

# **SMALL BUSINESS CYBERSECURITY: FEDERAL RESOURCES AND COORDINATION**

---

## **HEARING BEFORE THE COMMITTEE ON SMALL BUSINESS UNITED STATES HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS**

**FIRST SESSION**

---

**HEARING HELD  
MARCH 8, 2017**

---



Small Business Committee Document Number 115-007  
Available via the GPO Website: [www.fdsys.gov](http://www.fdsys.gov)

---

U.S. GOVERNMENT PUBLISHING OFFICE

24-421

WASHINGTON : 2017

---

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: [bookstore.gpo.gov](http://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

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*

STEVE KING, Iowa

BLAINE LUETKEMEYER, Missouri

DAVE BRAT, Virginia

AUMUA AMATA COLEMAN RADEWAGEN, American Samoa

STEVE KNIGHT, California

TRENT KELLY, Mississippi

ROD BLUM, Iowa

JAMES COMER, Kentucky

JENNIFER GONZALEZ-COLON, Puerto Rico

DON BACON, Nebraska

BRIAN FITZPATRICK, Pennsylvania

ROGER MARSHALL, Kansas

VACANT

NYDIA VELÁZQUEZ, New York, *Ranking Member*

DWIGHT EVANS, Pennsylvania

STEPHANIE MURPHY, Florida

AL LAWSON, JR., Florida

YVETTE CLARK, New York

JUDY CHU, California

ALMA ADAMS, North Carolina

ADRIANO ESPAILLAT, New York

BRAD SCHNEIDER, Illinois

VACANT

KEVIN FITZPATRICK, *Majority Staff Director*

JAN OLIVER, *Majority Deputy Staff Director and Chief Counsel*

ADAM MINEHARDT, *Staff Director*

## C O N T E N T S

### OPENING STATEMENTS

	Page
Hon. Steve Chabot .....	1
Hon. Nydia Velázquez .....	2

### WITNESSES

The Honorable Maureen K. Ohlhausen, Acting Chairman, Federal Trade Commission, Washington, DC .....	4
Chuck Romine, Ph.D., Director, Information Technology Lab, National Institute of Standards and Technology, Gaithersburg, MD .....	6
Mr. Charles Rowe, President & CEO, America's Small Business Development Centers, Arlington, VA .....	7
Mr. Jim Mooney, President and CEO, Chevron Federal Credit Union, Cybersecurity Committee Chair, National Association of Federally-Insured Credit Unions, Arlington, VA, testifying on behalf of the National Association of Federally-Insured Credit Unions .....	9

### APPENDIX

#### Prepared Statements:

The Honorable Maureen K. Ohlhausen, Acting Chairman, Federal Trade Commission, Washington, DC .....	22
Chuck Romine, Ph.D., Director, Information Technology Lab, National Institute of Standards and Technology, Gaithersburg, MD .....	34
Mr. Charles Rowe, President & CEO, America's Small Business Development Centers, Arlington, VA .....	42
Mr. Jim Mooney, President and CEO, Chevron Federal Credit Union, Cybersecurity Committee Chair, National Association of Federally-Insured Credit Unions, Arlington, VA, testifying on behalf of the National Association of Federally-Insured Credit Unions .....	48
Questions for the Record:	
Questions and Responses from Hon. Adriano Espaillat to Hon. Maureen K. Ohlhausen .....	77
Questions and Responses from Hon. Adriano Espaillat to Chuck Romine, Ph.D. ....	79
Questions and Responses from Hon. Adriano Espaillat to Charles Rowe ...	82
Questions and Responses from Hon. Adriano Espaillat to Jim Mooney ....	85
Additional Material for the Record:	
ICBA - Independent Community Bankers of America .....	87



## **SMALL BUSINESS CYBERSECURITY: FEDERAL RESOURCES AND COORDINATION**

---

**WEDNESDAY, MARCH 8, 2017**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON SMALL BUSINESS,  
*Washington, DC.*

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building, Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Luetkemeyer, Knight, Kelly, Blum, Comer, Bacon, Fitzpatrick, Velázquez, Evans, Murphy, Lawson, Clarke, Espaillat, and Schneider.

Chairman CHABOT. Good morning. I will call the Committee to order now. And we want to thank everyone for coming today.

Over the past year, this Committee has turned its attention to an issue that is increasingly serious for small business, and that is cybersecurity. In past hearings, we heard firsthand accounts from small business owners who have been victims of cyberattacks.

We have also heard dire warnings from cybersecurity experts about the new and varied cyber threats facing America's 28 million small businesses.

There is no question that advances in information technology have helped small businesses to increase their productivity, become more efficient, and ultimately more successful.

However, the same tools and resources that have given small business owners a greater role in the marketplace have also provided cyber criminals and foreign bad actors with more opportunities to steal sensitive and valuable information that small businesses rely on to remain competitive.

In 2015 alone, the United States Department of Justice recorded nearly 300,000 cybersecurity complaints.

We have also learned that a cyber attack can have serious consequences, not only for small businesses, but also their customers and their employees and business partners. Sixty percent of small businesses that fall victim to a cyberattack close up shop within 6 months. Sixty percent. A 2014 survey from the National Small Business Association estimated the average cost of cyber attacks on a small business to be over \$32,000.

In our Committee's efforts to spotlight these serious and growing threats, it has been abundantly clear that the Federal Government needs to step up its game when it comes to protecting the cybersecurity of small businesses and individuals. And, to some extent, Federal agencies have begun offering resources directly to small businesses in recent years.

Today we will hear from some of the Federal agencies that are already providing cybersecurity resources to small businesses. We will examine how these tools can be more easily accessed by small business owners and ensure that they are effective.

Since the late 1990s, the Federal Government has become increasingly active in protecting our Nation's critical infrastructure and information technology, IT, systems. It has gone to great lengths to coordinate these efforts with State and local governments, as well as the private sector. However, it was not until recently that the Federal Government was encouraged to engage in greater information-sharing practices with businesses through the development of an overall framework for cybersecurity protocols. The framework would enable businesses of all sizes to implement a set of best practices for assessing cyber threats and reinforce their cybersecurity systems.

Just last year, the House passed the Improving Small Business Cybersecurity Act, a bill that helps small businesses facing cyber threats by providing access to additional tools and resources through existing Federal cyber resources. The bill became law as part of the National Defense Authorization Act of 2017. The Department of Homeland Security, DHS, and other Federal agencies have been permitted to work through the Small Business Development Centers, SBDCs, to streamline cyber support and resources for small businesses.

While I believe this is a very good start, I think it is glaringly obvious that Federal agencies tasked with providing cybersecurity resources to small businesses can be better coordinated. They should drive down duplicative resources and processes and ensure that small businesses are equipped to deal with the growing cyber threats.

I look forward to hearing from our witnesses and their points of view on how we can more efficiently disseminate Federal cybersecurity resources to all of America's small businesses, and I would now like to yield to the ranking member for her opening statement.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Developing new innovations is fundamental to our nation's prosperity in the 21st century. But these technologies can only be beneficial if small businesses can adopt them without fear of malicious cyberattacks. Cybercrimes are becoming more commonplace and more sophisticated. And no matter what form they take, they can be devastating to business owners and their customers. A single attack can wipe out a small business, making cybercrime a severe problem for small entities.

While businesses of all sizes must increasingly monitor cyber threats, small firms must prepare for these problems with far fewer resources than their larger counterparts. Because of the complexity and cost associated with implementing a security plan, only 31 percent of small firms take active measures to guard against such attacks.

More than 80 percent of the time, the owner handles cybersecurity personally, making small firms more vulnerable than a competitor with a dedicated IT security consultant or staff mem-

ber. In fact, last year, 60 percent of all targeted attacks struck small- and medium-sized entities.

These actions have costly implications for the small companies. The average cost of a data breach is nearly \$200,000, and leads to 60 percent of targeted small businesses closing their doors within 6 months of being attacked.

Because small firms stand to lose so much without data protection, it is imperative that they have the resources of the federal government at their disposal. The federal government has a duty to secure federal information systems and assist in protecting private systems.

All agencies have their own duty to protect their systems, but due to rapid changes in cyberspace, agency roles are complex. The presence of over 50 relevant statutes addressing various aspects of federal cybersecurity responsibilities adds yet more confusion. And because agencies are busy navigating the rules pertaining to their own systems, efforts to help small firms have generally been neglected.

However, the Department of Defense and Homeland Security, and the National Institute of Standards and Technology, have all recently embarked on efforts to assist businesses with cybersecurity needs.

Additionally, federal spending on cybersecurity is expected to rise above \$20 billion over the next several years. Implementation of the Cybersecurity Information Sharing Act of 2015 continues moving ahead. Despite this progress, collaboration between agencies and small firms is lacking, which affects us all.

We must improve our efforts to help small businesses overcome these challenges. I was pleased, for example, that the National Defense Authorization Act includes a provision instructing SBA to coordinate with DHS to develop a small business cyber strategy.

Most importantly, it leverages the SBA's vast network of Small Business Development Centers, which have a proven record of helping entrepreneurs all over the country.

Although this is a step in the right direction, we must do more to encourage small firms to protect themselves and their customers from cyber threats. Today's hearing will give us an opportunity to review federal investment in cybersecurity and how we can facilitate collaboration with the small business community. We cannot accept the bare minimum as our nation seeks to end continued data breaches.

With that, I want to thank all the witnesses for being here today, for your participation and insights into this important topic.

I yield back, Mr. Chairman.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

And if Committee members have opening statements prepared, we would ask that they be submitted for the record.

And I will now take just a moment to explain our lighting system. It is really pretty simple. Each of you get 5 minutes. We all get 5 minutes. And the lights will assist you in kind of keeping within that. The green light will stay on for the first 4 minutes. The yellow light will come on to let you know you have got about a minute to wrap up. And then the red light will come on, and,

hopefully, you are finished by that time or will be shortly thereafter. So if you could stay within those, we would greatly appreciate it.

And I would like to introduce our very distinguished panel here this morning. I will begin with our first witness.

