got a lot of work to do and we have got to stay on this because we have got to develop new techniques to handle this new threat. Correct?

Mr. DREW. Absolutely.

Mr. JOHNSON. OK. Thank you, gentlemen.

Mr. Chairman, I yield back.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back.

The Chair recognizes the gentleman from Missouri, Mr. Long. Five minutes for questions, please.

Mr. LONG. Thank you, Mr. Chairman.

And, Mr. Drew, I understand that newer brand name devices are generally safer and less vulnerable to cyberattacks, but how much blame would you put on low end manufacturers cutting corners on security with the type of attack that happened in October?

Mr. DREW. Well, with specific regards to the type of attack that happened in October, a vast majority of the devices were those low end manufacturers from other countries. We spoke to a vast majority of those vendors. Those vendors had not really contemplated the idea that their devices could be used in that sort of fashion. Some were mortified and were trying to wrap their head around how they could deploy cybersecurity. And, frankly, other manufacturers had no interest in deploying because they had every belief that their consumers would continue to purchase their product.

Mr. LONG. OK. This is directed to all of you. I guess we will start with Dr. Drew since he is T'd up there, but what are some ways hardware and software manufacturers can band together to prevent a cyberattack like the recent one?

Dr. FU. So I would say——

Mr. LONG. Maybe we won't start with Dr. Drew.

Dr. FU. Oh.

Mr. LONG. No. That is fine. I was just——

Dr. FU. OK. Were you referring to me? I am sorry.

Mr. DREW. He is Dr. Fu, I am Mr. Drew.

Mr. LONG. Oh, OK. I am sorry.

Dr. FU. But together we are interdisciplinary, and I would say the key point here is interdisciplinarianism for the hardware and the software.

There is a good—function follows form. And if you look at the educational system, you will see that the people trained on hardware and the people trained on software don't actually have sort of the closest cultures in terms of education. I think it is going to be very important to educate people in a way that brings hardware and software together, because otherwise you are not going to have the workforce that is going to be skilled and trained to be able to solve these problems. So that is certainly something I am trying to do personally, is when I train students, I train them in both hardware and software, because you just can't abstract it away anymore.

Mr. LONG. So, Dr. Schneier.

Mr. SCHNEIER. So I think this is a particular challenge——

Mr. LONG. Mister. I am sorry. I have got too many—I can't see this angle with my glasses. I need new glasses or a different angle, I guess. There you go.

Mr. SCHNEIER. I think it is a particular challenge, because engineering operates in silos. The companies that made those DVRs got a chip with software on it. They didn't inspect it, because it is a blob, and they put it in their device. They sold that device to some other company that put their name on it, and sold it to the consumer. And you have this chain which is very opaque, and companies will hand off to each other. So banding together, I think, is going to be very difficult. And the way we can do that is to incent it. If I have liabilities that go up the chain, if I have regulations that will affect each other, then I am giving the companies reason to not just say, yep, this works, I am going to put it in my device and I am going to sell it cheaply. This is hard, and I don't have a good, crisp answer. Hopefully Mr. Drew does.

Mr. LONG. That is why we put him last.

Mr. DREW. Yes. I would say that I agree with regards to cheap IoT. I think with regards to cheap IoT, the focus primarily is on the specific set of application that they are looking to develop. They get hardware from another manufacturer, they get the baseline operating system from somebody else, and they just develop their application and don't really know how it all interconnects together as a global ecosystem.

I would say on more emerging IoT that is a bit more integrated and a bit more capable of being interconnected to other IoT devices, we are seeing a lot more sort of discipline and knowledge with regards to marrying both hardware and software disciplines together, as well as being able to achieve higher security standards as they interact with each other from device ecosystems. So a long way to go, but a lot of growth in that particular area.

Mr. LONG. Let me ask you something else. Could the recent cyberattacks have been avoided if the targeted sites registered with more than one company that provided the same services that Dyn provides?

Mr. DREW. Presumably, yes. What we did see, though, on the Dyn attack is that a number of the domains that were targeted, they fell back to another authoritative server, and the bad guy detected that and then launched an attack against that other authoritative server. So, you know, in this case, the bad guy was following specific victims and reacting to them as they mitigated and moved.

Mr. LONG. OK. Yes. I heard you say that earlier in the opening. I think—Dr. Fu, how's that? Is that OK? Dr. Fu, to what extent did default passwords play a role in these recent cyberattacks we have been discussing today?

Dr. FU. So default passwords played a key role because it was the entry point to take over this army of unwitting agents to attack Dyn.

Default passwords are everywhere. In my testimony, I provided a graphic of default passwords for medical devices. There is nothing stopping the same attack from happening to another industry, other IoT products. Default passwords are a big problem. The fact that we are even relying on passwords at all is a big problem.

Mr. LONG. OK. Thank you all.

My time has expired, and I yield back.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman.

The Chair recognizes the gentleman from Florida, Mr. Bilirakis. Five minutes for questions, please.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it very much.

On October 21st, the attack is unprecedented in size, and thought unforeseeable. On January 2015, the FCC staff reported the outlined security risks—thank you—Internet of Things devices present, including potential attacks on other systems.

Dr. Fu, it appears that one of the reoccurring problems identified in your testimony is the use of insecure operating systems, which are actually easier to infect a target for distributed denial of service attacks. Have you seen industry react to these issues and move forward more stable operating systems, and are there impediments to making such a switch?

Dr. FU. I have seen industry move to better operating systems, but like most communities, there is a wide distribution. There is a leader, there is maybe not the leader.

I still see Windows XP, which is a decades-old operating system, in critical systems. There is a photograph of one Windows XP system in a water treatment facility in Michigan in my testimony controlling water pumps for the city.

Windows XP is susceptible to the last decade of already released malware. It doesn't take anyone, more than a kid in their basement, to be able to cause a problem. It hasn't happened, because no one's wanted it to happen.

It is all about the economics. Certainly on the high-end devices, like linear accelerators, for example, or radiation therapy devices, you are talking multimillion-dollar machines. Certainly when a hospital buys a new device, they are more likely to get a new operating system because it just comes with the new system. However, most hospitals have capital equipment costs. And they don't want to have to buy a new MRI or whatnot every 10 years. You know, it should last 20 or 30. This is why you will still see Windows 95 machines, you will see Windows 98 machines—the year is important—in hospitals, because when they go to the manufacturers saying, hey, we really want to have an operating system that we can keep secure, they will say, oh, sure, just why don't you buy a whole new machine.

And so there was this unwritten assumption that the software would be maintained. It may not have been written into the agreement, but the healthcare community felt that it should have been kept secure, kept maintained, but from the manufacturing standpoint, it was, we have provided you this device.

Mr. BILIRAKIS. Thank you. Reports show that many devices used in the October attack were situated overseas. While some seek to regulate devices in our own country, how do we protect ourselves from devices that are outside the U.S.?

Dr. Fu, and then if someone wants to chime in, that is OK too.

Dr. FU. Sure. Let me just comment briefly, and I will let my fellow witnesses opine.

I think the important thing about computer security is not to be able to put yourselves in a secure environment, but you need to be able to tolerate an insecure environment. We are never going to be able to make networks, you know, blissful places full of rainbows. The networks are always going to be hostile. So we need to make sure that whatever we put on there is going to be able to tolerate malicious traffic. DDoS attacks, however, are extremely hard to defend against because they cut at the core of where we are least prepared, and that is high availability.

Mr. BILIRAKIS. Anyone else want to comment on that?

Mr. SCHNEIER. So it is two things. I think that U.S. regulation, especially if it is U.S. and Europe and some more major markets, can cause a new environment, which raises the tide for everybody, because companies are not going to make two devices. They are just going to make one device and sell it. So we can make a difference with us and like-minded countries, like we can in so many other industries.

But Dr. Fu is correct that we can't assume ever a benign environment; that it is going to be a combination of making the devices that we can touch more secure, which means the integrated devices are more a minority, and then building infrastructure controls to secure against this malicious minority. And it will always be that.

Mr. BILIRAKIS. Thank you.

Mr. Drew, do you want to comment quickly, because I have one more question?

Mr. DREW. I was just going to say that we have a fundamental belief of ensuring that we can try to route packets on the backbone that are based on reputation. So the more that businesses and backbones can collaborate together on data and route traffic based on reputation, I think the better prepared we are going to be.

Mr. BILIRAKIS. Thank you.

One of the biggest concerns—for Dr. Fu. One of the biggest concerns of the future distributed denial of service attacks is the potential impact on hospitals and their patients. We already know that hospitals are targets in other areas, such as ransomware hacks. Question for Dr. Fu: How can hospitals best protect themselves from these threats and their current technology, and should industry prioritize the healthcare sector in preventing current cyberthreats?

Dr. FU. Right. Well, in the short term, hospitals are in a sticky place. There is not a whole lot of mitigating solutions. So the best medicine I can recommend for hospitals right now is to really know their inventory of medical devices. I saw some discussion yesterday in a DHS report about a bill of materials of software. Hospitals don't even know what software is running on the inside of their facility because the manufacturers don't know themselves what are on those medical devices. If we only knew what was on the medical devices, we could better understand what risks we are taking.

Mr. BILIRAKIS. Thank you very much.

I yield back, Mr. Chairman. I appreciate it.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back.

The Chair recognizes the gentlelady from Indiana, Mrs. Brooks. Five minutes for your questions.

Mrs. BROOKS. Thank you. I am going to follow up, Dr. Fu, and if you would explain a bit more about what—your concern is is that the devices that are being used actually in the hospitals, the hospitals are not aware of what is on those devices. And so what kind of mechanisms should we have so that hospital systems are fully aware of what is in their hospital?

Dr. FU. Right. So let me just frame the context. So hospitals want to make sure that they have continuity of operations of their clinical work flow so they don't have to shut down, like the MedStar system shut down in this area for several days. And so the problem is when you don't know what your assets are, how are you going to protect that, if you don't know what ports are open? The manufacturers, they are not, I would say, willfully causing harm, as far as I know, but they are simply not providing enough information so that the hospital staff can do their jobs to assure the continuity of their clinical facilities.

So providing a bill of materials of what software comes on a device when it enters the hospital, it won't completely solve the problem, but it is going to really help, because you can't do step two until you do step one. You have to know your assets, you have to know your inventory before you can effectively control security mitigation controls.

Mrs. BROOKS. And so while that has obviously lifesaving or life-ending implications, what other sectors are you most concerned about—and this is for the panel—that—you know, that the sector integration, so to speak, of devices within maybe the system is not known?

Dr. FU. I will just say public utilities, water, gas, electric. It surprises me how people just sort of laugh about, oh, we don't have security, hahaha. And, you know, we are not going to be laughing when the lights go out.

Mr. SCHNEIER. So I think looking at it in sectors is almost self-defeating. So what we are worried about is interactions. And, you know, if you asked somebody a month and a half ago whether a vulnerability in a Web camera can affect Twitter, you know, people would say no. And in a lot of ways, we barely know how the Internet works. I mean, Mr. Drew's answer of whether this particular defense would have mitigated this particular attack, and the answer was we are not really sure. And it is the emergent properties of interconnecting everything that causes the vulnerabilities.

We focus on a sector, we risk missing the big picture. And they are all computers, whether they have wheels or propellers or in your body, and they affect each other, they are on the same Internet. So I urge you to think holistically and not—I mean, there are sectors that are more vulnerable, more critical, that is obvious, but the cause of the vulnerability could come from nowhere.

Mrs. BROOKS. Mr. Drew, a question whether or not—what your thoughts are as to whether or not hacking back or some other form of active defense should be permissible. Thoughts on that?

Mr. DREW. I know that this has been a fairly large debate within my industry. It has been a fairly large debate within the U.S. We have these conversations on a regular basis about green viruses where if we know a particular exposure exists and we know that we can write software to go out and patch this system on the user's behalf to get the malware off the system, then we would be better protecting both the consumer as well as the Internet as a whole. And I think that that is a fairly dark road to go down. I think that it is an excuse for us not fixing the ecosystem and providing the right incentives in the right locations, and potentially has impacts that, you know, the author writing that software isn't necessarily aware of, as he is touching a pretty broad set of devices out on the ecosystem. So I would say I fear more of the consequences of that than I do pushing the right incentives in the right layers.

Mrs. BROOKS. And going back to the question about whether or not we have the appropriate safeguards in place, we have 209,000 job openings right now, according to Dr. Fu, and what are the programs, degree programs or other types of certification programs, that should be offered that we are not offering enough in our higher ed institutions or training programs? And, you know, are degrees necessary or do we need to have different types of certifications short of degrees?

Dr. FU. I think we need all of the above, especially it is a little known discipline called embedded cybersecurity, but this is very related to IoT, bridging the hardware and the software. I think we need both at the community college level, I think we need both at the 4-year college, both in the graduate studies, also especially in advanced master's programs for already skilled workers who are perhaps experts at building cars or designing cars but need to know how do you build security into that thinking. There aren't enough opportunities for those workers to come back to get that training.

And a final comment is the pipeline. I think in the engineering, in some of the sciences, we have difficulty, I think, attracting, tapping new resources, different demographics. I think we need to be much more—doing much more outreach to high schools and some of the kids who are coming up to encourage them to go into these fields, and especially women and minorities.

Mrs. BROOKS. Thank you all for your work. I yield back.

Mr. BURGESS [presiding]. The Chair thanks the gentlelady. The gentlelady yields back.

And the Chair recognizes the gentleman from Illinois, Mr. Kinzinger. Five minutes for questions.

Mr. KINZINGER. Thank you, Mr. Chairman.

Thank you all for being here, taking the time and elaborating on these issues.

Mr. Drew, for you, is it accurate to categorize the recent DDoS attacks as an international issue?

Mr. DREW. It absolutely is an international issue. The device manufacturers were foreign. The majority of the locations where the devices were located was foreign. You know, most of what we are talking about here today, from a regulation perspective, wouldn't have a direct significant impact on at least the adversaries that were involved in the October 21 attacks.

Mr. KINZINGER. Do you know, are there any other countries, international groups, et cetera, focused on these security issues right now?

Mr. DREW. I mean, yes. I mean, there are a number of countries that are focused on very progressive cybersecurity controls. In Great Britain, as an example, there is a significant amount of cybersecurity work with regards to integrating that into the telecommunications sector, so—meaning that if you are going to be offering telecommunication services or if the Government is going to be purchasing services, you have to be certified at a certain cybersecurity level.

Mr. KINZINGER. So are you seeing, through these groups and countries, any kind of a consensus on how to move forward? And, I guess, what recommendations would you give to Congress to, in essence, marry up to that or work together on those issues, to help the conversation?

Mr. DREW. You know, I am going to go back to one of my original points, which is I do believe that we are missing, you know, defined standards in this space, that we can get some adoption around, that we can get some pressure focused on, and we can change buying and investment patterns.

I think that by setting those standards and by setting them by both domestic and international groups, whether it is NIST or ISO, you know, setting these standards so that you can force buying behaviors in both consumers as well as businesses I think is going to be a major step forward.

Mr. KINZINGER. A lot of reports are indicating, as we have discussed, a staggering increase in the number of connected devices over the next few years. It is a number we heard today anywhere between 20 and 50 billion devices, which is unreal. What do you think policymakers and stakeholders should think about, in general, regarding cybersecurity and interconnection moving forward? What would be kind of the takeaway you would want us to leave with?

Mr. DREW. I think innovation is progressing faster than discipline. And, you know, what tends to happen is we go on a biorhythm of a lack of discipline causing significant unintended and unforeseen consequences. Our ability to adapt and respond to those is the thing that is going to keep that infrastructure protected and as well as continue to evolve it.

So I think that, you know, the average CSO has to manage 75 separate security vendors, and that is to bolt on security controls for products and services that they are purchasing. And when we get one of those dials wrong, there are some significant consequences as a result. And so focusing on making sure that premarket controls are placed in that infrastructure is going to be a significant adaptable win for us.

Mr. KINZINGER. Dr. Fu, Congressman Long brought up the issue of default passwords, and you stated that we should get away from passwords all together. Can you elaborate on that?

Dr. FU. I mean, so passwords are just intrinsically insecure. You know, we are human. We write them down. We choose poorly. So pretty much any password system is going to encourage unwise security behavior. There are some technologies out there. There is one company in Ann Arbor, for instance, Duo, that does something called two-factor authentication where you have, for instance, a mobile phone in addition to a password.

But at the heart of it, we need to figure out other ways. And I am going to defer to the other witnesses for suggestions on that. But I just feel we really need to retire passwords. We need to kill those off, because these are going to be bringing down our most sensitive systems.

Mr. KINZINGER. Do any of you want to elaborate on that at all?

Mr. SCHNEIER. So I largely agree. I mean, there will always be a role for passwords. There will be low-security devices, applications, low amounts of latent time, times when you generally need security for a short amount of time. But, in general, passwords have outlived their usefulness, and there are other technologies. You can secure your Gmail account now with a code that comes to your phone as a second factor. I can sure this with my fingerprint.

There are many other systems that give us more robust authentication, and I think that would go a long way in a lot of our systems to help secure them. Because we are talking about two different ways to break into things. We are talking about vulnerabilities, which are exploited; we are talking about bad user practice, which is also exploited. And if I can get rid of one of them or at least reduce it, I am going to go a long way to making things better.

Mr. KINZINGER. OK. Great. Well, I am out of time, and thank you all for your time.

And I will yield back.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back.

The Chair would recognize Mr. McNerney for the purposes of followup questions.

Mr. MCNERNEY. I want to thank the Chair for an opportunity to ask another question. This one is a little philosophical, so I hope you don't mind.

Mr. Schneier, you mentioned that the attacks are easier than defense on this complex system and making more complexity opens up new vulnerabilities. But biological systems work in the other way. They build complexity in order to defend themselves. Is there some kind of parallel we can learn from on this?

Mr. SCHNEIER. So in the past decade or so, there has been a lot of research on sort of moving the biological metaphors of security into IT, and there are some lessons and there are some things that don't work. Biological systems tend to sacrifice the individual to save the species, which is kind of not something we want to think about in IT or even, you know, in our society.

But, yes, there are ways of thinking about a security-immune system, but the complexity of a biological system is complexity that is constrained. So, for example, you know, we all have a different genome, and that gives us a resistance, our species, against a disease. And you might be able to do that with an operating system, but it is not going to be two or three, it is going to be billions of different operating systems, which is suddenly much more expensive by, you know, orders and orders of magnitude.

So a lot of the lessons don't apply. Some do, and the researchers are trying to learn from them. And that is kind of the new cool way of thinking, and I think there is a lot of value there. But still, complexity, unintended consequences, interconnections, the attack surface, the enormous attack surface we are talking about, makes it so that in at least the foreseeable future, attack will have the advantage. My guess is there will be some fundamental advances in security which will give us, maybe not in our lifetimes but eventually, a defensive advantage, but no time soon.

Mr. MCNERNEY. All right. Thank you.

Mr. Chairman, I yield back.

Mr. BURGESS. Thank you.

Mr. Schneier—just recognize myself for a followup question. You had mentioned along this line and then you had mentioned in, I think, response to an earlier question about the autonomous vehicles. And, yes, yesterday in our Commerce, Manufacturing, and Trade Subcommittee, we did have a hearing on autonomous vehicles. So particular vulnerabilities or places where the focus should be as autonomous vehicles, self-driving vehicles develop as a separate entity?

Mr. SCHNEIER. So I think it is a really interesting test bed for what we are thinking about. And I don't know how much detail you went into on the vulnerabilities. What we learn is the vulnerabilities are surprising. There is one attack that used the DVD player as a way to inject malware into the car that controlled the engine. Now, that shouldn't be possible, but surprise. And similarly, I am worried about the USB port on the airplane seat potentially controlling the avionics. The airline companies will say that is impossible, but those in computer security don't believe it.

So, again, the more holistic we can be, the better. There are always going to be surprises. So to get back to the immune system model, how do we build resilience into the system? How do we ensure that it fails safely and fails securely? How do we ensure or at least make it more likely that a vulnerability here doesn't migrate to another vulnerability there causing something more catastrophic? So the more we can look at the big picture, the less we focus on this or that, because it is the connections. And so if you think about it, it is exponential.

I mean, I have five things, that is 25 connections. I have 100 things, that 10,000 connections. It goes up by a factor of square. I just did some math—so sorry—here, but—now, that is the vulnerability, and that is why this is so—that is why complexity is such a problem.

Mr. BURGESS. Well, I mean, I had posed the question earlier, and, really, this is for any of the three of you who wish to answer, you know, the question of thinking like a criminal. But, you know, really, we are still playing checkers and they are playing three-dimensional chess or perhaps a multifactorial level of three-dimensional chess. So, I mean, what are the things that keep you all up at night? What are the things that you have wondered about?

Mr. DREW. I would say the best advancement in the security space for us, as an example, is behavior analytics. It is being able to monitor the network, monitor the enterprise, monitor our infrastructure, and look for behavior that we have never seen before to determine whether or not that is unauthorized traffic or not.

But no matter what, that technology is based on a compromise already having occurred, a bad guy already being in the network. And so our ability to be more proactive, our ability to get ahead of that attack and predict those attacks before they occur and change the technology before they can be exploited, that is where we need to migrate.

Mr. BURGESS. Mr. Schneier.

Mr. SCHNEIER. I worry about catastrophic risk. You know, the Dyn attack is interesting. It was one person had the expertise to figure out how to do it. He encapsulated his expertise in software, and now anybody can do it. So it is unlike my home where I only have to worry about the burglars whom driving to my home is worth the bother. And there is some bell curve of burglar quality, and the average burglar is what I care about. On the Internet, it is the most sophisticated attacker I care about, anywhere in the world, because of the way computers encapsulate expertise into software.

Mr. BURGESS. Dr. Fu.

Dr. FU. I worry about something a little more human, and that is sort of bureaucracies. I worry about the inability to change. I worry about being stuck saying, well, we have never done it that way before. I worry about saying things like, you know, well, that is unprecedented. Well, the Internet of Things is unprecedented and so there are going to have to be some changes. So I do worry that we won't have the strength and resolve to do it. It will take some guts, I think, but this is foresight.

In the safety world, we saw this with handwashing. In the 1840s, handwashing was not even a thought that crossed your mind until after Ignaz Semmelweis. It took 165 years to get to the point where handwashing is common. It is going to take some time for security, but the time is ripe to do something now and to do something wise.

Mr. BURGESS. And I would just note for the record, I think Dr. Semmelweis did end up dying of a strep infection from not handwashing. So it——

Dr. FU. He also messed up his experiments. He didn't write them up well.

Mr. BURGESS. Well, wonderful. This has been a very informative hearing.

Seeing no further members wishing to ask questions, I do want to thank our witnesses for being here today.

Before we conclude, I would like to include the following documents to be submitted for the record by unanimous consent: A letter from the Online Trust Alliance; a letter from the National Electrical Manufacturers Association; a letter from the College of Healthcare Information Management Executives; a letter from AdvaMed, the Advanced Medical Technology Association; and a letter from CTA.

[The information appears at the conclusion of the hearing.]

Mr. BURGESS. Pursuant to committee rules, I remind Members they have 10 business days to submit additional questions for the record. I ask the witnesses to submit their response within 10 business days upon receipt of the questions.

I didn't say it, but, without objection, so ordered that all those things are inserted into the record.

And, without objection, the subcommittee is adjourned.

[Whereupon, at 12:19 p.m., the subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

## PREPARED STATEMENT OF HON. FRED UPTON

The explosive growth of connected devices—or the Internet of Things—has the potential to make a major impact on how consumers, industry, and even State governments measure and manage information from their homes and communities.

Companies back in my home State of Michigan are on the leading edge of this industry. From established businesses to startups, businesses are looking to the future and that, undoubtedly, includes IOT. For example, Herman Miller, the furniture manufacturer based in Zeeland, Michigan; the Detroit business accelerator, TechTown; and startup Tome, in Royal Oak, Michigan, are all focused on the future of connectivity, automation, and security with IOT devices.

As we learn more about how these devices can help consumers in their daily lives and how industry is moving to meet consumer demand, it is critically important for all stakeholders to keep security top of mind.

The recent cybersecurity attacks against Dyn illustrated just how pervasive Internet of Things connected devices are in our daily lives while also demonstrating the balance between functionality and security. Consumers should not be expected to have a degree in computer science to operate the devices they purchase to make their lives a little easier.

While perfect security is an aspirational goal, the increased level of attention these issues have received over the last decade has caught the attention and focus of executives across the country. Basic cyberhygiene, like password vigilance, running routine security scans, and maintaining your online health, is another component that has gained mainstream attention, and I am interested to hear how industry is moving forward to address these issues.

Today's hearing is a good opportunity to learn about what happened in the recent attacks and what issues we should be focused on moving forward. While some may point to Government regulation as the answer—I would strongly encourage caution here. This technology moves as fast as the hackers who are constantly trying to work around industry designs. Regulations have never proven capable of keeping up with that rate of change.

I thank both Chairman Burgess and Chairman Walden for holding today's joint hearing and the witnesses for taking the time to come and testify this morning.

## PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

There is truth to the saying—you don't know what you have until it's gone. Three weeks ago, a cyberattack on a single company—Dyn—left millions of Americans without access to some of the most popular Web sites on the Internet.

This was a disruptive attack coming at a critical time. Citizens couldn't get access to major news and weather sites. Commerce slowed. Online payment services went down.

And even though no one knew exactly what was happening, many guessed that the Internet itself was under attack. We didn't know how much bigger the outage could get or who was attacking us.

Fortunately, we now know that this particular attack was not as bad as it could have been. Looking ahead, we still don't know if the last attack was a dry run or a road map for a larger, more crippling attack. But we do know now just how vulnerable our systems can be. As some of the witnesses testifying before us today have noted, future attacks could target our health care systems or critical infrastructure. Everything from the stock market to the energy grid is connected in some way.

That's why I, along with ranking members Eshoo, DeGette, and Schakowsky, as well as Congressman McNerney, asked for this hearing. I was gratified that our Republican colleagues agreed that our committee needs to better understand these vulnerabilities.

So, what exactly happened? It appears a few hackers attacked a particularly crucial part of the Internet's infrastructure-the domain name service provider, Dyn. This one company helped keep a number of major Web sites online. So by attacking just one company, these cybercriminals were able to knock out a number of others.

But the way that these attackers went after Dyn is just as important as the effect of the attack. The hackers were able to turn our devices against us. They hijacked hundreds of thousands of seemingly innocent devices that so many consumers have in their homes-simple gadgets like digital video recorders and webcams.

The attackers were able to take over these connected devices because they could easily find the default passwords used by the device manufacturers. Some of these passwords were hardwired into the devices so that consumers couldn't change these weak passwords even if they wanted to.

That's why manufacturers of these devices need to take steps to address this problem. Better security is obvious. Hardwired default passwords are not acceptable.

And consumers may also have a role to play when it comes to device security. Using strong, unique passwords is critical. But the recent attack on Dyn makes it clear that consumers can't, and shouldn't be expected to fix this problem.

In fact, most people probably don't even know that their devices were used and those devices owners were not the ones affected by the attack. Instead, it was millions of Internet users across the country who couldn't access many popular Web sites who were affected. Because of this dynamic, I am concerned that although device owners and manufacturers may be in the best place to fix the problems, they have the least incentive to do so. That's why, if we are going to really fix this, the Government may need to take additional steps to keep us safe.

But before we reach that conclusion, we need to answer some tough questions. For instance, will regulations be effective, and what tradeoffs are we making if we regulate? What industry, if any, should be regulated? And what agency should be charged with this responsibility? I am hopeful that today's hearing will bring us closer to these important answers-and it's not a moment too soon because the next attack can come at any time.

With that, I'd like to thank all of our witnesses for being here today, and I'd like to yield the remaining balance of my time to Congressman McNerney.