Maureen Ohlhausen, who is acting chairman of the FTC, Federal Trade Commission. She was sworn in as the commissioner back in 2012. She also served as director of the Office of Policy Planning from 2004 to 2008, where she led the FTC's Internet Taskforce. And we welcome you this morning.

Our second witness will be Chuck Romine, director of the Information Technology Lab at the National Institute of Standards and Technology. Dr. Romine oversees a program that promotes U.S. innovation and industrial competitiveness by developing standards and guidelines for Federal agencies and U.S. industry, and we welcome you here, Doctor.

And our third witness will be Tee Rowe, who is the president and CEO of America's Small Business Development Centers. He is also the chairman of the Small Business Legislative Council and a member of the U.S. Chamber of Commerce's Council on Small Business. Mr. Rowe also served the Small Business Committee for 10 years as counsel. So welcome back.

And I would now like to yield to the ranking member to introduce our fourth witness.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

It is my pleasure to introduce Mr. James Mooney, President and CEO of Chevron Federal Credit Union, located in California, and serving members since 1935. Mr. Mooney is also the Cybersecurity Committee Chair for the National Association of Federally-Insured Credit Unions, NAFCU. He is testifying on behalf of NAFCU, which is the only national organization exclusively representing the nation's federally-insured credit unions. Welcome. Thank you for being here.

Chairman CHABOT. Thank you very much.

And now we will hear from our distinguished panel. And Ms. Ohlhausen, you are recognized for 5 minutes.

**STATEMENTS OF THE HONORABLE MAUREEN K. OHLHAUSEN,  
ACTING CHAIRMAN, FEDERAL TRADE COMMISSION; CHUCK  
ROMINE, PH.D., DIRECTOR, INFORMATION TECHNOLOGY  
LAB, NATIONAL INSTITUTE OF STANDARDS AND TECH-  
NOLOGY; CHARLES ROWE, PRESIDENT AND CEO, AMERICA'S  
SMALL BUSINESS DEVELOPMENT CENTERS; JIM MOONEY,  
PRESIDENT AND CEO, CHEVRON FEDERAL CREDIT UNION,  
CYBERSECURITY COMMITTEE CHAIR, NATIONAL ASSOCIA-  
TION OF FEDERALLY-INSURED CREDIT UNIONS**

**STATEMENT OF MAUREEN K. OHLHAUSEN**

Ms. OHLHAUSEN. Chairman Chabot, Ranking Member Velázquez, and members of the Committee, I am Maureen Ohlhausen, the Acting Chairman of the Federal Trade Commission. And I appreciate the opportunity to present the Commission's testimony on data security and, in particular, our efforts to coordinate

with our partners at NIST, who I am pleased to be with here today, and the SBA, to educate small business.

Data breaches are commonplace, and in the case of small business, a data breach can be devastating. While they may never make headlines, the majority of attacks target small- and midsized companies. And as you already mentioned, according to the National Cybersecurity Alliance, some 60 percent of all small businesses shutter their doors within 6 months of a breach.

The Federal Trade Commission is a small, independent agency with a large role to play when it comes to data security, and we are committed to protecting consumer privacy and promoting data security in the private sector through enforcement and education.

The Commission enforces several statutes and rules that place data security requirements on companies: the Gramm-Leach-Bliley Act, which covers certain financial institutions; the Children's Online Privacy Protection Act covering children's information; and the Fair Credit Reporting Act covering credit report information. The Commission also enforces the FTC Act, which applies to a broad range of companies.

The core requirement under each of these laws is that companies must maintain reasonable security. None of the laws contain prescriptive, detailed legal requirements; rather, their requirement of reasonable security is a flexible one that is scalable for small companies. A company's data security measures must be reasonable in light of the sensitivity of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.

Since 2001, the Commission has used its authority to take action against approximately 60 companies that it charged with failing to provide reasonable protections for consumers' personal information. In each of these cases, the data security failures were not merely isolated mistakes. Instead, the Commission challenged alleged data security failures that were multiple and systemic. The Commission has made clear that it does not require perfect security, that there is no "one size fits all" data security program, and that the mere fact that a breach occurred does not mean that a company has violated the law.

In addition to law enforcement, the FTC offers guidance to help businesses of all sizes improve their data security practices. In November, we released an update to "*Protecting Personal Information: A Guide for Business*," a guide we first published in 2007. Last fall, the FTC released guidance describing immediate steps companies should take when they experience a data breach. And in 2015, the FTC launched its *Start with Security* initiative, which includes a guide for business that summarizes the lessons learned from the FTC's data security cases. As part of this initiative, the FTC hosted events across the country, bringing business owners together with industry experts to discuss practical tips and strategies for implementing effective data security. Last year, staff presented our *Start with Security* materials to thousands of small business owners on six cybersecurity webinars sponsored by NIST and the SBA.

We are especially sensitive to the needs of small business. Sole proprietors and companies with just a few employees generally do not have full-time information technology or human resources staff,

and that is why I have directed FTC staff to create a one-stop shop on our website with materials specifically for small business. And in the coming months, we will expand our business outreach on data security issues with a focus on helping very small companies identify risks and develop data security plans.

So thank you for the opportunity to provide the Commission's views, and we look forward to continuing to work with the Committee and Congress on this critical issue.

Chairman CHABOT. Thank you very much.

Dr. Romine, you are recognized for 5 minutes.

#### **STATEMENT OF CHUCK ROMINE**

Dr. ROMINE. Chairman Chabot, Ranking Member Velázquez, members of the Committee, thank you for the opportunity to appear before you today to discuss NIST's cybersecurity efforts as they relate to small businesses.

The IT security challenge for small businesses looms larger than ever. Since nearly 99 percent of all U.S. businesses are small- or medium-sized, a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security.

NIST has worked with Federal agencies, industry, and academia in cybersecurity since 1972. NIST's role to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was reaffirmed in the Federal Information Security Modernization Act of 2014.

In 2016, NIST released a major revision to the popular report, "Small Business Information Security: The Fundamentals." The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems.

NIST's framework for improving critical infrastructure cybersecurity, or the framework, was released 3 years ago. The framework's voluntary, risk-based, prioritized, flexible, repeatable, and cost-effective approach was developed for use by organizations, including small businesses, to help manage cybersecurity-related risk. Key to the continuing success of the framework is that it is voluntarily implemented by industry and voluntarily adopted by infrastructure sectors.

In addition to the cybersecurity framework, NIST has developed over the past decade an extensive set of security standards and guidelines, including a risk management framework that can be customized for small businesses and voluntarily implemented to help protect intellectual property and organizational assets.

Building on the success of the cybersecurity framework and the Baldridge Performance Excellence Program, NIST released the draft Baldridge Cybersecurity Excellence Builder, a self-assessment tool, to help organizations of all sizes better understand the effectiveness of their cybersecurity risk management efforts. Using the Builder, organizations of all sizes can determine cybersecurity-related activities that are important to business strategy and the de-

livery of critical services, and prioritize investments in managing cybersecurity risk.

Since 2001, NIST has partnered with the Small Business Administration and the Federal Bureau of Investigation's InfraGard program to sponsor regional computer security workshops and provide online support for small businesses. The workshops feature security experts who explain information security threats and vulnerabilities, and describe protective tools and techniques that can be used to address potential security problems. In 2016, NIST partnered with the SBA, the Federal Trade Commission—I am grateful that we are here together—and the Department of Energy, to provide cybersecurity training webinars to hundreds of small businesses.

The National Initiative for Cybersecurity Education, or NICE, led by NIST, released the draft NICE Cybersecurity Workforce Framework in 2016, to help our Nation more effectively identify, recruit, develop, and maintain its cybersecurity talent.

NIST is also piloting the establishment of alliances to coordinate regional activities addressing the cybersecurity workforce shortage.

The NIST National Cybersecurity Center of Excellence, or NCCoE, collaborates with experts from industry, academia, and government to create and promote standards-based solutions to real world cybersecurity problems using commercially available products in the form of technical practice guides that can be used by organizations, including small- and medium-sized businesses.

The NCCoE project on mobile device security, for example, provides guidance on the implementation of capabilities to secure sensitive business data residing in the cloud and being accessed by employees on mobile devices.

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the IT security challenge looms larger than ever. The NIST programs described today demonstrate that NIST cybersecurity portfolio is applicable to a wide variety of users, including small businesses.

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

Thank you for the opportunity to present NIST's views regarding security challenges facing small businesses. I will be pleased to answer any questions that you may have.

Chairman CHABOT. Thank you very much, Doctor.

Mr. Rowe, you are recognized for 5 minutes.

#### **STATEMENT OF CHARLES ROWE**

Mr. ROWE. Chairman Chabot, Ranking Member Velázquez, members of the Committee. Thank you for inviting me to testify on behalf of America's SBDCs.

SBDCs operate in all 50 States and D.C., Puerto Rico, the Virgin Islands, American Samoa, and Guam. Every year, SBDCs assist over 200,000 small businesses, and last year we helped those clients gain nearly \$7 billion in sales.

But that statistic comes with a hidden peril, cybercrime. More of our clients do business online, and every one of them is vulnerable. They want to do more business online, but they have weaker online security, and they can be a gateway to clients, partners, and contractors. And those secondary attacks are now a regular problem for our small business clients.

And not all hacking is for financial gain. Two years ago, websites were plastered with Islamic State logos; among them, Montauk Manor in New York and El Dora Speedway in Ohio. No financial information was stolen, but they had to rebuild their sites and restore client confidence.

SBDCs are working to spread awareness of these threats and build training programs at SBDCs all across the country. Around the Nation, we are developing programs to build capacity and our training skills. In Florida, our network is working with former DHS Secretary Tom Ridge to develop a series of training videos. The New York SBDC published a cybersecurity planning guide, which I think all of you have in front of you, which we are disseminating to other States to help them build their capacity.

We began developing these resources because advising clients on the Internet as a business engine also requires education on the dangers of cybercrime.

Under the 2017 NDAA, SBDCs are now working with Homeland Security and SBA to leverage our resources and provide enhanced training and assistance. We want to develop cost-effective, high-quality tools for small business and a network to share information and threat analysis with those small businesses.