Statement for the Record
"Understanding the Role of Connected Devices in Recent Cyber Attacks"
United States House of Representatives
Committee on Energy and Commerce
Joint Hearing of the
Subcommittee on Communications and Technology and
Subcommittee on Commerce, Manufacturing, and Trade

By
Craig Spiezle
Executive Director & President
Online Trust Alliance
November 16, 2016
https://otalliance.org
425-455-7400

November 15, 2016

Chairman Walden and Chairman Burgess and Members of the Subcommittees,

Thank you for inviting me to submit a statement to the record regarding how the Internet of Things (IoT) connected devices are being used in cyber-attacks to cause disruption and impact the resiliency of online services. The Online Trust Alliance (OTA) applauds the leadership of the Committee in calling for this hearing.

For background, OTA was formed in 2005 is a 501c3, non-partisan think tank with the mission to enhance online trust, promote innovation and strengthen the integrity and resiliency of online services. Supported by an international coalition of organizations across the public and private sectors, OTA has been a convener bringing together developers, vendors and policymakers to proactively address these challenges, develop best practices, and provide benchmark research.[1]

The following statement provides 1) an overview of the unique security challenges introduced by the proliferation of IoT devices, 2) recommendations to help secure devices and Smart Homes, 3) an overview of the IoT Trust Framework, a set of security and privacy enhancing principles for connected devices, and 4) considerations to help prevent and mitigate the risks associated with products being sold and already in use in homes and businesses worldwide.

**Background**

The rapid rise in the Internet of Things (IoT) has brought forth a new generation of devices and services representing the most significant era of innovation and growth since the launch of the Internet. IoT solutions are game-changers offering consumers, businesses and governments across the globe countless benefits. From fitness trackers to connected thermostats and toys to "smart" cities and medical devices, society is on the cusp of a new technological era. With this great innovation come significant risks, concerns and responsibilities. While the majority of devices are safe and secure by today's standards, all too many lack security safeguards, privacy controls, or lifecycle support plans that leave them susceptible for abuse. When combined, these devices have a capacity for causing significant disruption and very real threats to life and safety.

Recognizing the mounting impact to security, privacy and most importantly personal and physical safety, in February 2015 OTA established the IoT Trustworthy Working Group, an inclusive coalition with the mission to develop essential key security and privacy principles and controls to better ensure human and physical safety. This group includes not only technology and privacy leaders such as Microsoft, Symantec, Verisign and TRUSTe, but others including ADT, the National Association of REALTORS, ACT; the App Association, the Houston School District, Guardian Life Insurance, HSB Group as well input from global organizations including the International Telecommunication Union (ITU), the Internet Society and the International Consumer Research & Testing organization.

Recognizing the importance of working with the public sector, over the past year OTA has briefed staff members of this Committee as well as the White House, Federal Trade Commission, Federal Communications Commission, Department of Homeland Security and the Department of Commerce.

We believe the recent Distributed Denial of Service (DDoS) attacks which have been increasing dramatically in frequency and scale since September, have been a "shot across the bow" and we need to prepare for the worst. Just last week, a similar attack led to the disruption of heating systems in the city of Lappeenranta Finland, leaving thousands of residents in subzero weather by disabling a central heating system.[2] Researchers and malicious actors continue to demonstrate ways an insecure IoT device can drive collective harm in the physical world. These include the ability to distribute ransomware, overheat

[1] Online Trust Alliance https://otalliance.org

[2] DDOs Attacks Central Heating System http://thehackernews.com/2016/11/heating-system-hacked.html

devices with the potential for causing fires and disabling security systems. As witnessed in all too many data breaches the fundamentals of IoT "security and privacy by design" are often overlooked.[3] [4]

**Unique Challenges**

The IoT ecosystem is made up of three dimensions: the device or sensor, the supporting applications, and the backend / cloud services. Combined with the supply chain of each, every facet and data layer is a potential risk. Each needs to be secured across multiple layers as does the flow of data between them. If the integrity of the data or device is compromised, connectivity interrupted, or the functionality remotely controlled by a malicious actor, the consequences can and will be catastrophic.

Incorporating security and privacy protections in the earliest stages of design is the most effective way to bring secure IoT devices to market and to help ensure their safety tomorrow. The processes, technologies and policies that protect users require ongoing support throughout the device's life. Support post-warranty (including usability, patch management, data ownership and portability) must be addressed. Defined as "sustainability," it is the risk and implications of devices left unpatched, orphaned (no longer supported), or bricked (disabled if the company shuts down the apps or backend service). Sustainability also includes the policy issues related to the ownership and transferability of the device and user data. Since devices may outlive an owner or be transferred to new home buyers, consumers and businesses need the assurance that companies will continue to address these needs post warranty. Continuing use of out-of-date devices abandoned or orphaned by their manufacturer will render them insecure and at risk of being targeted and exploited.

Still, it is important to recognize there is no perfect security and privacy and all products have a finite security lifespan. One example is Windows XP. In spite of Microsoft providing Windows XP users no-charge support for over a decade, today millions of PCs running XP remain at risk.[5] While such legacy devices may be secure when shipped, no degree of patching can address unforeseen threats decades later.

**Shared Responsibilities: What We Can Do Today & Tomorrow**

To address these combined issues, OTA convened a cross industry working group with the vision to develop best practices and create an IoT Trust Framework, a voluntary self-regulatory model. While this effort was in review, the OTA and National Association of REALTORS released the Smart Home checklist in October 2015 to help educate consumers and the real estate industry regarding the issues and risk of their devices and the connected home (see Exhibit B).[6]

The Framework was released this past March, identifying 31 criteria initially focused on the connected home, office and wearable technologies (Exhibit C).[7] Serving as a voluntary code of conduct, the Framework is the foundation for several certification and risk assessment programs in development. Further, the Framework is a tool to help assess security and privacy risks for retailers, home builders and businesses regarding the products they may sell, install and purchase.

Collectively, we have a shared responsibility to help protect the security and privacy of individuals, enterprises, and the nation. The Framework represents a major step to help shape products being developed, but we also need to consider what we can do to help address the risks in products being sold today and in use worldwide. We recommend the Committee to call on stakeholders to consider these initial guidelines. Where technically and economically feasible, these and other efforts are needed so together, we may build a safer, more secure world and enable the IoT industry to reach its full potential.

[3] OTA Research September 8, 2016 https://otalliance.org/IoTvulnerabilities

[4] 2016 Data Breach Readiness Guide https://otalliance.org/Breach

[5] Windows XP Support https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support

[6] https://otalliance.org/smart-home

[7] https://otalliance.org/news-events/press-releases/ota-releases-iot-trust-framework

**Recommendations to Help Secure Devices Being Sold & In Use**

1. **Developers and manufacturers**
    a. Proactively communicate to customers any security and safety advisories and recommendations.
    b. Products which can no longer be patched and have known vulnerabilities should either have their connectivity disabled, the product recalled and/or the consumers notified of the risk to their personal safety, privacy and security of their data.
    c. Provide disclosures, including on product packaging, stating the term of product / support beyond the product warranty.
    d. Update websites to provide disclosures and security advisories in clear, everyday language.
2. **Retailers / Resellers / eCommerce Sites**
    a. Voluntarily withdraw from sale products being offered without unique passwords or without a vendor's commitment to patching over their expected life.
    b. Apply supplementary labels or shelf-talkers advising buyers of products with exemplary security data protection and privacy policies.
    c. Notify past customers of recalls, security recommendations and of potential security issues.
3. **Consumers and users** have a shared responsibility. Users need to
    a. Maintain devices and stay up to date on patches.
    b. Update contact information including email address for all devices.
    c. Regularly review device settings and replace insecure and orphaned devices (see Exhibit A).
4. **ISPs** should consider the ability to place users in a "walled garden" when detecting malicious traffic patterns coming from their homes or offices. In concept this would allow basic services such as 911 access and medical alerts, while limiting other access. Such notifications can advise consumers of the harm being incurred, and the need to make changes, replace devices or seek third party support. It is important to clarify as outlined by the FCC's Communication Security & Reliability Council in 2012, such notifications should not directly burden ISPs or carriers to remedy the problem unrelated to their services provided.[8]
5. **Government**
    a. Fund outreach and education, working with trade organizations, ISPs, local grassroots organizations, media, State Agencies and others to raise awareness of the threats and responsibilities. Focus on teachable moments such as at time of purchase, inclusion in billing statements and emails to installed base of users and notices to ISP customers.
    b. Prioritize "whole-of-government" approach to the development, implementation, and adoption of efforts and initiatives, with a global perspective. Coordinated efforts will help to ensure industry can innovate and flourish while enhancing the safety, security, and privacy of consumers, enterprises, and the nation's critical infrastructure.

**Working Together**

The future of IoT cannot be realized without addressing security, data privacy and life-safety issues. Making security and privacy part of every product's feature set and designing it in from the onset is a shared responsibility for both the public and private sectors. Creating a culture of security, privacy and sustainability with transparency will yield long-term benefits to society. OTA looks forward to working with members of the Committee to accelerate the development of best practices, including core safety and privacy requirements, to realize the potential of IoT while promoting safety and privacy innovation helping to protect our economy and society from abuse.

[8] See FCC Anti-Botnet Code of Conduct for ISPs and related recommendations http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Exhibit A

OTA
Online Trust Alliance

# Enhancing the Security, Privacy & Safety of Connected Devices

## Addressing cyber threats, identity theft and personal safety risks

| | |
|---|---|
| □ | Inventory all devices within your home and workplace that are connected to the Internet and network. Router reports can help determine what devices are connected to your network. Disable unknown and unused devices. |
| □ | Contact your Internet Service Provider (ISP) to update routers and modems to the latest security standards. Change your router service set identifier (SSID) to a name which does not identify you, your family or the device. |
| □ | Check that contact information for all of your devices are up-to-date including an email address regularly used to receive security updates and related notifications. |
| □ | Confirm devices and their mobile applications are set for automatic updating to help maximize protection. Review their sites for the latest firmware patches and updates. |
| □ | Review all passwords creating unique passwords and user names for administrative accounts and avoid using the same password for multiple devices. Delete guest codes no longer used. Where possible implement multi-factor authentication to reduce the risk of your accounts being taken over. Such protection helps verify who is trying to access your account—not just someone with your password. |
| □ | Review the privacy policies and practices of your devices, including data collection and sharing with third parties. Your settings can be inadvertently changed during updates. Reset as appropriate to reflect your preferences. |
| □ | Review devices' warranty and support policies. If they are no longer supported by the vendor, disable the device's connectivity or discontinue usage of the device. |
| □ | Before discarding, returning or selling any device, remove any personal data and reset it to factory settings. Disable the associated online account and delete data. |
| □ | Review privacy settings on your mobile phone(s) including location tracking, cookies, contact sharing, bluetooth, microphone and other settings. Set all your device and applications to prompt you before turning on and sharing and data. |
| □ | Back up your files including personal documents, financial records, music and photographs to storage devices that are not permanently connected to the Internet. |

https://otalliance.org/IoTconsumer

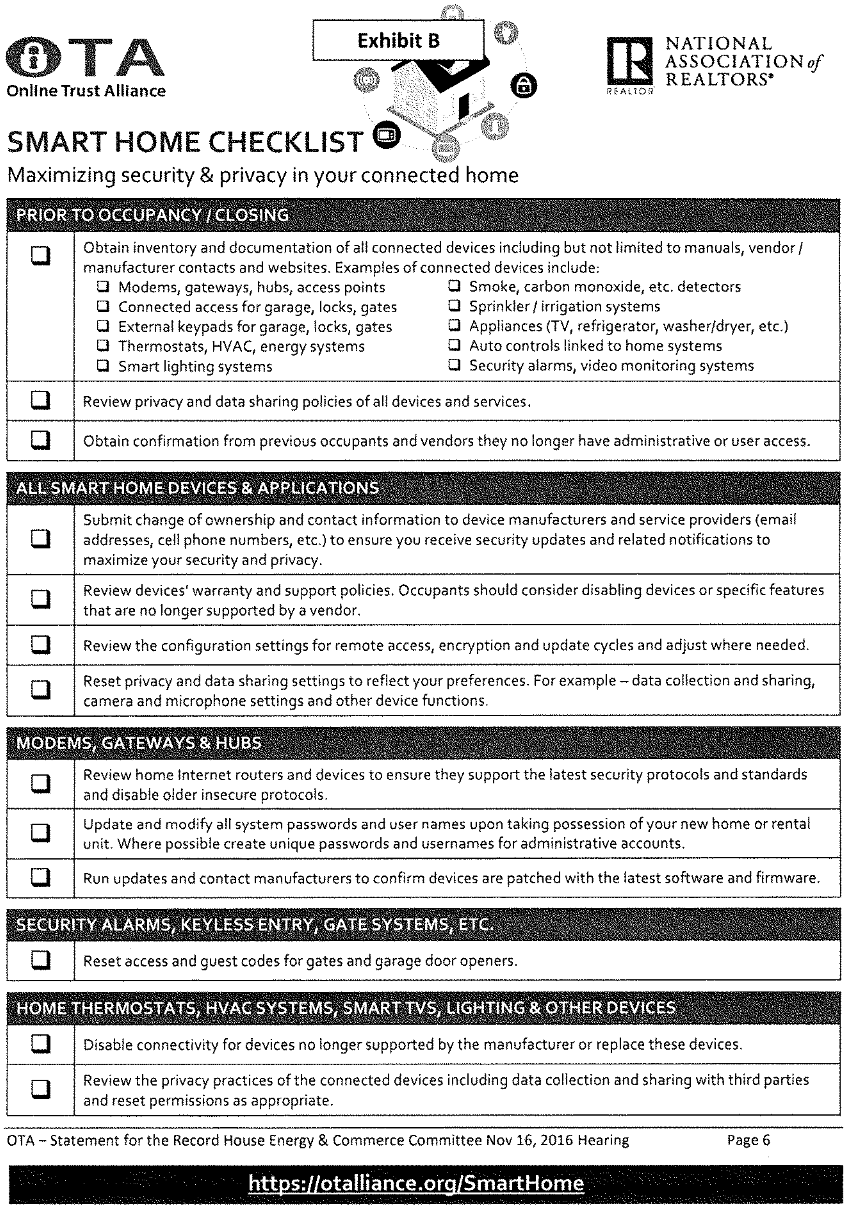


Exhibit B

OTA
Online Trust Alliance

NATIONAL ASSOCIATION *of* REALTORS®

# SMART HOME CHECKLIST

Maximizing security & privacy in your connected home

| | PRIOR TO OCCUPANCY / CLOSING |
|---|---|
| ☐ | Obtain inventory and documentation of all connected devices including but not limited to manuals, vendor / manufacturer contacts and websites. Examples of connected devices include:<br>☐ Modems, gateways, hubs, access points<br>☐ Connected access for garage, locks, gates<br>☐ External keypads for garage, locks, gates<br>☐ Thermostats, HVAC, energy systems<br>☐ Smart lighting systems<br>☐ Smoke, carbon monoxide, etc. detectors<br>☐ Sprinkler / irrigation systems<br>☐ Appliances (TV, refrigerator, washer/dryer, etc.)<br>☐ Auto controls linked to home systems<br>☐ Security alarms, video monitoring systems |
| ☐ | Review privacy and data sharing policies of all devices and services. |
| ☐ | Obtain confirmation from previous occupants and vendors they no longer have administrative or user access. |