I want to thank the members of this Committee for working on that language and getting it into the NDAA. The timing could not be more critical.

While SBDCs are training small business on the first line of their cybersecurity needs, the internal focus of basic security practices, threats and weaknesses, ways to help them protect their customers and themselves, we are looking at a bigger effort, and that is the external demands of cybersecurity.

On the commercial side, large businesses are going to place growing demands on their small business suppliers. What certifications are they going to ask for? What kind of systems? And who is going to supply those certifications? And more important, who is setting the standards?

Last year, the FCC stepped in and declared ISPs to be common carriers. Now they have pulled back in favor of harmonization, but small businesses are left wondering who is actually making rules? And while Verizon and Comcast are battling Google and Facebook over this, what regulations will end up being placed on small business?

We know small businesses can be a back door. Does that mean the rules will be set by the biggest firms at the expense of the small firms?

Google already declared certain websites to be unsafe if they do not have what Google considers adequate security. Now, http versus https is serious, but how many small businesses know this? And how much business will they lose because eBay was not http-

compliant and Google users could not find them, or would not go to them.

And then there is the government side. The previous administration was proud of meeting small business goals. Will that last? They also put out a lot of cybersecurity regulations. The DOD and the FAR Council issued cybersecurity amendments to their acquisition regulations, and Homeland Security recently released three more proposed regulations for their acquisition regs. How are all of these regulations going to operate, and how will the agencies harmonize them with FSMA and the FTC? And will the standards be set at the convenience of the largest contractors? And what about the subcontractors? If you have a cybersecurity protocol for large prime contractors that flows down, it can easily freeze out small subcontractors.

That is why SBDCs are glad we are working with DHS and SBA now, because we want to head off this confusion. A lot of our members work with PTACs and do a lot of procurement assistance with small businesses, as well as regular business assistance, and we want to ensure that opportunity is not sacrificed for cybersecurity.

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

Chairman CHABOT. Thank you very much.

Mr. Mooney, you are recognized for 5 minutes.

#### **STATEMENT OF JIM MOONEY**

Mr. MOONEY. Chairman Chabot, Ranking Member Velázquez, members of the Committee, thank you for inviting me here for this meeting today on behalf of NAFCU.

As you know, cyber and data crime have reached epic proportions in nearly all sectors of the economy. As the ranking member mentioned in her opening statement, 65 percent of all targeted attacks last year were struck at small- and medium-sized companies.

Now, credit unions and other financial institutions are required to protect data consistent with provisions of the Gramm-Leach-Bliley Act. Unfortunately, for other entities that handle sensitive, personal, and financial data, there is no comprehensive regulatory structure comparable or similar to GLBA. It is with this in mind that NAFCU supports comprehensive data and cybersecurity measures to create a national standard to protect consumers' personal information.

From the perspective of the financial services industry, cybersecurity and data security are inherently linked. Securing consumers' personal information and financial accounts requires the entire payments ecosystem to take an active role in addressing emerging threats.

Since 1999, GLBA and its regulations have proven to be effective in limiting data breaches and protecting valuable information among financial institutions. Regulators have developed robust guidance to help institutions create information security programs and enterprise risk management policies to address data and cybersecurity needs.

In addition, they oversee financial institution cybersecurity through periodic examinations designed to assess the risk associated with IT environments of various sizes and complexity.

The Federal Financial Institutions Examination Council has adopted the guidance of our friends from NIST in creating a cybersecurity assessment tool, or CAT. The CAT is a voluntary tool that credit unions and banks can use to gauge their cybersecurity readiness in advance of regulatory examinations.

Credit unions and banks have also benefitted from the availability of government initiatives aimed at coordinating information sharing, identifying emerging threats, and providing greater cybersecurity expertise.

A recent NAFCU survey found that credit unions use a range of government resources to maintain an awareness of emerging data security threats and to develop stronger cybersecurity standards. NAFCU has also engaged Treasury's Office of Critical Infrastructure Protection to suggest areas of improvement and future opportunities for public-private collaboration.

Information sharing is a key weapon in credit unions' arsenal against cybercrime. To that end, NAFCU has recently collaborated with the industry-led Financial Services Information Sharing and Analysis Center to promote awareness of a new information sharing initiative specific to credit unions.

Now, financial institutions are not the only targets of cyberattacks. Cybercriminals are realizing that merchants and retailers are often the weak link in the payment system. Retailers are an attractive target because they are not currently subject to any Federal laws on data security or breach notification.

Data breaches at retailers can have a significant cost to financial institutions. From 2013 to 2016, data breaches have cost my credit union an estimated \$833,000 just in member notification and card-reissue expenses. This does not even account for the actual fraud losses. These costs are almost double what Chevron Federal Credit Union pays annually for information security systems and services.

Unfortunately, credit unions are rarely reimbursed for the costs associated with the majority of data breaches. As member-owned, not-for-profit cooperatives, it is our members who ultimately bear the burden. These concerns have led NAFCU to urge Congress to create a national standard for data security. I outlined the key principles of this in my written testimony.

In conclusion, cyber and data security are the responsibility of every participant in the payments chain. Credit unions and their 106 million members across the country are looking to Congress to advance meaningful and robust data security legislation. It is time to level the playing field and create a national data and cybersecurity standard for everyone in the payments ecosystem.

Thank you for the opportunity to appear before this Committee, and I welcome your questions.

**Chairman CHABOT.** Thank you very much. And we thank all the witnesses for their testimony this morning. And I will begin the 5-minute questioning by each of us. I recognize myself.

I will begin with you, Ms. Ohlhausen. You thoroughly outlined the differences and the different resources that the FTC offers to small businesses, from guides on best practices to blog posts encouraging businesses to use email authentication and how to identify ransomware. And this is precisely the kind of information that small businesses need. No question about that.

However, I have concern that we are just not reaching small business owners quickly enough or comprehensively enough; that there are a lot of them out there that just do not know about these offerings that are there for them. Do you have metrics on how many small businesses you are impacting? And what efforts are being made at the FTC to disseminate information more broadly? And finally, do you have any suggestions on how the Federal Government as a whole can provide a broader audience with cybersecurity resources?

Ms. OHLHAUSEN. Thank you for your question, Chairman.

First, starting with metrics, we do try to keep track of how frequently people access our materials, our guides, our videos, websites, things like that, and just one small measure is we actually have disseminated field orders for 500,000 printed copies of some of our business education. It is available on our website. We do try to reach out to let people, small business know about it, and we work with our Federal partners. We are always happy also to work with members of Congress if you would like to put this on your website or brand it on a website. We also work with other organizations, community organizations, and we are happy to go out and do events around the country to bring this to small business. I have actually personally participated in several of those.

Chairman CHABOT. Thank you very much.

Dr. Romine, in your testimony you mentioned this partnership with the Small Business Administration and the FBI, as well as your cooperation with the SBDCs. Have these partnerships been effective in reaching small businesses? And if so, do you think they could serve as models for future interagency collaborations to assist small businesses developing cybersecurity systems?

Dr. ROMINE. I would say, Mr. Chairman, yes, they have been highly effective. The extent of penetration we do not have statistics for, but I think small businesses have definitely benefitted from the partnership and from our campaign in partnership with both the InfraGard program with the FBI and also the SBA. I think it has been highly effective.

Chairman CHABOT. Thank you.

Mr. Rowe, do you think it would be beneficial to have a single entity to coordinate cybersecurity resources across Federal agencies, and if so, what would be the architecture of such? And today, are there any existing agencies or government entities that would be positioned to take on such a role?

Mr. ROWE. Well, I am almost kind of loath to suggest creating more government, but I do think, at least on the procurement side, the FAR Council is there for a reason. And the FAR Council should be, frankly, focusing better on making sure that everyone in the Federal procurement arena is informed and has adequate resources. Now, that is just a specialized area.

On the commercial side of it, I think we have got a lot of resources here, and as you said, I think the biggest problem we have is they are not coordinated. I mean, we have 1,000 centers and we are working like crazy to try and keep people informed and give them the best possible resources. The biggest problem you have is the average small business owner is, well, we like to call it trapped in the whirlwind. They have got 5,000 things to worry about and

sometimes this is not the wolf closest to the sled. I believe we need to coordinate much the same way we have an interagency trade promotion coordinating committee. There should be a cybersecurity coordinating committee between the agencies.

Chairman CHABOT. Okay. Thank you very much.

Mr. Mooney, with the remaining time, I would like to move to you. I know that there have been these distributed denial of service attacks going on and ransom, et cetera, and it has been hitting the big folks, but it has been hitting small business folks as well. It seems like a 21st century bank heist where the robber basically says give me your money or I will shut down your website, in essence. Could you comment on that? What is being done about that? How can people protect themselves from that type of thing when they literally grab a hold of everything and want ransom in order to give you back your computer system?

Mr. MOONEY. Mr. Chairman—

Chairman CHABOT. If you could turn on the mic. Sorry.

Mr. MOONEY. Mr. Chairman, the key is to have a security system that is multifaceted and multilayered. And in our case, we have built in for as many of those kinds of contingencies and attacks as we may face, as well as we can predict. And so what we find again is that there is no one answer to any security problem. You have to attack it in multiple ways, and that is what we tend to do.

Chairman CHABOT. Thank you very much. My time is expired. The ranking member is recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

You have testified about ways the FTC has provided resources to consumers and businesses to improve data security. You mentioned today that you hope to centralize information for small businesses. The number one consumer request for 13 years running has been an annual report on ID theft and data security. So has the FTC considered such a report that includes information on the latest threats and how we can mitigate those efforts?

Ms. OHLHAUSEN. Thank you for your question. The FTC does collect information about what the biggest consumer threats are. We have a system called Consumer Sentinel. ID theft, you are absolutely right, has been very much a top concern. We have tried to counter that on several fronts. One is giving advice to businesses about how they can secure their data. Another is we have an identifytheft.gov tool on our website that helps victims of identity theft create a personalized plan to get their good credit and name back. I think that in addition to those things, we also bring, you know, enforcement actions where necessary if a company has not taken appropriate steps.

Ms. VELAZQUEZ. And why is it that difficult for the FTC to produce a report geared to small businesses that provides a comprehensive view of all the threats and how they can mitigate them?

Ms. OHLHAUSEN. Well, we could certainly consider doing a report. We do have our *Start with Security* brochure that gives a step-by-step approach for small business on how to take steps to protect data, and then if there is a breach, how they can remedy that breach. And if a report that is tied to current threats would

be of additional interest to businesses, we can certainly consider that.

Ms. VELAZQUEZ. Thank you.

Mr. Mooney, despite the widespread nature of cybercrime, there remains a great deal of confusion in the legal system as to when individuals and businesses should bear losses and when financial institutions should be held responsible. Do you think that legislation is required to address this issue on a national basis?

Mr. MOONEY. I believe it can. And the reason I say that is, as you noted, it is very ambiguous right now. And what I think really would clarify matters tremendously is if we had a national standard related to security practices, one that goes beyond what we have today. Today, Gramm-Leach-Bliley, as I mentioned before, provides that kind of clarity for banks, credit unions, and other financial institutions. Outside of that, there is really no clarity at all. And what we recommend is that there be a national standard along the lines of GLBA that provides the kind of flexibility, scalability, and risk-based assessments that will add to the clarity and allow everybody to step up to the plate in the payment system.

Ms. VELAZQUEZ. Okay. Thank you.

Tee, would you like to comment on that?

Mr. ROWE. Well—

Ms. VELAZQUEZ. I know that you do not like legislation.

Mr. ROWE. Well, I cannot say that. I made my living off of legislation. But I think you raised a good point. We have so many small business clients who are surprised to find out that when their account got drained there is no recourse. They are not like a consumer who is—I think it is Regulation E that protects them. They are under the Uniform Commercial Code. So basically, it defaults to that reasonableness standard. And the whole problem with the reasonableness standard is what is reasonable is shifting all the time. And it is hard to tell if you are a small business where the bar has moved to.

Ms. VELAZQUEZ. Okay. I know that it has not been long since we passed the NDAA, it was signed into law, but in terms of the SBDCs, working on implementing and disseminating cyber strategy, what type of progress has there been so far?

Mr. ROWE. Well, we always run into the problem in the transition, but, you know, we have been talking with SBA. Jack Bienko at SBA has been very helpful, and Holly Jackson from Homeland Security, who is in their cybersecurity and stakeholder engagement, which I never knew you had that in cybersecurity, which is great. So we are getting started. As I said, we have already organically begun our own efforts. The larger concern for us is going to be what you talked about, how do we develop—you talked about the report, but how do we develop basically a threat analysis and information network for small business? An annual report, well, that tells you what happened over the last year. It does not tell you what is going on now.

Ms. VELAZQUEZ. Thank you.

Chairman CHABOT. The gentlelady's time is expired.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Chairman CHABOT. Thank you.

The gentleman from Missouri, Mr. Luetkemeyer, who is the vice chairman of this Committee, is recognized for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Mr. Rowe, in your testimony, or in your written testimony I should say, you have some statistics there that are mindboggling. Cybercrime costs the global economy \$445 billion every year with the damage to business from theft of intellectual property exceeding \$160 billion loss to individuals. So you are looking at \$600 billion of loss total there. Fifty percent of the businesses as you say, I mean, small businesses, have been victims of cyberattacks, and over 60 percent of those will go out of business.

My question to you is did they go out of business or will they go out of business because of the liability exposure that they have there? Or did they go out of business because of the money that is stolen from them or because of the reputational problems that they have had to be able to stay in business? A combination of all those? Can you answer that?

Mr. ROWE. Sir, I would say it is a combination of all of those. I would say that the financial loss is generally the hardest hit for a small business. As you and the members of the Committee know, small business, they live off of cash flow. They live off of their capital. And a hard hit to that is something that is very difficult to overcome.

Mr. LUETKEMEYER. Now, with regard to the small businesses, though, do you see any of them being sued for the lack of adequate cyber protection?

Mr. ROWE. Well, that goes to what Ms. Ohlhausen was talking about. What is reasonable? If a small business has got decent cyber protection, is that a reasonable amount? I honestly do not know. The problem is that that bar keeps shifting as technology changes. We are working on things now that, frankly, block chain technology is going to change massively.

Mr. LUETKEMEYER. Ms. Ohlhausen, would you like to comment on that?

Ms. OHLHAUSEN. I think there are probably a variety of reasons that a company, a small business, may go out of business after a data security breach, including the financial implications that Mr. Rowe mentioned, as well as that small businesses are close to their customers. Right? If they lose customer trust, then I think that could also be a problem.

Mr. LUETKEMEYER. Okay. So my concern is we know we are being attacked. How do we protect the business' viability against that attack? Have you seen some businesses go out of business because they are being sued because of lack of data security protections?

Ms. OHLHAUSEN. I am aware that some businesses have—

Mr. LUETKEMEYER. Because I can tell you from the financial side, if I am a financial services regulator and I go into a financial services credit union, bank, whatever, and I see I have got a small business there that is highly leveraged and they deal with lots of personal data, there is an exposure there that I am very concerned about that if they have a data breach, is the viability of that business going to be affected? And so how does that small business pro-

tect themselves against that liability exposure? What kind of safe harbor can we put together?

Where I am going with the question is can we find a way to provide a safe harbor? Or is the safe harbor something like an insurance policy that is put in place to protect a small business which does not have the resources of a Target or a Home Depot when they have some data breaches? I mean, I had a large supermarket in my area that had its own debit card got breached and cost several hundred thousand dollars. It was dispersed, but it was significant. So how do we come up with a safe harbor for these small businesses? Is it an insurance policy that you go down this road to be able to help them or are they just exposed?

Mr. ROWE. Honestly, you are right. They are just exposed right now. There is a fledging industry on cybersecurity insurance, but, frankly, even if you are insured, I wonder how the actuarial effort would work. You can go now and you can get your car insured, if you have LoJack sometimes you will get a rebate on your insurance. Sometimes you will not.

Mr. LUETKEMEYER. Well, my concern is if we have got some exposure, how do we protect the small businesses against that? And while Dr. Romine was very specific about some of the guidelines and principles that he is recommending here, that is fine. But if it does not provide the safe harbor, and if I am looking at the viability of the business, to me an insurance company is a whole lot more nimble and flexible to be able to come out and tell the small business we found a new way, especially with the Fintech industry today continuing to evolve and continuing to have all sorts of—I do not want to say the word “exotic,” but there are certainly interesting products out there that help integrate all these different businesses and the payment systems. To me, you only have to figure out a way to have some sort of—I think the private sector is a better way to go about this, provide that kind of coverage and safe harbor.

Mr. ROWE. Well, I would agree with you because I think in general the private sector is much more nimble. Rather than insurance, I would think about it from the financial sector point of view. There is a lot of money invested, whether it is through lenders like credit unions or 7(a) lenders or you name it, Fintech, who all have a stake because if the small business gets hacked and goes under, they are not going to get repaid. So they have a stake in trying to build that up.

Mr. LUETKEMEYER. Thank you.

Chairman CHABOT. The gentleman's time is expired.

It is my understanding that the gentleman from Missouri wants to make a unanimous—

Mr. LUETKEMEYER. Yes, ICBA has a letter to the Committee and I would like to put it into the record.

Chairman CHABOT. Without objection, so ordered.

Mr. LUETKEMEYER. Thank you.

Chairman CHABOT. And the gentleman from Illinois, Mr. Schneider, who is the ranking member of the Subcommittee on Agriculture, Energy, and Trade, is recognized for 5 minutes.

Mr. SCHNEIDER. Thank you, Chairman. And again, thank you to the witnesses for making time to not just be here, but to pre-

pare. I know how much work goes into this, so thank you for sharing your expertise and insight.

The issue of cybersecurity, the issue of dealing with these challenges for small businesses are complex, confusing, and constantly changing. That is one of the problems we face and the risks keep growing.

Mr. Mooney, you talked about the idea of trying to establish a national standard. I would imagine one of the challenges we face in doing that, that once we get consensus, it is going to be out of date. So opening this up to the whole panel, how in partnership, private sector-government, might we best work to address the dynamism, if you will, of the threat?

Mr. MOONEY. Well, if I might take the first shot at that question, Congressman, I think the experience that we have had in the financial services industry suggests that there is a way to not be locked into any particular perspective or way of doing things. The way that Gramm-Leach-Bliley works is it provides a great deal of flexibility. It is risk-based. It is scalable so that it addresses the concerns as they exist at the time. And in suggesting that we would want to have some sort of national application of that, we would recommend that it has and follows those same principles.

Mr. SCHNEIDER. Mr. Rowe?

Mr. ROWE. Well, you are absolutely right. The shifting nature of the problem is sort of what militates against a national standard unless that standard is based on responsibility. And it then becomes a question of who is going to be responsible? I would say in so many areas, whether it is a small medical practice that is dealing with HIPAA information or a small business that may have a fair amount of financial information—a small insurance agency or an investment advisor—you have got to begin to follow the money.

And you have also got to place responsibility on the merchant services corporations who you are dealing with. Amazon and eBay make a fair amount of money supporting small businesses who are selling. It might be an interesting idea to say they bear some responsibility in helping to educate the people who work with them.

Mr. SCHNEIDER. You talk about a small insurance agency. I had the privilege of running a small insurance agency. There were two producers and we had a staff of eight. None of the 10 of us were the technology expert. Now, this was in 1997 to 2003, an entirely different environment than what we are facing today. And as I think through this problem, I know the time we spent on technology, on handling a lot of classified personal information and making sure that it was always safe and always protected. That just keeps getting increasingly hard. Are there ways, whether it is the work you do, things that we can do to help small businesses continue to stay ahead of the curve?

Mr. ROWE. And that is the whole key to what we are trying to accomplish here is build the resources and get the resources out so that small businesses can stay ahead of the game.

Mr. SCHNEIDER. Yeah, and I will add, as you talked about in your testimony, large corporations have resources and the people to do this. It falls oftentimes to the smaller companies, especially, for example, the ones trying to do business through Amazon and eBay and other opportunities that are there.