| | ALL SMART HOME DEVICES & APPLICATIONS |
|---|---|
| ☐ | Submit change of ownership and contact information to device manufacturers and service providers (email addresses, cell phone numbers, etc.) to ensure you receive security updates and related notifications to maximize your security and privacy. |
| ☐ | Review devices' warranty and support policies. Occupants should consider disabling devices or specific features that are no longer supported by a vendor. |
| ☐ | Review the configuration settings for remote access, encryption and update cycles and adjust where needed. |
| ☐ | Reset privacy and data sharing settings to reflect your preferences. For example – data collection and sharing, camera and microphone settings and other device functions. |

| | MODEMS, GATEWAYS & HUBS |
|---|---|
| ☐ | Review home Internet routers and devices to ensure they support the latest security protocols and standards and disable older insecure protocols. |
| ☐ | Update and modify all system passwords and user names upon taking possession of your new home or rental unit. Where possible create unique passwords and usernames for administrative accounts. |
| ☐ | Run updates and contact manufacturers to confirm devices are patched with the latest software and firmware. |

| | SECURITY ALARMS, KEYLESS ENTRY, GATE SYSTEMS, ETC. |
|---|---|
| ☐ | Reset access and guest codes for gates and garage door openers. |

| | HOME THERMOSTATS, HVAC SYSTEMS, SMART TVS, LIGHTING & OTHER DEVICES |
|---|---|
| ☐ | Disable connectivity for devices no longer supported by the manufacturer or replace these devices. |
| ☐ | Review the privacy practices of the connected devices including data collection and sharing with third parties and reset permissions as appropriate. |

https://otalliance.org/SmartHome

Exhibit C

OTA
Online Trust Alliance

## OTA IoT Trust Framework

| **IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable** | |
|---|---|
| 1. Ensure devices and associated applications support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, and Bluetooth connections. | ● |
| 2. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted. | ● |
| 3. All IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. | ● |
| 4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least annually. | ● |
| 5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). | ● |
| 6. All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. | ● |
| 7. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process including unit, system, acceptance, regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components utilized. Employ generally accepted code and system hardening techniques. | ● |
| 8. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. Domains should implement SPF, DKIM and DMARC, for all security and privacy related communications and notices as well as for parked domains and those that never send email. | ● |
| 9. For email communications within 180 days of publishing a DMARC policy, implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication verification checks. | ○ |
| 10. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message. | ○ |
| 11. For user access, provide unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets. | ● |

| **IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable** | |
|---|---|
| 12. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential re-set using multi-factor verification and authentication (email and phone, etc.) where no user password exists. | ● |
| 13. Take steps to protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts. | ● |
| 14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s). | ● |
| 15. Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually and/or after significant internal system, technical and / or operational changes. | ● |
| 16. Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download, or enrollment. In addition to prominent placement on their website, it is recommended companies utilize QR Codes, user friendly short URLs and other similar methods. | ● |
| 17. Disclose the duration of security and patch support, (beyond product warranty). Such disclosures should be aligned the expected lifespan of the device. | ● |
| 18. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes. | ● |
| 19. Disclose what features will fail to function if connectivity becomes disabled or stopped including but not limited to the potential impact to physical security. | ● |
| 20. Disclose the data retention policy and duration of personally identifiable information stored. | ● |
| 21. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services. | ● |
| 22. Publically disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker). | ● |
| 23. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require third party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access | ● |
| 24. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default." | ● |
| 25. Commit to not selling or transfering any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained. | ● |
| 26. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance. | ● |

| IoT Trust Framework ● Required O Recommended N/A – Not Applicable | |
|---|---|
| 27. Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end-user. | ● |
| 28. Comply with applicable international privacy, security and data transfer regulatory requirements.[9] | ● |
| 29. Publicly post the history of material privacy notice changes for a minimum of two years, including date stamping, redlines, and summary of the impacts of the changes. | O |
| 30. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing, loss, or sale of device. | O |
| 31. Provide device or service data erasure and zeroization in the event of transfer, loss or sale. | O |

**Updates to the Framework, and supporting resources are posted at https://otalliance.org/IoT**

**Terminology, Definitions & Clarifications**

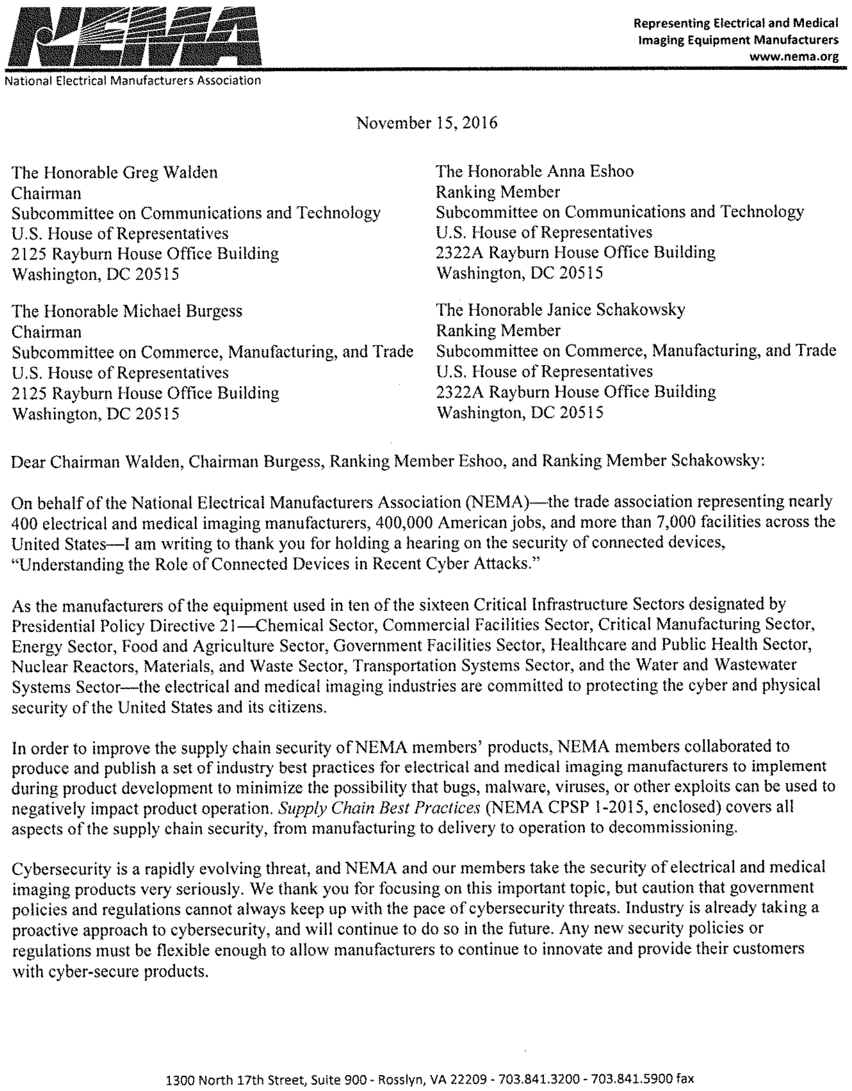
1. Unless specified otherwise, the terms device manufacturers, vendors, application developers, service providers and platform operators are all indicated by the term "Companies."
2. It is expected companies disclose of sharing data with law enforcement and reference any applicable transparency reports as legally permitted.
3. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
4. Smart Cars including autonomous, self-driving vehicles as well as medical devices and HIPPA data[10] are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable. Respectively they fall under regulatory oversight of the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration, (FDA). [11]

Material in this publication is for educational and informational purposes only. Neither the Online Trust Alliance (OTA), its members, nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent and license by OTA.

[9] Companies, products and services must be in compliance with any law or regulation of the jurisdiction that governs their collection and handling of personal and sensitive information, including but not limited to the adherence to the EU-US Privacy Shield Framework www.commerce.gov/privacyshield and/or the EU General Data Protection Regulation (GDPR) www.eugdpr.org. Failure to comply constitutes non-compliance with this framework and would result in the automatic disqualification from any code of conduct or certification program.

[10] U.S Department of Health & Human Services, Health Information Privacy http://www.hhs.gov/hipaa/index.html

[11] http://www.nhtsa.gov/Vehicle+Safety and http://www.fda.gov/MedicalDevices/default.htm



NEMA

National Electrical Manufacturers Association

Representing Electrical and Medical
Imaging Equipment Manufacturers
www.nema.org

November 15, 2016

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Michael Burgess
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Communications and Technology
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

The Honorable Janice Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden, Chairman Burgess, Ranking Member Eshoo, and Ranking Member Schakowsky:

On behalf of the National Electrical Manufacturers Association (NEMA)—the trade association representing nearly 400 electrical and medical imaging manufacturers, 400,000 American jobs, and more than 7,000 facilities across the United States—I am writing to thank you for holding a hearing on the security of connected devices, "Understanding the Role of Connected Devices in Recent Cyber Attacks."

As the manufacturers of the equipment used in ten of the sixteen Critical Infrastructure Sectors designated by Presidential Policy Directive 21—Chemical Sector, Commercial Facilities Sector, Critical Manufacturing Sector, Energy Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and the Water and Wastewater Systems Sector—the electrical and medical imaging industries are committed to protecting the cyber and physical security of the United States and its citizens.

In order to improve the supply chain security of NEMA members' products, NEMA members collaborated to produce and publish a set of industry best practices for electrical and medical imaging manufacturers to implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. *Supply Chain Best Practices* (NEMA CPSP 1-2015, enclosed) covers all aspects of the supply chain security, from manufacturing to delivery to operation to decommissioning.

Cybersecurity is a rapidly evolving threat, and NEMA and our members take the security of electrical and medical imaging products very seriously. We thank you for focusing on this important topic, but caution that government policies and regulations cannot always keep up with the pace of cybersecurity threats. Industry is already taking a proactive approach to cybersecurity, and will continue to do so in the future. Any new security policies or regulations must be flexible enough to allow manufacturers to continue to innovate and provide their customers with cyber-secure products.

If you have any questions, please contact Patrick Hughes, Senior Director of Government Relations and Strategic Initiatives, at 703-841-3205 or patrick.hughes@nema.org.

Sincerely,

[redacted]

Kyle Pitsor
Vice President, Government Relations

CC: The Honorable Fred Upton
The Honorable Frank Pallone, Jr.

Enclosure: NEMA Guideline Document *Supply Chain Best Practices* (NEMA CPSP 1-2015)

*NEMA Guideline Document*
*CPSP 1-2015*

# Supply Chain Best Practices

*Published by:*

**National Electrical Manufacturers Association**
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

The requirements or guidelines presented in this NEMA white paper are considered technically sound at the time they are approved for publication. They are not a substitute for a product seller's or user's own judgment with respect to the particular product discussed, and NEMA does not undertake to guarantee the performance of any individual manufacturer's products by virtue of this document or guide. Thus, NEMA expressly disclaims any responsibility for damages arising from the use, application, or reliance by others on the information contained in this white paper.

## EXECUTIVE SUMMARY

### PURPOSE

This document identifies a recommended set of supply chain best practices and guidelines that electrical equipment and medical imaging manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. The document addresses United States supply chain integrity through four phases of a product's life cycle:

- An analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain;
- Tamper-proofing to ensure that the configurations of the manufactured devices have not been altered between the production line and the operating environment;
- Ways that a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment;
- Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks.

This document is not meant to be all-inclusive but rather a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain. Each type of manufactured product will have some tolerance to the risks identified in this document. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

### DOCUMENT STRUCTURE

For each phase of the product life cycle, the following information is provided:

- Identification of threats and their relevance (including appropriate informative reference standards or other documents that might apply);
- Analysis to determine implications;
- Recommendations that electrical equipment and medical imaging manufacturers should incorporate.