I appreciate that. I am nearly out of time. I will yield back the balance of my time to keep us on schedule.

Chairman CHABOT. Thank you very much. The gentleman yields back.

The gentleman from Kansas, Mr. Marshall, is recognized for 5 minutes.

Mr. MARSHALL. Thank you, Mr. Chairman.

My first question is for Dr. Romine. You may know I am a physician and help run a hospital as well, and health care seems to be particularly vulnerable to cyberattacks. Does NIST have any ideas on how to ensure the safety of healthcare data from cyberattacks? Are there any best practices? And especially I am thinking of smaller community hospitals, that type of thing.

Dr. ROMINE. Thank you for your question. We have projects going on through our National Cybersecurity Center of Excellence having to do with specifically that. We have a program in protection of health care and healthcare information. We also have, as part of that program, the protection of medical devices. So, for example, we have a program on trying to secure wireless infusion pumps in hospitals and trying to understand the threat that they present to the patient, as well as to the enterprise of the hospital, as an entry point for getting into other parts of the system.

With regard to the relation to small business, one of the things that we are looking at now and have completed recently for publication is trying to understand how to secure patient information or protected information when a physician is using a mobile device, to access that patient information. Anecdotally we hear, for example, the physician really just wants to do the best for the patient. Some of the rules regarding the transfer of that patient information can get in the way of providing that, and so we are trying to find ways that we can secure that communications mechanism to make it both more efficient for patient care, as well as more secure.

Mr. MARSHALL. As a physician, I am more concerned about patient confidentiality today than I was 10 years ago. The worst thing I had 10 years ago was someone could come in and steal a chart, but now if they crack the code they have access to thousands of charts. So it is almost like this has backfired on us.

I am into solutions. One of the biggest concerns I hear from the banking institutes, credit associations, is when they have a breach, there are significant fines. Small businesses, I am thinking of convenience stores where they are just doing thousands of transactions a day with a credit card, if they have a data breach, it still falls back on the banking institute. And I am looking for solutions. How can we help both sides here? What is the solution that anyone would have to that problem so it does not always fall just on the banking institutes or the credit cards?

Mr. MOONEY. May I take that?

Mr. MARSHALL. Please. Yeah.

Mr. MOONEY. Well, Congressman, I think our approach here and the suggestions that we are making regarding some sort of consistent level of standards for all players in the payment system we think is vital to accomplishing what you were just talking about. Under Gramm-Leach-Bliley, we are really given the duty to make data security our responsibility and our focus. And what we

think is for the payment system to be viable, everybody has to be playing at the same level. Now, again, we talk about small businesses and big businesses. As GLBA has functioned, it is scalable. So the risks that a large multinational financial institution has is going to be much greater than a small credit union, and the risk assessments accordingly are much different and the responsibilities are much different, but everybody is on the same page in terms of the responsibilities of protecting consumer, financial, and personal data.

Mr. MARSHALL. Okay. Anybody else have a comment?

Ms. OHLHAUSEN. The Federal Trade Commission has in previous Congresses supported on a bipartisan basis Federal data security and breach notification legislation that would give a clearer standard, a process-based standard, to businesses and also have a Federal requirement that if there is a breach, under certain conditions they have to notify consumers about it. So they can also take steps to protect themselves.

Mr. MARSHALL. Okay.

Mr. MOONEY. And if I may, just to add to that, and that is the environment that financial institutions operate under today. And so you are suggesting just broadening, which is what we think makes a lot of sense.

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

Chairman CHABOT. Thank you very much. The gentleman yields back.

The gentlelady from Florida, Ms. Murphy, is recognized for 5 minutes. And she is the ranking member of the Subcommittee on Contracting and Work Force.

Ms. MURPHY. Thank you to our witnesses for testifying today.

As was just mentioned, I serve as the ranking member on Contracting and Workforce. And you have discussed at length today in your testimony the great number of challenges that small businesses face in complying or dealing with cybersecurity. But I am specifically interested in honing in on the challenges that face small businesses in the contracting community and how these issues will affect the ability of small firms to compete for and win Federal contracts.

As you may know, it is becoming an increasingly common prerequisite for small businesses to be able to meet regulations that demonstrate their ability to maintain safe and secure networks before they can even participate in the competitive contracting process. My concern is that over time this may lead to more small firms losing bids or it may even discourage them from engaging in the bidding process at all because they simply cannot compete with larger companies that, unlike them, have the resources to hire and retain dedicated cybersecurity and IT personnel.

So Mr. Rowe, in your experience, how has the sheer complexity of these regulations so far affected the small business contractors that you have worked with? And what do you advise them as they face uncertain regulations and prohibitive compliance costs?

Mr. ROWE. Well, the hardest thing any of them have facing them is just knowledge of the Federal Register. I would be willing to bet half of them have no idea that the Department of Homeland Security just put out a proposed regulation on, what do they call

it, confidential unclassified information. Now, I am not even sure what that is. But in all of these situations—and these are all operating from the best of intentions, all of these agencies. They are trying to protect sensitive information on everything from weapon systems to medical equipment. But there is that tendency to go with the sledgehammer to kill a gnat.

And small businesses are left behind in all of these regulatory efforts because they have got to know what the Federal Register is, comment in the Federal Register, have that comment taken seriously, while, frankly, Lockheed and Boeing and SAIC have guys like me that they pay lots of money to do that for them.

To date, it has not really become horrible. My concern is if you have got a defense acquisition regulation system, a Federal acquisition regulation system, a Department of Homeland acquisition regulation system, all of which have cybersecurity regulations which may not all be exactly the same, and then you are requiring security protocols for a small business that may be working three or four agencies and trying to get their security to match up with the security systems in four different computer systems, we all know that at a certain point it just does not work. And that is the biggest concern that we have is getting enough flexibility so that the small business can protect the data without having to do all their work in triplicate.

Ms. MURPHY. Do you have any suggestions on how that regulatory process can be streamlined or rationalized in a way that would avoid the scenario that you just laid out?

Mr. ROWE. Yes. Again, it goes back to what I said to the chairman. I think there needs to be an interagency coordinating committee on cybersecurity so that when the FAR Council, which is really just DOD, GSA, and the Office of Management and Budget, make a decision, there has been input from all the other agencies and from small business.

Ms. MURPHY. Great. Thank you. And I will yield back the remainder of my time.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

The gentleman from Pennsylvania, Mr. Fitzpatrick, is recognized for 5 minutes.

Mr. FITZPATRICK. Thank you, Mr. Chairman. Thanks to everyone on the panel for your time today.

I want to ask specifically about law enforcement corroboration and collaboration. Department of Homeland Security, Department of Justice, particularly the FBI, are the two main law enforcement organizations responsible for investigating cyber-related crimes and national security-related cyberattacks. Dr. Romine mentioned the InfraGard program. That is one of several programs that exist.

My question, not only from the small business standpoint, but also I am on the Cyber Subcommittee of Homeland Security, what is the collaboration currently? How has it been going in both directions?

Because not only is it important that law enforcement receive this information to track digital fingerprints and patterns of cyberattacks; it is equally important for the small business community that there be a good relationship that the Bureau and Depart-

ment of Homeland Security can share tips on the private side on how to best protect small businesses from cyberattacks. So if any one of you could just comment on what the status of relationships is with those two Federal agencies, what works and what has not worked.

Dr. ROMINE. Thank you for the question.

I am happy to reiterate the importance that we accord to the partnership with FBI's InfraGard program and the SBA as a mechanism for outreach to provide the kind of information that you just discussed, to the private sector broadly, but particularly to small- and medium-sized businesses. I think that has been very effective and it is a strong relationship.

Mr. FITZPATRICK. Department of Homeland Security. Has there been any relationship or outreach with them?

Dr. ROMINE. We have ongoing relationships with the Department of Homeland Security. They were vigorous participants during the development of the cybersecurity framework, for example. They spent a lot of time generating a voluntary program that they used in concert with, and using the cybersecurity framework as it emerged, to provide that kind of outreach. We had a lot of strong input from them and provided them a lot of useful information that they could then use in their voluntary program for people to adopt the framework or to get assistance in using the framework.

We have partnerships with the FBI in other areas such as biometrics technologies, for example. That is a slightly different topic, but with the understanding of trying to improve the accuracy of biometrics. That partnership goes back to 1963 with the FBI, so we consider that a pretty strong relationship.

Mr. FITZPATRICK. Has there been any frustrations that you have heard from the small business community with regard to law enforcement not taking certain cases because they do not fall within the threshold that would allow for an investigative activity?

Dr. ROMINE. NIST would not hear something like that.

Mr. FITZPATRICK. Okay.

Dr. ROMINE. I think that is not the kind of information that they would share with us. We do ensure that we have outreach to small businesses so that we can ensure that our work products, our cybersecurity guidance is scalable and digestible at all levels. We are working much harder on that to ensure that it is useful across the spectrum, all the way from small to very large enterprises.

Mr. FITZPATRICK. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentleman from Pennsylvania yields back.

That concludes our questions to the panel. We want to thank the very distinguished panel for their testimony here today. It has been very helpful. I think once things clear, and that is the people up here, the members on both sides of the aisle want to do everything we possibly can to ensure that small businesses have the best possible cybersecurity resources available to them.

And along those lines, we, being the Committee, are going to be putting this up online today. These are easy-to-understand security packets that will be available to small businesses. They are kind of step-by-step guides on how to protect themselves, small business

folks, from cyberattacks. And these will be up on the Small Business Committee's website today. So I just wanted to mention that.

And I would remind folks that members would have 5 legislative days to submit statements and supporting materials for the record.

And if there is no further business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:11 p.m., the Committee was adjourned.]

**A P P E N D I X**

**PREPARED STATEMENT OF**

**THE FEDERAL TRADE COMMISSION**

**on**

**Small Business Cybersecurity: Federal Resources and Coordination**

**Before the**

**COMMITTEE ON SMALL BUSINESS**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**Washington, D.C.**

**March 8, 2017**

## I. Introduction

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, I am Maureen Ohlhausen, Acting Chairman of the Federal Trade Commission (“FTC” or “Commission”).<sup>1</sup> I appreciate the opportunity to present the Commission’s testimony on data security and, in particular, its efforts to educate small businesses.