## Contents

**EXECUTIVE SUMMARY** .......... 2

ACKNOWLEDGEMENTS .......... 4

INTRODUCTION .......... 5

DOCUMENT SCOPE .......... 5

DEFINITIONS .......... 5

RISK TOLERANCE .......... 5

SUPPLY CHAIN COMMUNICATION .......... 5

BEST PRACTICES .......... 6

MANUFACTURING AND ASSEMBLY .......... 6

Identification of Threats .......... 6

Analysis and Recommendations .......... 7

TAMPER-PROOFING .......... 10

Identification of Threats .......... 10

Analysis and Recommendations .......... 11

SECURITY DEVELOPMENT LIFE CYCLE .......... 13

Identification of Threats .......... 13

Analysis and Recommendations .......... 14

DECOMMISSIONING/REVOCATION .......... 17

Identification of Threats .......... 17

Analysis and Recommendations .......... 18

Appendix A REFERENCE DOCUMENTS .......... 20

Appendix B REFERENCE ARCHITECTURES .......... 23

**Figures**

Figure 1 SGAM Framework .......... 23

Figure 2 Interoperability Layered Categories Defined by GWAC .......... 26

**Tables**

Table 1 SGAM Domains .......... 24

Table 2 SGAM Zones .......... 25

## Acknowledgements

This white paper guideline document was developed by the cybersecurity working group of the National Electrical Manufacturers Association (NEMA). The group includes representation across the following divisions within NEMA: Industrial Automation, Electronics, Building Systems, Power Equipment, Lighting, Wire & Cable, and the Medical Imaging and Technology Alliance (MITA). At the time this white paper was published, the cybersecurity working group was composed of the following member companies:

ABB, Inc.—Raleigh, NC
Acuity Brands, Inc.—Conyers, GA
Eaton—Cleveland, OH
Encore Wire Corporation—McKinney, TX
GE Healthcare—Waukesha, WI
GE Industrial Solutions—Plainville, CT
Honeywell Automation & Control Solutions—Golden Valley, MN
Landauer, Inc.—Glenwood, IL
Panasonic Corporation of North America—Secaucus, NJ
Panduit Corporation—Tinley Park, IL
Phillips Healthcare—Andover, MA
Rockwell Automation—Milwaukee, WI
S&C Electric—Chicago, IL
Schneider Electric—Andover, MA

## INTRODUCTION

This document will identify a recommended set of supply chain best practices and guidelines that NEMA and MITA manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. Successful implementation of the practices described in this document will also address a known area for development, alignment, and collaboration (supply chain risk management) identified in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was developed as a response to Presidential Executive Order 13636—Improving Critical Infrastructure Cybersecurity.

## DOCUMENT SCOPE

This guideline document addresses United States supply chain integrity through four phases of the product life cycle: manufacturing and assembly, tamper-proofing, security development life cycle, and decommissioning/revocation. This document is not meant to be all-inclusive but rather a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain.

## DEFINITIONS

Key terms used throughout this document:

**Manufacturer:** an organization or entity that makes a device through a process that includes raw materials, components, or assemblies

**Embedded component:** a component with a dedicated function within a larger electrical or mechanical device

**Tamper-proofing:** a methodology used to hinder, deter, or detect unauthorized access to a device

**Operational compliance:** a state of being in accordance with established guidelines, specifications, or requirements

**Revocation:** the act of recall or annulment

**Decommissioning:** a formal process for removing a device from active status

**Upstream suppliers:** those who supply components to a manufacturer, including chip manufacturers and software driver developers

## RISK TOLERANCE

Each type of manufactured product will have some tolerance to the risks identified in this document. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

Understanding the level of acceptable risk is also required for establishing correct upstream and downstream supply chain relationships. It is typically difficult, if not impossible, to have a greater level of security (i.e., lower level of risk) than the upstream supply chain can provide.

## SUPPLY CHAIN COMMUNICATION

An often unspoken risk is lack of communication across the supply chain. Depending on the expected lifetime of a product, the requirement for communication can be a major source of overhead. The requirement for communication extends upstream to all embedded component providers and downstream to all manufacturers and customers.

## BEST PRACTICES

Each of the following sections contains an identification of threats, their relevance (including appropriate informative reference standards or other documents that might apply), an analysis to determine implications, and recommendations that NEMA and MITA manufacturers should incorporate.

## MANUFACTURING AND ASSEMBLY

This section focuses on an analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain. Embedded components could be hardware-related, such as a microprocessor chip or an Ethernet chip on a motherboard, or software-related, such as an embedded operating system (O/S) or firmware/code stored in a non-volatile memory device, such as ROM or flash memory. The analysis done in this section needs to take into account security considerations of upstream suppliers in the supply chain to determine their levels of malware protection and detection.

### Identification of Threats

1. Maliciously Tainted Components

   A maliciously tainted component is one that has been procured through a manufacturers' authorized channel but has been tampered with or altered in a way that is not compatible with its design specification. When describing software components, the term "malware" is sometimes used. Components that have been corrupted might not perform as intended and could enable a specific attack on an entity or organization using the particular product that includes the installed components. Failure, degraded performance, rogue functionality, and weakened security mechanisms are all possible outcomes of maliciously tainted components.

2. Counterfeit Components

   A counterfeit component is one that is supplied to a manufacturer directly or indirectly by other than an authorized channel and is presented as being legitimate even though it is not. Counterfeiting poses a risk because the component's integrity cannot be validated, the performance might be substandard, and specific technical support services are not available.

3. Practices of Upstream Suppliers

   Components could be supplied to a manufacturer via a normal distribution channel or a gray-market source. A normal distribution channel refers to the established chain of business(es) through which a component passes before it reaches the manufacturer. A gray market is the trade of a component through a distribution channel that while legal, is unofficial, unauthorized, or unintended. Manufacturers need to understand how procured components are moving through their distribution channels in order to verify legitimacy. Whenever components are purchased outside normal distribution channels, there is additional risk of maliciously tainted or counterfeit components being entered into the product.

4. Lack of Formal Design Processes

   A formal design process is a multi-step process that includes research, conceptualization, feasibility study, establishment of design requirements, preliminary design, detailed design, production planning and tool design and, finally, production of a specific product. Ideally, this process should be documentable and repeatable. In addition, manufacturers need to understand how security considerations would be integrated into every step of the process, beginning with its initiation.

   There are two sources of risk with design processes. First, the design processes of upstream suppliers place limits on the risk of the integrating manufacturer. Second, the design processes of a manufacturer will have obvious impact on the components and products provided downstream to other manufacturers or consumers.

5. Software Executables

   A software executable or executable code is software in a form that can be run on a computer. It usually refers to machine language, the set of native instructions the computer carries out in hardware. Executable code may also refer to programs written in interpreted languages that require additional software to execute. There might be unnecessary capabilities or features of these executables that would affect the product's overall security. The challenge is to identify and then either disable or lock down these particular aspects without affecting the overall intended functionality of the software.

**Analysis and Recommendations**

1. Maliciously Tainted Components

   Several published standards speak to the need for malware detection and protection. Manufacturers can choose to follow any or all of the techniques described in the documents identified below:

   a) The *Open Trusted Technology Provider™ Standard* (section 4.2.1.12). Malware detection tools should be deployed as part of the code acceptance and development process. These techniques should also be used before final packaging and delivery.

   b) The SAFECode *Software Integrity Controls* document. Malware scanning at exchange points between parties, using the most recent malware signature files and more than one scanning engine.

   c) NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.6) speaks to the need to apply static analysis tools to search for virus/malware signatures.

   d) IEC 62443-1-1, *Industrial Communication Networks—Network and System Security* (section 5.6.6) calls out scanning for malicious software as an effective threat countermeasure.

   **Recommendations:** Manufacturers should work with upstream component suppliers to identify component versions and should thoroughly evaluate each new version of a component. This evaluation should include a malware analysis. In addition, each component supplier should identify the methods used to ensure that the component is not altered between manufacture and receipt.

Where technically feasible, code signing is one method of ensuring deliverables have not been altered. It also provides methods to ensure the authenticity of the deliverable and supplier. Code signing is the process of digitally signing executables and scripts by use of a cryptographic hash to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. Almost every code-signing mechanism will provide some sort of digital signature mechanism that answers the questions of authentication (who signed the code?) and integrity (has the code been tampered with since it was signed?).

The code signing white paper developed by Certificate Authority Security Council (https://casecurity.org/wp-content/uploads/2013/10/CASC-Code-Signing.pdf) includes a number of best practices that can be used to address the biggest issue with code signing: the protection of the private signing key associated with the code-signing certificate.

2. Counterfeit Components

Some suggested procedures and techniques that manufacturers can use to address fraudulent/counterfeit components are identified in the standards documents listed below:

a) SAE International SA AS5553, *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*, was created in response to a significant and increasing volume of fraudulent/counterfeit electronic parts entering the aerospace supply chain. The document was expanded to address fraudulent/counterfeit risk mitigation on a global scale across multi-sector electronic supply chain industries and to provide uniform requirements, practices, and methods to mitigate the risks of receiving and installing fraudulent/counterfeit electronic parts. Section 4 describes a control plan that documents processes used for risk mitigation, disposition, and reporting of suspect or confirmed fraudulent/counterfeit parts and/or assemblies containing such parts.

b) ISO/IEC 27036-1: 2014 (parts 1, 2, and 3) is an introductory part of ISO/IEC 27036, *IT Security—Security techniques—Information security for supplier relationships*. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships.

c) The *Open Trusted Technology Provider™ Standard* (section 4.2.1.11) lists counterfeit mitigation techniques, such as security labeling and scrap management.

d) NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 3) describes a supply chain risk-management plan that addresses an organization's internal and external practices and controls employed to minimize the risk posed by counterfeits.

**Recommendations:** It is suggested that manufacturers follow a documented purchasing process that gives preference to procuring components from only the original component manufacturers or their authorized suppliers. Manufacturers should also have in place some type of industry-recognized incoming inspection technique in order to discover counterfeit components before they become physically integrated into a product.

Tracking disposition of components might also be necessary if counterfeit detection occurs after a device has been shipped, in order to facilitate a recall.

3. Practices of Upstream Suppliers

As previously recommended, manufacturers should follow a documented purchasing process that gives preference to procuring components from only original component manufacturers or their authorized suppliers. Manufacturers can further mitigate the risks associated with upstream suppliers by adopting any of the following:

- Inclusion of terms and conditions related to security requirements in procurement contracts;
- Additional component acceptance procedures;
- Independent, third-party validation of supplier conformance;
- A practice for sampling incoming components (per lot/unit). This could be done at the upstream supplier before shipment or at the manufacturer's facilities upon arrival.

4. Lack of Formal Design Processes

The following identified standards address the need for a formal design process that includes software, firmware, hardware, and security aspects. Manufacturers can choose to follow any or all of the methods described.

- The *Open Trusted Technology Provider™ Standard* (section 4.1) describes the need to include documented requirements that are traceable, a well-defined engineering method, configuration management, quality and test management, and product sustainment capabilities. Additional levels of security are obtained by following a secure development engineering method.
- NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems,* states that a prerequisite for successful supply chain risk management begins with the fundamental performance of good system design that includes security requirements at inception.
- Both NIST IR 7622 (section 4.6) and IEC 62443-1-1, *Industrial Communication Networks—Network and System Security* (section 5.4) mention defensive design techniques, the practice of anticipating all possible ways an end user might misuse a product, and then designing to make such use impossible or minimize its negative consequences.

**Recommendations:** Manufacturers should have in place a documented design process. This process should be repeatable and measurable and should effectively identify and address potential vulnerabilities. Ideally it should be auditable via some type of organizational quality assurance procedure. This process should be documented in a way that can be shared with downstream manufacturers. Manufacturers should request process documentation from upstream suppliers as part of the contract agreement.

5. Software Executables

   Suggested manufacturing techniques to address the unnecessary capabilities of software executables that could pose additional security risk are mentioned in the standards below.

   - The SAFECode *Software Integrity Controls* document addresses examining "out of the box" defaults on the source code and configuring it to be secure by default.

   - IEC/TR 80002-1, *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software,* is a report aimed at risk management practitioners who perform risk management when software is included in a medical device/system. It details a management process that analyzes risk identifying known or foreseeable hazards that software failures could contribute to, evaluates the risk to determine if reduction is required, and suggests various risk controls that can be implemented in the software itself.

   - NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.9) mentions the possibility of software service/maintenance agreements for critical software elements.

   **Recommendations:** Manufacturers should have well-defined processes to identify and remediate vulnerabilities of software/firmware associated with a particular device throughout its life cycle. Several industry-recognized software vulnerability mitigation techniques (e.g., stack buffer overrun protection) are available for manufacturers to use as they work to develop software for a particular product.

## TAMPER-PROOFING

This section focuses on tamper-proofing, which ensures that the configurations of the manufactured devices have not been altered between the production line and the operating environment. Another term often used in the same context is tamper-resistance. Tamper-proofing ranges from simple features like screws with special heads, to more complex elements, such as devices that render themselves inoperable or encrypt all data transmissions between individual chips, or the use of materials requiring special tools and knowledge. Effective tamper-proofing of a manufactured device ensures its integrity. If tamper-proofing measures can't be provided, procedures to detect tampering should be made available to the receiver.

### Identification of Threats

The system aspects listed below would require some form of tamper-proofing:

1. Hardware (embedded components)

   Embedded hardware components could include a microprocessor or an Ethernet chip on a motherboard. Tamper-resistant microprocessors are used to store and process private or sensitive information. Examples of tamper-resistant chips include a secure crypto processor and chips used in smartcards or integrated circuit cards.

2. Software Components

   Software components include an operating system and any additional applications. Software tamper-proofing refers to protecting it against reverse engineering and modification.

   Tamper-proofing is not a single measure but rather a collection of different transformations that individually protect each other, as well as the software to be protected. Consideration should be given to possible impact on software performance as a result of any tamper-proofing mechanisms.

3. Data Storage Devices

   Storage could be either volatile or non-volatile. The main difference between the two is what happens when power is turned off. Volatile storage, such as memory, requires constant power in order to retain the data. With non-volatile storage, such as a hard disk drive, once the data is written it will remain for a considerable amount of time. However, there are also several types of non-volatile memory, such as read-only memory (ROM) or flash memory. The move to more non-volatile memory types in systems introduces new vulnerabilities as sensitive data (such as passwords) might still reside in main memory after a system is powered off or rebooted. Tamper-proofing storage devices would ensure that the data present on those devices has not been compromised.

4. Communications

   System communications can occur via wired network, wireless network, cellular, or Bluetooth, for example. Data transmitted through these various channels should be secured in order to prevent unauthorized access and misuse. It is widely known and accepted by the industry that some open-standard industry protocols in use today cannot be secured.