Reports of data breaches affecting millions of American consumers have become commonplace.<sup>2</sup> Data is an increasingly vital asset for every business, including small businesses, and as companies collect more personal information from consumers, the databases they create become more attractive targets for criminals. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers’ sensitive information, and potentially misuse it in ways that can cause serious harms to consumers and businesses.

Failing to take reasonable precautions to secure data from identity thieves and other malicious actors hurts consumers and legitimate businesses alike. Consumers face the risk of fraud, identity theft, and other harm.<sup>3</sup> In addition, data breaches can harm a business’s financial interests and reputation as well as result in the loss of consumer confidence in the businesses to whom they entrust their data. In the case of small businesses, a data breach can be devastating.

---

<sup>1</sup> This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

<sup>2</sup> See, e.g., Vinod Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. Times, Dec. 14, 2016, available at [https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?\\_r=0](https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0); Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times, Oct. 21, 2016, available at <https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html> (describing the Dyn DDoS attack that relied on hundreds of thousands of IoT devices); Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, N.Y. Times, Jan. 25, 2014, available at <http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html> (discussing Michaels Stores’ announcement of potential security breach involving payment card information).

<sup>3</sup> See Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 2015), available at <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (estimates that 17.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2014).

Although such incidents rarely make the headlines, the majority of attacks target small and mid-sized businesses, and, according to the National Cyber Security Alliance, some 60% of small businesses go out of business within six months of a breach.<sup>4</sup>

The Federal Trade Commission is a small, independent agency with a large role to play when it comes to data security. The Commission, a bipartisan body, has operated effectively for more than 100 years, with a unique dual mandate to protect consumers and maintain competition in broad sectors of the economy. As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector using the flexible tools Congress gave us. The Commission has undertaken substantial efforts throughout the 21<sup>st</sup> century to promote data security in the private sector through civil law enforcement, business outreach and consumer education, policy initiatives, and recommendations to Congress to enact legislation in this area. This testimony provides an overview of those efforts.

## II. THE COMMISSION'S DATA SECURITY PROGRAM

### A. Law Enforcement

The Commission enforces several statutes and rules that impose data security requirements on companies. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, sets forth data security requirements for

---

<sup>4</sup> See Gary Miller, *60% of Small Companies That Suffer a Cyber Attack Are Out of Business Within Six Months*, The Denver Post, Oct. 23, 2016, available at <http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>; Oscar Marquez, *The Costs and Risks of a Security Breach for Small Businesses*, Security Magazine, July 26, 2016, available at <http://www.securitymagazine.com/articles/87288-the-costs-and-risks-of-a-security-breach-for-small-businesses>; Robert Strohmeyer , *Hackers Put a Bull's-Eye on Small Business*, PCWorld, Aug. 12, 2013, available at <http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html>.

financial institutions within the Commission’s jurisdiction.<sup>5</sup> The Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,<sup>6</sup> and it imposes safe disposal obligations on entities that maintain consumer report information.<sup>7</sup> The Children’s Online Privacy Protection Act (“COPPA”) requires reasonable security for children’s information collected online.<sup>8</sup> In addition, the Commission enforces the FTC Act, which prohibits unfair or deceptive acts or practices, such as businesses making false or misleading claims about their data security procedures, or failing to employ reasonable security measures and, as a result, causing or likely causing substantial consumer injury.<sup>9</sup>

Since 2001, the Commission has used its authority under these laws to take enforcement action and obtain settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers’ personal information.<sup>10</sup> In each of these cases, the practices at issue were not merely isolated mistakes. Instead, the Commission examined the company’s practices as a whole and challenged alleged data security failures that were multiple and systemic. And through these actions and orders, the Commission has made clear that it does not require perfect security; that reasonable security is a continuous

---

<sup>5</sup> 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

<sup>6</sup> 15 U.S.C. § 1681e.

<sup>7</sup> *Id.* at § 1681w. The FTC’s implementing rule is at 16 C.F.R. Part 682.

<sup>8</sup> 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 (“COPPA Rule”).

<sup>9</sup> 15 U.S.C. § 45(a). If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5. Further, if a company’s data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.

<sup>10</sup> *See generally* [http://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field\\_consumer\\_protection\\_topics\\_tid=249](http://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249).

process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.

An example of this approach can be found in the FTC's recent settlement with AshleyMadison.com. In that case, the FTC alleged that the companies responsible for the site failed to protect 36 million users' personal information in relation to a massive data breach of their network – one of the largest data breaches that the FTC has investigated to date.<sup>11</sup> According to the FTC, although the defendants assured users their sensitive information was private and securely protected, the security of AshleyMadison.com was lax. According to the complaint, the defendants had no written information security policy, no reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security. Intruders accessed the companies' networks several times between November 2014 and June 2015, but due to their lax data-security practices, the defendants allegedly did not discover the intrusions. Following a major data breach in July 2015, the hackers published sensitive information for more than 36 million AshleyMadison.com users. According to the complaint, this included information that the defendants had retained on users who had paid for an account deletion option that purportedly removed users' data from the site.

The FTC also brought a data security enforcement action last year against computer hardware maker ASUSTeK Computer, Inc. According to the complaint, ASUS marketed its routers as including numerous security features that the company claimed could "protect computers from any unauthorized access, hacking, and virus attacks" and "protect [the] local

---

<sup>11</sup> *FTC v. Ruby Corp. et al.*, No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), available at <https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison>.

network against attacks from hackers.”<sup>12</sup> Despite these claims, the FTC’s complaint alleged that ASUS failed to take reasonable steps to secure the software on its routers. The Commission charged that critical security flaws in ASUS’ routers put the home networks of hundreds of thousands of consumers at risk. The FTC also alleged that the routers’ insecure “cloud” services led to the compromise of thousands of consumers’ connected storage devices, exposing their sensitive personal data on the internet.

The Ashley Madison and ASUS settlements, along with the FTC’s other data security settlements, are available on the FTC website, and descriptions of the proposed complaints and consent orders are published in the Federal Register before each settlement is made final. The settlements provide companies with insight into the practices that the FTC has alleged to be unreasonable.<sup>13</sup> By learning about alleged lapses that led to law enforcement action, companies can improve their practices to avoid fundamental security missteps.

Commission complaints are not the only enforcement-related source of information that may assist businesses. The FTC closes far more data security cases than it pursues to settlement or litigation. Staff is currently working to provide the public with more information about these closed matters, which will help further illustrate, through additional examples, how the Commission has consistently applied the principles contained in its longstanding existing public guidance materials, discussed below.

#### **B. Business Guidance and Consumer Education**

In addition to law enforcement, the FTC engages in extensive business and consumer education on data security. Our goal is to provide information to help businesses protect the data

---

<sup>12</sup> *ASUSTeK Computer Inc.*, No. C-4587 (July 28, 2016), available at <https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter>.

<sup>13</sup> See generally [www.ftc.gov/datasecurity](http://www.ftc.gov/datasecurity).

in their care and understand what practices may run afoul of the FTC Act. In fiscal year 2016, the FTC filled orders for more than 500,000 free printed publications for businesses on data security. We provide general business education about security issues, as well as specific guidance on emerging threats, such as ransomware, which is discussed below.

For general education, the FTC offers user-friendly guidance to help companies of all sizes improve their data security practices and comply with the FTC Act. For example, in November the FTC released an update to *Protecting Personal Information: A Guide for Business*.<sup>14</sup> The FTC first published this guide in 2007 and has updated it periodically ever since.

Last fall, the FTC released *Data Breach Response: A Guide for Business*, which outlines steps businesses should follow when they experience a data breach.<sup>15</sup> The Guide, and a related video, describe immediate steps companies should take, such as taking breached systems offline, securing physical areas to eliminate the risk of further harm from the breach, and notifying consumers. And the Guide includes a model data breach notification letter businesses can use to get started.

Also, in 2015, the FTC launched its *Start with Security* initiative, which includes a guide for businesses that summarizes the lessons learned from the FTC's data security cases,<sup>16</sup> as well as 11 short videos.<sup>17</sup> These materials discuss ten important security topics and give advice about

---

<sup>14</sup> *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

<sup>15</sup> *Data Breach Response: A Guide for Business* (Oct. 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>.

<sup>16</sup> *Start with Security: A Guide for Business* (June 2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

<sup>17</sup> *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), available at <https://www.ftc.gov/news-events/audio-video/business>.

specific security practices for each. As part of this initiative, the FTC hosted events in San Francisco, Austin, Seattle, and Chicago, bringing business owners and app developers together with industry experts to discuss practical tips and strategies for implementing effective data security.<sup>18</sup> Last year, FTC staff presented our *Start with Security* materials on six cybersecurity webinars sponsored by the National Institute of Standards and Technology (NIST) and the SBA; thousands of small business owners attended these webinars. We also issued a publication directed toward businesses to educate them on how the NIST Cybersecurity Framework applies to FTC best practice.<sup>19</sup>

In addition to general data security guidance, the FTC also provides businesses with specific guidance on emerging threats. For example, most recently the FTC released a staff perspective and related blog post to help businesses prevent phishing scams.<sup>20</sup> These materials encourage businesses to use email authentication – a technical solution that businesses can use to protect their reputations and prevent phishing emails from getting through to their customers.<sup>21</sup> The FTC has also educated businesses about threats like ransomware – malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data “hostage” until the victim pays a ransom. Following a workshop,<sup>22</sup> the FTC published a

<sup>18</sup> See, e.g., FTC Event, Start with Security – Seattle (Feb. 9, 2016), available at <https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle>.

<sup>19</sup> FTC Business Blog, *The NIST Cybersecurity Framework and the FTC*, Aug. 31, 2016, available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.

<sup>20</sup> FTC Staff Perspective, *Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication* (Mar. 2017), available at <https://www.ftc.gov/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff>; FTC Business Blog, *Want to stop phishers? Use email authentication*, Mar. 3, 2017, available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication>.

<sup>21</sup> Email authentication is a collection of techniques that allow ISPs and others to verify the domain of the sender of an email. These techniques include Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC).

<sup>22</sup> Fall Technology Series: *Ransomware* (Sept. 7, 2016), available at <https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware>.

blog post describing the nature of the ransomware threat, how to defend against ransomware, and essential steps to take if businesses become victims of ransomware.<sup>23</sup>

Further, the FTC develops guidance for companies in specific industries. For example, we developed *Careful Connections*, business guidance that includes a series of steps for companies to consider if they design and market Internet-connected products.<sup>24</sup> We have also developed specific security guidance for mobile app developers.<sup>25</sup>

In the coming months, the FTC plans to expand its outreach to small businesses around data security issues, with a focus on helping very small businesses identify risks and develop data security plans.

Very small businesses, including sole proprietors and companies with just a few employees, generally do not have full-time information technology or human resources staff. Some of the cybersecurity challenges they face are similar to those confronting consumers, such as securing their wireless networks or avoiding phishing scams. The FTC offers free resources and educational materials to help consumers protect themselves from the evolving threats they face while using technology. For example, the FTC has provided guidance for consumers on securing their home wireless networks, a critical security step for protecting devices and personal information from compromise.<sup>26</sup> These and other resources are accessible on the FTC's

---

<sup>23</sup> FTC Business Blog, *Ransomware – A Closer Look* (Nov. 10, 2016), available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look>.

<sup>24</sup> *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>.

<sup>25</sup> *Mobile App Developers: Start with Security* (Feb. 2013), available at <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security>.

<sup>26</sup> FTC Consumer Blog, *Securing Your Wireless Networks*, Sept. 2015, at <https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network>.

consumer guidance website, consumer.ftc.gov.<sup>27</sup>

Finally, the FTC launched an improved version of IdentityTheft.gov<sup>28</sup> (robodeidentidad.gov in Spanish<sup>29</sup>) last year. It's a free, one-stop resource consumers can use to report and recover from identity theft. As part of the site, identity theft victims obtain personalized recovery plans based on their specific experience with identity theft, and get customized letters and forms to send to credit bureaus, debt collectors, and other businesses.

More than 400,000 victims have used IdentityTheft.gov in the last year.

#### C. Policy Initiatives

Finally, the FTC pursues numerous policy initiatives to enhance data security. The FTC has hosted workshops and issued reports recommending best practices designed to improve data security and privacy and to highlight the privacy and security implications of new technologies and business practices. For example, last year the FTC hosted a three-part Fall Tech Series to examine new and evolving technologies that raise critical consumer protection issues, focusing on ransomware, drones, and smart TVs.<sup>30</sup>

The FTC works across the government, providing comments to other agencies as they engage in cybersecurity initiatives. For example, the FTC provided comments to NHTSA during the development of the Federal Automated Vehicle Policy.<sup>31</sup>

---

<sup>27</sup> See generally <https://www.consumer.ftc.gov/>.

<sup>28</sup> See <https://identitytheft.gov/>.

<sup>29</sup> See <https://robodeidentidad.gov/>.

<sup>30</sup> Press Release, *FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues* (Mar. 31, 2016), available at <https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues>.

<sup>31</sup> Comment of Jessica L. Rich, Director, Bureau of Consumer Protection, to the National Highway Traffic Safety Administration Supporting the Inclusion of Consumer Privacy and Cybersecurity Guidance in the Document "Federal Automated Vehicles Policy" (Nov. 2016), available at <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/11/comment-jessica-l-rich-director-bureau-consumer>.

In addition, in January, the FTC announced an Internet of Things (IoT) security challenge.<sup>32</sup> The Commission is offering a cash prize of up to \$25,000 for the best technical solution that helps consumers quickly identify security vulnerabilities in their IoT devices and pushes out updates to address those vulnerabilities. The FTC is particularly interested in tools that can prompt consumers to change default passwords to decrease the risk of their IoT devices being compromised. This important initiative will draw attention to IoT security problems and facilitate solutions that consumers and small businesses can use.

### **III. Legislation**

The Commission continues to reiterate its longstanding, bipartisan call for comprehensive data security legislation that would (1) strengthen its existing data security authority and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.<sup>33</sup> Reasonable security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data. For example, in the case of a breach of a database with Social Security numbers, notifying consumers will enable them to request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other

---

<sup>32</sup> Press Release, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), <https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security>.

<sup>33</sup> Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits and common carriers, and the authority to issue implementing rules under the notice and comment rulemaking procedures of the Administrative Procedure Act, 5 U.S.C. § 553. The Court of Appeals for the Ninth Circuit recently held that the FTC could not bring a case against AT&T because the common carrier exception in Section 5 of the FTC Act precluded FTC enforcement of the Act against any company with the status of a common carrier, even if the case involved non-common-carrier activities. See *FTC v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016). The Commission has asked the court to rehear the case en banc, and its petition remains pending.

steps to protect themselves. And although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected.

**IV. Conclusion**

Thank you for the opportunity to provide the Commission's views on data security. The FTC is committed to keeping data secure without imposing unnecessary or undue costs on businesses, including small businesses. We look forward to continuing to work with the Committee and Congress on this critical issue..

Testimony of

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

National Institute of Standards and Technology  
United States Department of Commerce

Before the  
United States House of Representatives  
Committee on Small Business

*“Small Business Cybersecurity: Federal Resources and Coordination”*

March 8, 2017

### **Introduction**

Chairman Chabot, Ranking Member Velázquez, members of the Committee, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). ITL cultivates trust in information technology and metrology through measurements, standards and testing. Thank you for the opportunity to appear before you today to discuss NIST's cybersecurity efforts as they relate to small businesses. Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology (IT), but the IT security challenge for small businesses looms larger than ever.

### **NIST Role in Cybersecurity**

With programs focused on national priorities from the Smart Grid and electronic health records to forensics, atomic clocks, advanced nanomaterials, computer chips, and more, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541<sup>1</sup>), and reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are often voluntarily adopted by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective and accepted globally. NIST disseminates these resources through a variety of means that encourage the broad sharing of information security standards, guidelines, and practices, including outreach to stakeholders, participation in government and industry events, and online mechanisms.

### **Small Business Role**

NIST recognizes that small businesses play an important role in the U.S. economy. These businesses produce approximately 46% of the Nation's private-sector output and create 63% of all new jobs in the country.<sup>2</sup> Since information technology is critical to the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber-environment cannot be overstated.

---

<sup>1</sup> FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

<sup>2</sup> Small Business Administration, [https://www.sba.gov/sites/default/files/FAQ\\_March\\_2014\\_0.pdf](https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf)

Since nearly 99% of all U.S. businesses are small or medium-sized,<sup>3</sup> a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house sensitive personal information including healthcare or financial information. Many small businesses also provide services to the federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which Americans currently operate, it is vital that small businesses are aware of and actively manage cyber risks.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. The risks to systems are so complex and pervasive that one cannot reasonably expect small businesses to be experts in all areas of security, including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology. Cybersecurity incidents can have a devastating effect on small businesses—60% of small companies will close within six months following a cyberattack.<sup>4</sup>

NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Ensuring that business-related information is secure is essential to the functioning of America's economy. NIST's broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, including small- and medium sized businesses.

#### **Cybersecurity Fundamentals**

In November 2016, NIST released a major revision to the popular report *Small Business Information Security: The Fundamentals* (NIST Interagency Report, NISTIR 7621R1). The report is designed for small business owners with little cybersecurity expertise and provides basic steps needed to help protect their information systems. NISTIR 7621R1 guides readers through a simple risk assessment to understand the organization's vulnerabilities. After identifying and determining the value of the organization's information, the users evaluate the risk to the business and customers if its confidentiality, integrity, or availability were compromised.

The guide describes how to:

- Limit employee access to only appropriate data and information,
- Train employees about information security,
- Create policy and procedures for information security,
- Encrypt data,
- Install web and email filters, and
- Patch or update operating systems and applications.

NISTIR 7621R1 is also aligned with NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), a set of voluntary standards, guidelines, and practices to promote the protection of our nation's critical infrastructure. NISTIR 7621R1 can be used as a step from cybersecurity fundamentals to more advanced cybersecurity risk management described in the Framework.

---

<sup>3</sup> Small Business Administration, [https://www.sba.gov/sites/default/files/Whats\\_New\\_With\\_Small\\_Business.pdf](https://www.sba.gov/sites/default/files/Whats_New_With_Small_Business.pdf).

<sup>4</sup> <https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic>

### **Cybersecurity Framework**

NIST released the initial version of the Framework three years ago, in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Framework, created through collaboration between industry and government, consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework's voluntary, risk-based, prioritized, flexible, repeatable, and cost-effective approach, developed for use by organizations – including small businesses – to help these organizations to manage cybersecurity-related risk. Key to the continuing success of the Framework is that it is not regulatory or mandatory in nature, but rather is voluntarily implemented by industry and voluntarily adopted by infrastructure sectors, contributing to reducing cyber-risks to the Nation's critical infrastructure. According to a June 2015 presentation by Khushbu Pratap and Earl Perkins of Gartner, Inc., by 2020, more than 50% of organizations will use the NIST Cybersecurity Framework, up from 30% in 2015.

Last month, NIST released a proposed update to the Framework incorporating feedback received since the release of Framework version 1.0, comments from a December 2015 Request for Information, and from a 2016 Cybersecurity Framework Workshop. Draft version 1.1 of the Framework, for which NIST is seeking public comments through April 10<sup>th</sup> of this year, provides new details on managing supply chain risks, clarifies key terms, and introduces measurement methods for cybersecurity.

NIST collaborates with the Department of Homeland Security's Critical Infrastructure Cyber Community (C<sup>3</sup>) Voluntary Program to promote Framework implementation among SMBs within the 16 sectors of critical infrastructure. NIST and DHS coordinate on a range of events promoting Framework implementation and understanding, such as webinars and workshops.