**Analysis and Recommendations**

1. Hardware (embedded components)

   Several published standards mention procedures for tamper-proofing hardware-embedded components: The *Supply Chain Security Assurance* document suggests that hardware products might mitigate the threat of tampering by using one or more of these techniques: tamper-resistant labeling, smart tags, or delivery via a trusted courier.

   - NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.9) recommends incoming inspections and acceptance testing of incoming items to detect evidence of tampering. It also stresses the importance of a configuration baseline.

   - Federal Information Processing Standard (FIPS) PUB 140-3 (section 4) lists security requirements for hardware cryptographic modules used within a security system protecting sensitive information in computer and telecommunications systems. It identifies four security levels; as the levels increase, so do the corresponding security and tamper-proofing requirements.

   **Recommendations:** At minimum, manufacturers should be required to use some type of tamper-resistant coating or seal for all hardware components.

2. Software Components

Some suggested procedures and techniques that manufacturers might use to address tamper-proofing software are listed in the following standards documents:

- The *Supply Chain Security Assurance* document suggests that cryptographic checksums or a digital signature can be implemented to mitigate the tampering threat.

- FIPS PUB 140-3 (section 4) lists security requirements for software and firmware cryptographic modules used within a security system protecting sensitive information in computer and telecommunications systems. It identifies four security levels; as the levels increase, so do the corresponding security and tamper-proofing requirements.

**Recommendations:** At the Operating System (O/S) layer, manufacturers should consider using an O/S with minimal kernel features and reduced application sets. With the advent of Software Development Kits (SDKs), malicious individuals can manipulate commercial O/S kernels. Making the kernel harder to manipulate increases the integrity of the O/S component. Development-specific features should be disabled prior to shipping, and code should be stripped of debugging features and symbols. Joint Test Action Group (JTAG) is one such feature. JTAG is the common name for the IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture. It is a method for testing interconnects on printed circuit boards or sub blocks inside an integrated circuit.

Manufacturers should use tamper-resistant techniques to produce software that is more difficult for an attacker to modify. Code signing, as mentioned earlier, should also be used.

3. Data Storage Devices

Tamper-resistant storage techniques provide a level of assurance for data integrity. Some processes that manufacturers should consider: increasing the level of authentication required for updating, modifying, or deleting data; encrypting data to ensure limited data access; hashing or assigning a digital signature to data; or creating immutable storage that can never be changed.

**Recommendations:** Manufacturers should consider the operational threat landscape that data will exist and implement appropriate data integrity controls. There are several publications that can assist manufacturers in selecting appropriate controls, including:

- NIST SP 800-111, *Guide to Storage Encryption Technologies for End Use Devices* (sections 3 and 4) provides guidance for organizations in understanding storage encryption technologies for devices and planning, implementing, and maintaining storage encryption technologies.

- IEEE STD 1619, *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices,* specifies cryptographic transform and key archival methods for protection of data in sector-level storage devices.

4. Communications

Tamper-resistant communication starts with a focus on ensuring that data cannot be manipulated maliciously. As an example, to assess the opportunity for malicious individuals to intercept, modify, and then send data to the intended recipient or device, manufacturers should consider the logical path by which the data will travel. This is called a "man-in-the-middle" attack. There are several ways to provide a level of tamper-proofing to communications. Secure-by-default protocols, such as SFTP, HTTPS, FTPS, and SSH, add levels of authentication to data streams and are relevant and industry-accepted.

**Recommendations:** Manufacturers should tamper-proof communications by permanently disabling historically unsecure communications services (e.g., TFTP, FTP, and Telnet) and should opt for secure-by-default protocols for their communication services. Manufacturers that use secure communications should understand the requirements of the protocols they use and configure them correctly. If PKI is used, for example, then the manufacturer should understand the necessary certificate and cipher requirements to ensure security. At minimum, a manufacturer should request external validation of security code if there is no in-house knowledge.

Suggested standards that address secure communications protocols in more detail include:

- IEC 62351 is a series of standards developed for information exchange for power systems and related systems, including energy management, supervisory control and data acquisition (SCADA), and distribution automation. However, not all industrial protocols are addressed in IEC 62351.

- ISO/IEC 27033 (parts 1-5) is a series of standards that provide detailed guidance on security aspects of the management, operation, and use of information-system networks and their inter-connections.

## SECURITY DEVELOPMENT LIFE CYCLE

This section addresses ways the manufactured device enables asset owners to comply with the security requirements and necessities of the regulated environment. Depending on the environment where the device is installed, this could range from demonstrating auditable configuration management procedures to conformance with additional standards.

### Identification of Threats

1. Configuration Management Practices

   Configuration Management is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, and design and operational information throughout its projected life cycle. This type of process facilitates orderly management of system information, as well as system changes.

2. In-house and Third-party Quality Assurance Audits

   Quality Assurance (QA) is a method of preventing mistakes or defects in manufactured products and avoiding problems when delivering the items. QA is applied to physical products in pre-production to verify that what will be made meets specifications and requirements, and during manufacturing production runs by validating that unit/lot samples meet quality controls. QA is also applied to software to verify that features and functions meet objectives and that the code is immune to known bugs prior to shipping or release of new software products or versions.

A QA audit is conducted by an internal (in-house) or external (third-party) auditor that helps to ensure an organization's processes and systems are in place and being followed. The objective of the audit is to draw attention to necessary improvements and ensure that requirements are being followed in order to deliver consistent products.

3. Risk Management

   It is important for manufacturers to understand the regulatory, contractual, physical, and operational environment in which a device will be installed. Understanding this environment allows the manufacturer to characterize the threats and vulnerabilities to which the device will be subjected.

   Once this characterization has been completed, manufacturers should develop a risk response by analyzing the identified threats and vulnerabilities with their impact and likelihood. Additional operating or design controls might need to be developed, or specialized warnings and instructions to the asset owner might be necessary to address risk. As manufacturers change, update, or create new devices, this same risk management approach should be applied.

4. In-house/Third-party Testing

   Testing a particular product within the confines of a manufacturer's facility serves to provide an internal level of confidence that the product is performing as intended. This testing could include specifying additional conditions for the environment in which the product will be installed.

   Third-party certification testing refers to testing of a particular device or product (such as an accredited testing lab) to the specified requirements of the operational environment. Third-party labs typically generate an official results document upon successful test completion.

5. Incident (or Event) Management Plan

   "Incident, or event, management" describes the activities of an organization to identify, analyze, and correct hazards or threats in an effort to prevent future occurrences. The absence of effective incident management can rapidly disrupt business operations, information security, IT systems, employees, customers, upstream suppliers, and other vital functions.

**Analysis and Recommendations**

1. Configuration Management Practices

   Several standards mention the need for a formal configuration management practice. Manufacturers can follow any of the methods described in the documents below:

   - The *Supply Chain Security Assurance* document lists suggested configuration management practices for the provider and the evaluator.

   - NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.3) includes configuration management in its list of 21 practices that an organization should consider when creating the list of measures it will employ as part of its information security strategy.

- FIPS PUB 140-3 (section 4.10) includes configuration management in the life cycle assurance (design, development, and operation) of a cryptographic module. Depending on the security level of the module, it might require additional life cycle assurances, such as automated configuration management.

**Recommendation:** At minimum, manufacturers should have a formal, documented configuration management process in place that includes the following five distinct disciplines:

- A formal document and plan to guide the configuration management program as part of the security development process;

- Configuration identification that consists of setting and maintaining baselines that define the system or subsystem architecture, components, and any developments at any point in time;

- Configuration control, which includes evaluation of change requests and change proposals and their subsequent approval or disapproval;

- Configuration status accounting, which includes the process of recording and reporting configuration item description and all departures from the baseline during design and production;

- Configuration verification and audit, which is an independent review of hardware and software for the purpose of assessing compliance with established performance requirements, appropriate standards, and product baselines.

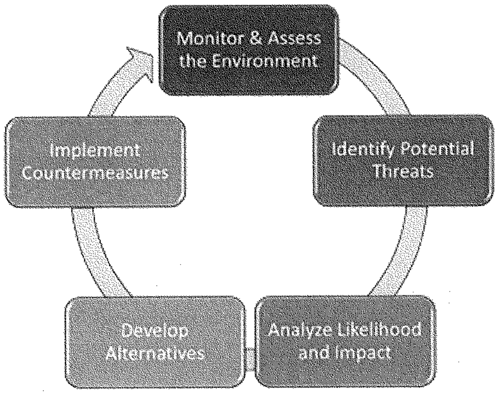
2. In-house and Third-party Quality Assurance Audits

Many security standards, such as NIST SP 800-53 Rev. 4, IEC 62443, ISO/IEC 15408, and the ISO 27000 series, are available to add further levels of assurance and rigor into the product development, production, and IT environments. Some manufacturers might consider third-party testing as an additional level of assurance.

**Recommendations:** The standards described above specify management systems that are intended to bring information security under explicit management control. Manufacturers should adopt a methodology and engage a third party to audit that methodology at agreed-upon periodic intervals.

3. Risk Management

According to the *US Department of Homeland Security (DHS) Risk Lexicon,* 2010 Edition, "risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken." The implication of this definition for manufacturers is that they have a method in place to deal with ongoing threats to their devices. This leads to the standard wheel diagram for risk management:


Monitor & Assess the Environment
Identify Potential Threats
Analyze Likelihood and Impact
Develop Alternatives
Implement Countermeasures

This diagram is not intended to illustrate the definitive method for designing a company's risk management system but to label the kind of considerations it should take into account. Additional considerations include:

- Internal versus external risks
- Communicating about risks and impacts to:
  - Upstream providers
  - Downstream asset owners

Many standards mention risk management approaches. Manufacturers might choose to follow (or evaluate for operational risk that would impact their security development life cycle and supply chain implications) the techniques described in any of the documents listed below.

- NIST SP 800-30 Rev.1 is a risk management guide for Information Technology Systems.
- ISO 31000 is a family of standards that provides principles and generic guidelines on risk management.
- The NIST Cybersecurity Framework provides a common language for understanding, managing, and expressing cybersecurity risk, both internally and externally.

4. In-house and Third-party Testing

There are several published standards that speak to the need for testing as a means to evaluate a particular system's compliance with its specified security requirements. Manufacturers might choose to implement the testing procedures described in these documents:

- NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (section 4.6) describes multiple types of testing (manual review, fuzz testing, static and dynamic analysis, penetration) that should be done throughout the system development life cycle.

- FIPS PUB 140-3 (section 4.9) specifies the testing requirements of the security functionality implemented in the cryptographic module.

**Recommendations:** At minimum, manufacturers should test their products or devices in order to validate compliance with the security requirements and necessities of the regulated environment. Depending on the environment, third-party testing might be required.

5. Incident, or Event, Management Plan

   **Recommendations:** Manufacturers should develop a plan to manage incidents or vulnerabilities. Ideally, it should include incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, monitoring the progress of the incident resolution, and a communication plan to inform affected parties about the status of the resolution.

   Manufacturers should maintain tight communication channels with consumers/customers and upstream suppliers in order to keep abreast of any vulnerability issues and steps to mitigate the issues.

   By extension, manufacturers should practice responsible disclosure. ISO/IEC 30111, *Information technology—Security techniques—Vulnerability handling processes* (sections 6-8) and ISO/IEC 29147, *Information technology—Security techniques—Vulnerability disclosure* (sections 6-9) are two standards that a manufacturer might choose to follow.

**DECOMMISSIONING/REVOCATION**

This section focuses on decommissioning and revocation processes to prevent compromised or obsolete devices from being used to penetrate active security networks. This can be especially important for manufacturers who deal in used or factory-refurbished equipment. When such a device is pulled from an active network, how does the manufacturer or asset owner dispose of it? For refurbished equipment, how is the privacy and security information wiped from the device to the satisfaction of regulators and customers? In some instances, the type of data that passed through the device might require that the device be destroyed or disabled.

**Identification of Threats**

1. Protection/Disposal of Legacy Data

   Legacy data present on any type of storage device should be protected in a secure format or properly deleted or disposed of in order to prevent its extraction or reuse. This data might reside somewhere on an asset owner network or some form of cloud storage in addition to the device. Data remanence should be taken into consideration, as this is the residual representation of digital data that can exist even after attempts have been made to erase it.

2. Physical Disposition/Destruction of Device

   With the physical destruction of a storage device, the primary goal is to render the disk physically inoperable or, at minimum, leave the platters severely fragmented.

3. Communication pathways

   A device pulled from an active network will have used some type of communication pathway (e.g., Ethernet, wireless, Bluetooth, internet). "Pivoting" refers to a method used by penetration testers that uses a compromised or obsolete system (whose media access control or MAC address is known to the network) to attack other systems on the network. Using the compromised system, an attacker has an improved aspect of remaining undetected and can leave less of a fingerprint.

**Analysis and Recommendations**

1. Protection/Disposal of Legacy Data

   **Recommendations:** At minimum, manufacturers should use purging/sanitization techniques to remove sensitive data from a system or storage device with the intent that the purged data cannot be reconstructed by any known technique. For those environments with stronger security requirements, manufacturers should consider using some type of self-encrypting hard drive that would render all data on the hard drive unreadable via a cryptographic erase of the data encryption key.

   The following standards address sanitization techniques that manufacturers might choose to follow.

   - NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization* (sections 3-5).

   - Department of Defense 5220.22M, *National Industrial Security Program Operating Manual* (chapter 5, section 7) addresses disposition and retention of classified information and materials.

2. Physical Destruction/Disposition of a Device

   **Recommendations:** Manufacturers should use any of the following options to physically destroy a hard disk drive: shredding the circuit boards into a size smaller than .5 inches, thereby destroying the flash memory in the process; drilling 6-10 holes with a sheet metal or masonry bit throughout the disk platters; heating the magnetic media to a particular temperature in order to deform the shape so that the data is completely removed.

   Physical destruction/disposition of a device is addressed in the following standards, which manufacturers might choose to follow.

   - NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization* (sections 3-5) is a guideline for media sanitization that includes destruction/disposal procedures.

   - Department of Defense 5220.22M, *National Industrial Security Program Operating Manual* (chapter 5, section 7) addresses the disposition and retention of classified information and materials.

3. Communication Pathways

   **Recommendations:** Manufacturers should remove/decommission the systems appropriately, rather than leaving them connected to a network. By performing penetration tests, manufacturers can actually replicate the types of actions a malicious attacker would take, providing a more accurate representation of a particular system's security posture. Penetration testing is the process of attempting to gain access to resources without knowledge of user-names, passwords, and other normal means of access. The primary factor that separates a penetration tester from an attacker is permission.

The wide variety of tools used in penetration testing consists of two main types: reconnaissance, or vulnerability, testing tools and exploitation tools. Several O/S distribution systems (popular examples include Kali Linux, Pentoo, and WHAX), geared toward penetration testing, are available.

## Appendix A
## REFERENCE DOCUMENTS

CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Reference Architecture* (November 2012)

*GridWise Interoperability Context-Setting Framework* (March 2008)

*Open Trusted Technology Provider™ Standard (O-TTPS)*, version 1.0 (April 2013)

SAFECode *Software Integrity Controls* document (June 2010)

NIST IR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems* (October 2012)

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015)—may replace some NIST IR7622 references in the future

IEC 62443-1-1:2009, *Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models* (July 2009)

ISO 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements* (September 2013)

ISO 27002:2013, *Information technology—Security techniques—Code of practice for information security controls* (September 2013)

SAE International Standards Organization, SA AS553, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition* (January 2013)

NIST SP.800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013)

IEC/TR 80002-1:2009, *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software* (September 2009)

FIPS PUB 140-3, *Security requirements for cryptographic modules* (Draft, September 2009)

NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* (September 2012)

NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010)

NIST SP 800-39, *Managing Information Security Risk* (March 2011)

Certificate Authority Security Council Code Signing Whitepaper

*Supply Chain Security Assurance* document (August 2013)

ISO 27799:2008, *Health informatics—Information security management in health using ISO/IEC 27002* (July 2008)

ISO/IEC 15408-1:2009, *Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model* (December 2009)

ISO 31000:2009, *Risk management—Principles and guidelines* (December 2009)

ISO 30111:2013, *Information technology—Security techniques—Vulnerability handling processes* (October 2013)

ISO 29147:2014, *Information technology—Security techniques—Vulnerability disclosure* (February 2014)

NIST *Cybersecurity Framework*, version 1.0 (February 2014)

NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* (November 2007)

IEC/TS 62351-1:2007, *Power systems management and associated information exchange—Data and communications security—Part 1: Communication network and system security—Introduction to security issues* (May 2007)

IEC/TS 62351-3:2007, *Power systems management and associated information exchange—Data and communications security—Part 3: Communication network and systems security profiles including TCP/IP* (June 2007)

IEC/TS 62351-4:2007, *Power systems management and associated information exchange—Data and communications security—Part 4: Profiles including MMS* (June 2007)

IEC/TS 62351-5:2013, *Power systems management and associated information exchange—Data and communications security—Part 5: Security for IEC 60870-5 and derivatives* (April 2013)

IEC/TS 62351-6:2007, *Power systems management and associated information exchange—Data and communications security—Part 6: Security for IEC 61850* (June 2007)

IEC/TS 62351-7:2010, *Power systems management and associated information exchange—Data and communications security—Part 7: Network and system management (NSM) data object models* (July 2010)

IEEE Std. 1619-2007, *IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices* (April 2008)

ISO/IEC 27033-1:2009, *Information technology—Security techniques—Network security—Part 1: Overview and concepts* (December 2009)

ISO/IEC 27033-2:2012, *Information technology—Security techniques—Network security—Part 2: Guidelines for the design and implementation of network security* (July 2012)

ISO/IEC 27033-3:2010, *Information technology—Security techniques—Network security—Part 3: Reference networking scenarios—Threats, design techniques and control issues* (Dec 2010)

ISO/IEC 27033-4:2014, *Information technology—Security techniques—Network security—Part 4: Securing communications between networks using security gateways* (February 2014)

ISO/IEC 27033-5:2013, *Information technology—Security techniques—Network security—Part 5: Securing communications across networks using Virtual Private Networks (VPNs)* (July 2013)

ISO/IEC 27036-1:2014, *Information technology—Security techniques—Information security for supplier relationships—Part 1: Overview and concepts* (March 2014)

ISO/IEC 27036-2:2014, *Information technology—Security techniques—Information security for supplier relationships—Part 2: Requirements* (August 2014)

ISO/IEC 27036-3:2013, *Information technology—Security techniques—Information security for supplier relationships—Part 3: Guidelines for information and communication technology supply chain security* (November 2013)

Energy Sector Control Systems Working Group (ESCSWG) *Cybersecurity Procurement Language for Energy Delivery Systems* (April 2014)

NIST SP 800-88, *Guideline for Media Sanitization Techniques* (September 2006)

Department of Defense (DoD) 5220.22M, *National Industrial Security Program Operating Manual* (February 2006)

Department of Homeland Security (DHS), *DHS Risk Lexicon* (September 2010)

## Appendix B
## REFERENCE ARCHITECTURES

Two reference architectures are applicable for the supply chain best practices described in the NEMA guideline document.

The first is the Smart Grid Architecture Model (SGAM) developed by the CEN-CENELEC-ETSI Smart Grid Coordination Group. The SGAM framework and its methodology are intended to present the design of smart grid use cases with an architectural approach allowing for a representation of interoperability viewpoints in a technology neutral manner, both for current implementation of the electrical grid and future implementations of the smart grid.

The SGAM framework consists of five layers representing business objectives and processes, functions, information exchange and models, communication protocols, and components. These layers represent an abstract and condensed version of the interoperability dimensions. Each layer covers the smart grid plane, which is spanned by electrical domains and information management zones. The intention of this model is to represent on which zones of information management interactions between domains take place. It allows presentation of the current state of implementations in the electrical grid, and also depicts the evolution to future smart grid scenarios by supporting the principles of universality, localization, consistency, flexibility, and interoperability.

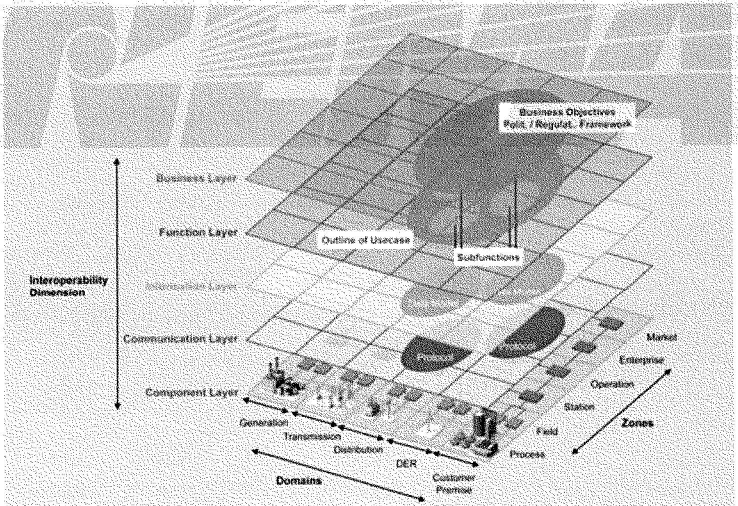


**Figure 1**
**SGAM Framework**

The business layer represents the business view on the information exchange related to smart grids.

The function layer describes functions and services, including their relationships, from an architectural viewpoint. The functions are represented independent from actors and physical implementations in applications, systems, and components. The functions are derived by extracting the use case functionality, which is independent from actors.

The information layer describes the information that is being used and exchanged between functions, services, and components. It contains information objects and the underlying canonical data models. These information objects and canonical data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.

The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service, and related information objects or data models.

The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired/wireless communication connections, routers, switches, servers), and any kind of computers.

In general, power system management distinguishes between electrical process and information management viewpoints. These viewpoints can be partitioned into the physical domains of the electrical energy conversion chain and the hierarchical zones (or levels) for the management of the electrical process. Applying this concept allows the foundation of the *Smart Grid Plane* (see Figure 1). The smart grid plane enables the representation on which levels (hierarchical zones) of power system management interactions between domains take place. The domains and their descriptions are listed in Table 1. The zones and their descriptions are listed in Table 2.

**Table 1**
**SGAM Domains**

| **Domains** | **Description** |
|---|---|
| **Bulk Generation** | Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, offshore wind farms, large-scale solar power plant typically connected to the transmission system |
| **Transmission** | Representing the infrastructure and organization that transport electricity over long distances |
| **Distribution** | Representing the infrastructure and organization that distribute electricity to customers |
| **DER** | Representing distributed electrical resources directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10,000 kW) |
| **Customer Premises** | Hosting end users and producers of electricity. The premises include industrial, commercial, and home facilities. |

**Table 2**
**SGAM Zones**

| Zones | Description |
|---|---|
| **Process** | Including the physical, chemical, or spatial transformations of energy (electricity, solar, heat, water, wind) and the physical equipment directly involved (e.g., generators, transformers, circuit breakers, overhead lines, cables, electrical loads—any kind of sensors and actuators that are part or directly connected to the process) |
| **Field** | Including equipment to protect, control, and monitor the process of the power system, e.g., protection relays, bay controller—any kind of intelligent electronic devices that acquire and use process data from the power system |
| **Station** | Representing the areal aggregation level for field level, e.g., for data concentration, functional aggregation, substation automation, local SCADA systems |
| **Operation** | Hosting power system control operation in the respective domain, e.g., distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems |
| **Enterprise** | Includes commercial and organizational processes, services, and infrastructures for enterprises (utilities, service providers, energy traders), e.g., asset management, logistics, work force management, staff training, customer relation management, billing and procurement |
| **Market** | Reflecting the market operations possible along the energy conversion chain, e.g., energy trading, mass market, retail market |

The second reference architecture is the GridWise Architecture Council (GWAC) Interoperability Framework.

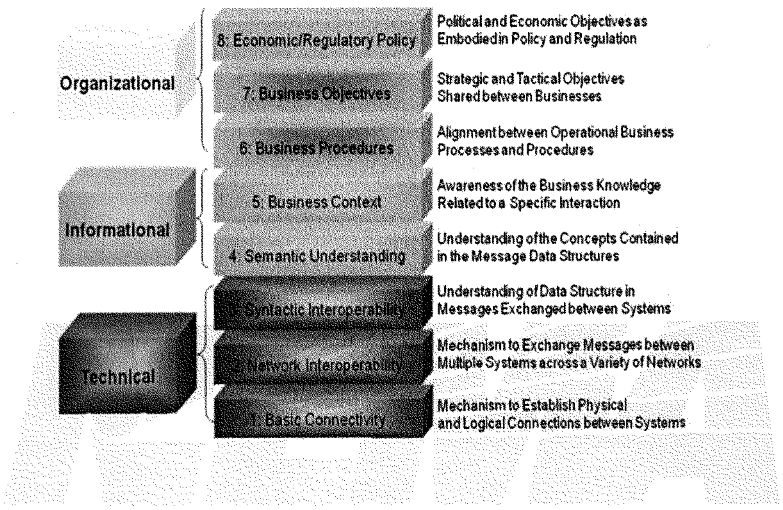

Organizational
Informational
Technical
8: Economic/Regulatory Policy
Political and Economic Objectives as Embodied in Policy and Regulation
7: Business Objectives
Strategic and Tactical Objectives Shared between Businesses
6: Business Procedures
Alignment between Operational Business Processes and Procedures
5: Business Context
Awareness of the Business Knowledge Related to a Specific Interaction
4: Semantic Understanding
Understanding of the Concepts Contained in the Message Data Structures
3: Syntactic Interoperability
Understanding of Data Structure in Messages Exchanged between Systems
2: Network Interoperability
Mechanism to Exchange Messages between Multiple Systems across a Variety of Networks
1: Basic Connectivity
Mechanism to Establish Physical and Logical Connections between Systems

**Figure 2**
**Interoperability Layered Categories Defined by GWAC**

The GridWise interoperability context-setting framework identifies eight interoperability categories that are relevant to the mission of systems integration and interoperation in the electrical end-use, generation, transmission, and distribution industries. The major aspects for discussing interoperability fall into the following categories: technical, informational, and organizational. The organizational categories emphasize the pragmatic aspects of interoperation. They represent the policy and business drivers for interactions. The informational categories emphasize the semantic aspects of interoperation. They focus on what information is being exchanged and its meaning. The technical categories emphasize the syntax or format of the information. They focus on how information is represented within a message exchange and on the communications medium.

Basic Connectivity focuses on the digital exchange of data between two systems and the establishment of a reliable communications path. This is achieved by agreeing to conform to specifications describing the data transmission medium, the associated low-level data encoding, and the transmission rules for accessing the medium. Network Interoperability pertains to agreement on how to address the issues arising from transporting information between interacting parties across multiple communication networks. Syntactic Interoperability refers to agreement on the rules governing the format and structure for encoding information exchanged between transacting parties.

Semantic Understanding refers to rules governing the definition of things, concepts, and their relationship to each other. Together, they make up an informational "model" of how the world works. A model is usually "domain-specific", e.g., pertaining to one area of expertise. The idea of establishing a business context refers to restricting and refining the aspects of an information model relevant to the specific business process in question.

Effective information interoperability between business organizations requires that the involved organizations have compatible processes and procedures across their interface boundaries. In addition, it's required that the strategic and tactical objectives of the business organizations be complementary and compatible. Business organizations require that the political and regulatory policies that govern commerce provide the proper environment, incentives, or both, to build business relationships with other organizations, some of which might be considered competitors. This includes national, state, and local governance.

NOTE—No reference architecture exists for embedded systems that include hardware or affected physical systems in a generic fashion.

CHiME & AEHiS

## Statement from the College of Healthcare Information Management Executives and the Association for Executives in Healthcare Information Security

House Committee on Energy and Commerce
Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing and Trade

Hearing on "*Understanding the Role of Connected Devices in Recent Cyber Attacks*"

2322 Rayburn House Office Building

November 16, 2016

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit a statement for the record of the November 16, 2016, Committee on Energy and Commerce joint hearing with the Subcommittee on Communications and Technology and the Subcommittee on Commerce, Manufacturing and Trade entitled, "Understanding the Role of Connected Devices in Recent Cyber Attacks." We appreciate the committee's interest in this timely issue and welcome the opportunity to offer perspective from the nation's healthcare chief information officers and chief information security officers.

CHIME is an executive organization serving more than 2,000 CIOs and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformati on. CHIME members are among the nation's foremost health IT experts including cybersecurity. Within CHIME is AEHIS, an organization launched in 2014 which represents more than 600 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems.

**Cybersecurity in the Healthcare Industry**
The Department of Homeland Security deems healthcare one of the nation's 16 critical infrastructure sectors. Already highly-regulated, healthcare organizations are subject to both divergent and duplicative guidance on data security and privacy by various federal entities, state regulators and business agreements. Through market pressures and regulatory requirements, including Meaningful Use and the shift to alternative payment models, CIOs and CISOs have been working feverishly over the past decade to transform their healthcare systems to become digital enterprises. This includes trying to balance the need for enabling providers with the capability for having immediate access to electronic protected health information (ePHI), while at the same time maintaining strict cybersecurity protocols.

There are several unique distinctions of the healthcare sector's data security environment that warrant consideration, including:

- Healthcare's highly-regulated environment
- The various settings where healthcare is delivered
- Limited resources available to devote to information technology and security
- Healthcare's unique financial models
- Frequency and volume of data exchange within healthcare delivery
- The increasingly mobile nature of healthcare technology and healthcare delivery

Healthcare has entered an era of ubiquitous connection, and the internet of things (IoT) is transforming healthcare along with the world's economy. Just in healthcare alone, the growth of IoT connections from 2014 to 2015 increased by 26 percent.[1] Smart devices at the point of care (i.e. heart monitors, infusion pumps, fitness trackers) and throughout the entire healthcare system (i.e. smart toasters and vending machines), are often connected to the same broader network. Wearables and additional devices are being connect to electronic health record (EHR) systems, which generates additional data for clinical decision making but also increases the threat surface with the addition of yet another device. Patient records are accessed remotely on clinician laptops and are stored in the cloud, which introduces another realm of security threats. The lines between commercial consumer devices and medical devices are blurring rapidly, thus it is vital to view the recent cyber attacks holistically and recognize the importance of coordination across all critical infrastructure sectors.

Much of the attention in healthcare when it comes to cybersecurity is centered on data breaches and threats to patient information. Unfortunately, medical devices also present and expand threat attack surfaces, as these devices can be directly connected or implanted in a patient. Often, these devices are connected to the hospital network and upload vital information to electronic health records. Medical device vendors use the internet to link to their machines to install updates or patches. Unfortunately, weak security protocols make medical devices prime candidates for us in distributed denial of service (DDoS) attacks like that on Dyn. These attacks can be extremely detrimental and have grave consequences on patient care.

**Networked Medical Devices**

Tens-of-thousands of medical devices can be used throughout large healthcare systems, many of which, as stated above, are connected directly to the patient or serving to provide information to inform clinical decision making. The lifecycle of a medical device within a healthcare institution can be lengthy as the cost to replace them can be crippling. Given the intent to employ devices for upwards of 10 to 15 years, many of the devices in place today were not developed or intended to be networked, yet the U.S. Chamber of Commerce Technology Engagement Center/ Morning Consult survey says 61% of respondents believe that in the near future it will be "important" or "somewhat important" that medical devices that monitor your heart rate to be connected to the internet.[2] Given the consumer expectations about devices being networked, we must ensure proper security management, including thorough risk assessments and risk treatment, are incorporated in the device's design. Meanwhile, wearables and remote monitoring technologies are on the uptick making blurring the links between what are strictly consumer devices and what is a medical device. As more connected devices enter the healthcare realm, additional attack surfaces and vulnerabilities become available to bad actors.

The highly interconnected nature of medical devices, combined with the constraints of inconsistent patching cycles, has created an ecosystem ripe with technical vulnerabilities that cannot be managed with standard processes and procedures. Some examples of existing challenges posed by networked medical devices within healthcare delivery organizations include:

- Medical devices are being released into the marketplace often without basic security requirements in place such as: encryption, access control mechanisms, passwords that can be changed by healthcare organizations, and the ability to restrict access controls.
- Known vulnerabilities within medical devices cannot be patched or mitigated in a timely manner due to the requirement that device manufacturers follow extensive quality control processes. Additionally, in many cases it is not possible to patch a device without first investing in an upgrade to newer versions, and threats of device warranties being voided if patches are done by the healthcare provider. Upgrades can be quite costly and usually require long planning cycles in order to secure the correct budget. Purchasing new equipment to remediate security vulnerabilities is not always the best or most realistic answer for the healthcare industry.
- Medical devices are increasing their storage capacities, which potentially increases the amount of patient data stored on these devices. This creates significant risk to patient privacy and compliance challenges with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).
- There are no expiration dates on Food and Drug Administration (FDA) pre-market approvals for medical IT devices despite medical device manufacturer and FDA knowledge of end of support dates for major operating systems.

The FDA has increased its focus on the critical issues surrounding cybersecurity of medical devices and their impact on patient safety. From a healthcare provider perspective, the ever increasing interconnectedness of

[1] *State of the Market: Internet of Things 2016, https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf*

[2] *Internet of Things, Most Americans Don't Know What Caused Recent Internet Outages, http://ctecintelligence.com/*

medical devices into a health systems operating network has become an area of great concern. We believe an increased and formalized collaboration between the medical device manufacturers and healthcare organizations is critical. For several decades, there has been a tension between the identification of medical device vulnerabilities and the device manufacturer's capability to mitigate or manage those risks. Generally speaking, when a device vulnerability is discovered or enumerated, these vulnerabilities cannot be easily rectified due to costly quality control mechanisms, such as 21 CFR Section 806.

This has become even more of a problem as general operating systems, such as Microsoft Windows, are considered integral components of the medical device architecture and must be managed through these same quality control mechanisms. Security vulnerabilities resulting from these types of operating systems are occurring at a much higher frequency than manufacturers can resolve. CIOs and CISOs are generally left with managing devices on isolated and segregated networks with the hopes of reducing their exposure to threats. This, however, has proven to be ineffective.

**Improving Security of Networked Medical Devices**

To better safeguard healthcare systems and the patient data they have been entrusted to protect, we must improve threat and incident information sharing across the industry. No single sector of the healthcare ecosystem can solve the problem alone. Only by pulling together and sharing best practices can we thwart cyber criminals and protect patients. This type of collaboration is vital towards remaining nimble to the threats of today, for every day a new threat is introduced into the industry. Today it is ransoming an institutions data or operations, tomorrow it could be holding hostage the ability to deliver care through medical devices. The vehicle by which the threat is delivered will change, but we know for a fact that criminals will look at introducing "new markets" for extorting money above and beyond what they are doing today.

CHIME and AEHIS are pleased with the important advances recommended in the Cybersecurity Information Sharing Act of 2015. The healthcare-specific directives, particularly the cyber resources that are to be scalable to the entire industry and the coordination plan across the Department of Health and Human Services (HHS) will be important to move the industry forward. In addition, discussions and clarification on what Information Sharing Analytics Organizations (ISAO) can and cannot share will be very beneficial. Many ISAO participants are concerned about minimum necessary and appropriate use guidelines as dictated by HIPAA in a CISA/ISAO environment.

Further, we have seen proactive initiatives from the administration, including efforts to evaluate needed enhancements to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, a crosswalk of HIPAA to the NIST Framework and draft guidance from FDA on the post-market cybersecurity management of medical devices. It will be imperative for the industry to work in conjunction with the administration and Congress to ensure healthcare providers are best positioned to combat cyber threats.

The recent spate of publically reported networked medical device vulnerabilities disclosed by security researchers has garnered attention from patients, providers and most recently lawmakers[3]. With the changes finalized by the U.S. Copyright Office of the Library of Congress in October 2015, which contained several exemptions to the Digital Millennium Copyright Act, including expanded access to medical device computer programs and the patient data they generate, it is anticipated to that the detection of new device vulnerabilities will increase.

CHIME and AEHIS offer some suggestions for consideration as the sector matures in its efforts to improve the cyber hygiene of networked medical devices:

1. Signal that the security of a device must be considered when evaluating the safety and efficacy of its performance. In conjunction with the FDA, Congress should ensure that manufacturers configure their devices according to an industry accepted security standard that accounts for the basic principles of cybersecurity controls and alleviates risks. Manufacturers should, as part of the pre-market approval process, be required to undergo a level of security validation in order to provide healthcare providers with a very simple and easy to implement mechanism for managing its security.
2. Ensure that the FDA is able to oversee vulnerability submissions and notification of risks to providers, as all known device risks should be reported to the healthcare delivery organizations that own said devices. "Controlled" risks should be reported on a regular basis (i.e. quarterly) and "uncontrolled" risks on an immediate basis. The definition of controlled vs. uncontrolled risks should encompass both patient safety and patient privacy issues. Cybersecurity risks in the medical device space should be classified either as "risks to patient safety" or "risks to patient privacy" to provide a more holistic view of the cybersecurity ecosystem.

[3] *Letter from Representatives Diana DeGetter and Susan Brooks to FDA Commissioner Califf and CDRH Director Shuren, November 3, 2016*

3. Support the expansion of programs similar to the NIS National Cybersecurity Center of Excellence (NCCoE)'s work to investigate how to improve the wireless intravenous (IV) medical infusion pump security by focusing on device security risk assessment and risk management.

As the committee continues to evaluate the cyber threat landscape, we urge members to ensure that networked medical devices factor into the broader conversation of consumer-facing devices that could be leveraged in a denial of service cyber-attack or manipulated to cause harm to patients. A more proactive policy management process is vital for healthcare organizations. Viewing security as a component of safety and efficacy of device functions is necessary to keep pace with these variable threats. A secure healthcare system will ultimately enable greater consumer confidence and will spur better care coordination, enhanced information exchange and improved patient care.

AdvaMed
Advanced Medical Technology Association

**AdvaMed, the Advanced Medical Technology Association**
**Statement for the Record**

**Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology**
**"Understanding the Role of Connected Devices in Recent Cyber Attacks"**

**Wednesday, November 16, 2016**

AdvaMed is the world's largest trade association representing medical technology manufacturers. AdvaMed member companies produce the medical devices, diagnostic products and health information systems that are transforming health care through earlier disease detection, less invasive procedures and more effective treatments.

Patient safety is critical to the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve.

Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. Similarly, manufacturers implement proactive and risk-based approaches to manage medical device cybersecurity, including the use of "good cyber hygiene" through routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

It is important that whenever potential vulnerabilities involving a medical device are discovered, such findings should first be brought to the attention of the manufacturer for review, analysis, and possible remediation. Any other approach potentially places patients' lives at risk.

Additionally, medical technology cybersecurity is a shared responsibility among all stakeholders, including manufacturers, hospitals, physicians, and users. Device manufacturers play an important role; however, all stakeholders within the larger system must work together to ensure system-level integrity.

The medical technology industry is actively working with FDA and other key stakeholders to raise awareness about potential cybersecurity concerns, and we look forward to working with all stakeholders to further these efforts.

**FOR IMMEDIATE RELEASE**

|  |  |  |  |
|---|---|---|---|
| **Contact:** | **Bronwyn Flores**<br>**703-907-7679**<br>**bflores@CTA.tech**<br>***www.CTA.tech*** | **or** | **Tyler Suiters**<br>**703-907-7654**<br>**tsuiters@CTA.tech** |

## Statement for the Record Joint Hearing of the Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology House Energy and Commerce Committee Understanding the Role of Connected Devices in Recent Cyber Attacks

**Arlington, VA, November 16, 2016** – The following statement is attributed to Gary Shapiro, president and CEO, Consumer Technology Association (CTA)™:

"Implementing strong security of our IoT devices and systems is an important issue for the technology industry and the nation overall, given the recent series of scripted DDoS attacks.

"The IoT offers an amazing opportunity to change the way our world works – enhancing our health care while reducing costs; providing increased security or automated approaches to dangerous jobs; offering more personalized services and experiences; increasing energy savings through greater efficiencies; and so much more – all while driving an estimated trillions of dollars in new economic value. As with any immense opportunity, there are risks involved – in this case, bad actors who in the name of chaos or blackmail disrupt the communication and connectivity we all depend on. But we must not let these cybercriminals hinder innovation and the countless ways in which technology is changing our lives for the better.

"To that end, the industry can consider adopting a set of best practices for security, including developing voluntary testingand certification programs which buyers may use to specify and identify products. CTA is working with our member companies – among the key players in the future of the IoT and its evolution – on multiple programs across tech market categories including self-driving vehicles, health and wellness devices, and smart home technology. Our recent work includes revising CTA-TR-12, *Securing Connected Devices for Consumers in the Home*, which provides guidance to product designers and managers on how to enhance cybersecurity; developing guidance for product installers to get the best security out of existing devices; and helping develop and launch the Building Security In Maturity Model (BSIMM) online assessment tool, which companies can use to gauge how well they're addressing security in their internal processes and end products.

"Consumers also can take steps to enhance the security of their connected devices including changing default passwords supplied with the products, buying well-known brands and having their systems installed by certified professionals.

“The government should facilitate dialogue  and set achievable expectations for industry stakeholders rather than rush regulations which slow innovation and raise prices on consumers. We will continue to work closely with the tech industry and government to improve IoT security measures and fully enable the remarkable – sometimes life-saving – benefits technology holds for us all.”

**About Consumer Technology Association:**

Consumer Technology Association (CTA)™, is the trade association representing the $287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world’s best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. The Consumer Technology Association also owns and produces CES® – the world’s gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA’s industry services.

# # #