In addition to the Cybersecurity Framework, NIST has developed, over the past decade, an extensive set of security standards and guidelines, including a Risk Management Framework (RMF), that can be customized for small businesses and implemented on a voluntary basis to help protect a small business's intellectual property and organizational assets. The flexibility of the RMF is backed up by a set of comprehensive, state-of-the-practice security and privacy controls that can help small businesses be less susceptible to a range of cyber threats that can impact their competitiveness and survivability in a high risk, Internet-based operating environment.

### **Baldridge-Based Tool for Cybersecurity Excellence**

Building further on the success of the Cybersecurity Framework, NIST released the draft Baldridge Cybersecurity Excellence Builder, a self-assessment tool to help organizations of all sizes better understand the effectiveness of their cybersecurity risk management efforts. The Builder blends the best of two globally recognized and widely used NIST resources: the organizational performance evaluation strategies from the Baldridge Performance Excellence Program and the risk management mechanisms of the Cybersecurity Framework. Using the Builder, organizations of all sizes and types can:

- Determine cybersecurity-related activities that are important to business strategy and the delivery of critical services;
- Prioritize investments in managing cybersecurity risk;

- Assess the effectiveness and efficiency in using cybersecurity standards, guidelines, and practices;
- Assess their cybersecurity results; and
- Identify priorities for improvement.

Like the Cybersecurity Framework, the Baldridge Cybersecurity Excellence Builder is adaptable to meet an organization's specific needs, goals, capabilities, and environments.

#### **Interagency Collaborations**

Since 2001, NIST has partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems.

NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers, providing participants with information to increase awareness of NIST resources. In addition to its work with SBA and InfraGard, NIST is also working with the National Cyber Security Alliance (NCSA) to bring more online tools to small businesses on the NCSA's small business website<sup>5</sup>.

In 2016, as part of the Cybersecurity National Action Plan (CNAP), NIST partnered with the Small Business Administration, the Federal Trade Commission, and the Department of Energy to develop and provide cybersecurity training webinars for small businesses. These webinars were attended by hundreds of small businesses and attendees from 68 SBA District Offices, nine NIST Hollings Manufacturing Extension Partnership program (MEP) Centers, and other regional networks across the country.

#### **National Initiative for Cybersecurity Education**

A cybersecurity educated workforce in all organizations is critical to improving the Nation's cybersecurity capabilities. Cybersecurity is particularly challenging for small businesses because they often have few, if any, staff devoted to IT or cybersecurity, and these staff tend to be generalists – not specialists. Alternatively, businesses outsource IT or cybersecurity functions and rely on third-party service providers. Consequently, the workforce needs of small businesses are both nuanced and unique.

In 2008, the National Initiative for Cybersecurity Education (NICE), a public-private collaboration among government, academia, and industry, was established to enhance the overall cybersecurity capabilities of the United States. The NICE program seeks to energize and promote a robust ecosystem for cybersecurity education, training, and workforce development. As the lead agency for this initiative, NIST works with more than 20 federal departments and agencies, as well as with industry and academia, to ensure a digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

In November 2016, NIST released the draft NICE Cybersecurity Workforce Framework for public comment to help our Nation more effectively identify, recruit, develop, and maintain its cybersecurity talent. The framework provides a common language to categorize and describe

---

<sup>5</sup> <https://staysafeonline.org/business-safe-online/>

cybersecurity work that will help organizations build a strong labor staff to protect systems and data. The NICE Challenge Project, funded by NIST and developed and maintained by California State University, San Bernardino, creates virtual challenges to test students and professionals on their ability to perform NICE Framework tasks.

In 2016, CyberSeek, an interactive online tool designed to help close the cybersecurity skills gap, was released to the public. CyberSeek, developed by CompTIA and Burning Glass, with funding from NIST, provides detailed, actionable data about supply and demand in the cybersecurity job market. CyberSeek includes an interactive map that indicates relative concentrations of cybersecurity job postings and worker supply. The Career Pathway portal of CyberSeek provides information on different types of cybersecurity positions to help students, job seekers, and education and training providers. The Career Pathway portal features information on common job titles, salaries, in-demand skills, education, and certifications related to careers in cybersecurity, as well as pathways to reaching the mid- to advanced-level career positions.

NIST is also piloting the establishment of Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development in five communities across the United States. The RAMPS work to bring together K-12 schools, community colleges, universities, training providers, economic development organizations, local and state government, and employers, especially from small and medium-sized businesses in the community, to coordinate regional activities addressing the cybersecurity workforce shortage and expand their local economy.

#### **National Cybersecurity Center of Excellence**

The National Cybersecurity Center of Excellence (NCCoE) turns standards and best practices into practical solutions to address some of the Nation's thorniest cybersecurity challenges. The NCCoE collaborates with experts from industry, academia, and government to create and promote solutions to real-world cybersecurity problems using commercially available products in the form of technical practice guides that can be used by organizations including small and medium-sized businesses. For example, the NCCoE project on Mobile Device Security provides guidance to small and medium-sized businesses on the implementation of capabilities to secure sensitive business data residing in the cloud and being accessed by employees on mobile devices.

Health care providers increasingly are using mobile devices to collect, access, process, and transmit patient information. The NCCoE project Securing Electronic Health Records on Mobile Devices provides guidance for healthcare organizations of all sizes seeking to improve the security of these ubiquitous devices. This guide can be used by local and regional hospitals as healthcare providers leverage mobile devices to the workplace. These projects and all of the work at the NCCoE help strengthen the security of the Nation's businesses.

#### **Conclusion**

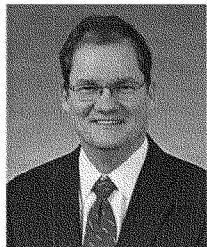
Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology, but the IT security challenge for small businesses looms larger than ever. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power.

Small businesses must take steps to secure systems against malicious activity, or accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST recognizes that it has an essential role to play in helping small businesses. The NIST programs described here demonstrate that NIST's cybersecurity portfolio is applicable to a wide variety of users, from small and medium-sized enterprises to large private and public organizations.

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

Thank you for the opportunity to present NIST's views regarding security challenges facing small enterprises. I will be pleased to answer any questions you may have.

**Charles H. Romine**

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of \$150 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

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

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

**Education:**

Ph.D. in Applied Mathematics from the University of Virginia.

B.A. in Mathematics from the University of Virginia.



Testimony  
of  
C. E. "Tee" Rowe  
President/CEO  
America's SBDC

March 8, 2017  
Committee on Small Business  
Hearing on  
Cybersecurity: Federal Resources and Coordination

Chairman Chabot, Ranking Member Velazquez, members of the committee. Thank you for inviting me to testify on behalf of America's SBDC, the Association of Small Business Development Centers.

SBDCs operate over 1,000 centers in all fifty states as well as the District of Columbia, Puerto Rico, the Virgin Islands, American Samoa and Guam. SBDCs provide management and technical assistance to over 200,000 small businesses every year and training to over 300,000 business owners and their employees. All of these small business owners have the same basic question, "How do I succeed?". That's not always a simple answer but, for almost every business that means maximizing sales, and we've been able to aid those clients to the tune of nearly 7 billion of new sales every year.

This is a great statistic, but it contains a not too hidden peril, cyber-crime. More and more of our clients do business online. Every single one of them is vulnerable, and they may not even know it. They may not even have a website but they are potential victims. Every time they run a credit card transaction, or answer their email they expose themselves and their customers to the risk of hacking, phishing and ransomware. And the dangers go beyond e-commerce. Any business, whether a vendor or a contractor, is at risk if they are connected and have personally identifiable information or the potential to be an access point to others who do.

By now I assume everyone is aware of the alarming statistics about cyber-crime. Cybercrime costs the global economy about \$445 billion every year, with the damage to business from theft of intellectual property exceeding the \$160 billion loss to individuals. Fifty percent of small businesses have been the victims of a cyber-attack and over 60 percent of those attacked will go out of business.

Despite these facts many small businesses continue to ignore or avoid the risk. Many of our clients believe, "I don't do business online or I don't have any valuable information." Of course, the truth is exactly the opposite. Every time they take an order, swipe a credit card or send an email they put themselves and their customers at risk. Too often the concern is for customer privacy but corporate clients and vendors are at risk too.

Small business present cybercriminals with an easy way to gain access to customer credit card records and bank accounts, supplier networks and employee financial and personal data.

They want to do more and more business online but they have weaker online security. Or they use cloud services that don't have strong encryption. As a result, the small business can be a gateway to gain access to clients, business partners, and contractors and a backdoor into many large organizations. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick. If a small business has any Fortune 500 companies as customers, they are an even more enticing target. These secondary attacks are now a regular problem for small business.

Small businesses are particularly vulnerable to email attacks mimicking their banks or other trusted institutions and citing an urgent need for account or some other vital information, and often

multiple employees have access to that information. Further, business accounts do not enjoy the same protection against loss as consumer accounts—something many small-business owners do not discover until it's too late. Consumers are protected by regulations which limit their liability. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC) and enjoy no such protections. Under the UCC banks aren't liable for unauthorized payments if their security is considered "commercially reasonable". As a result, few small businesses that are the victims of cyber theft ever recover their funds.

More than ever, sensitive data, intellectual property and personal information of small and medium sized firms are targeted by an ever increasing and sophisticated community of cybercriminals. Symantec has found that over the last several years there has been a steady increase in cyber-attacks targeting businesses with less than 250 employees.

And not all hacking is for financial gain. Two years ago, several businesses were simultaneously hacked and their websites were taken over by what appeared to be ISIS. Islamic State logos and Arabic script was plastered all over the sites for Montauk Manor in the Hamptons; Eldora Speedway in New Weston, Ohio; Dogwoods Lodge dog kennel in Des Moines, Iowa; Sequoia Park Zoo in Eureka, CA; Montgomery Inn in Montgomery, Ohio; the Moerlein Lager House in Cincinnati; and Elasticity, a vocational charity St. Louis, MO. No financial information was stolen but imagine the time, effort and lost business for each of these firms. They had to rebuild their sites and try to rebuild client confidence. After all, if you knew a hotel had been hacked would you give them a credit card to hold a reservation?

At the SBDCs we have been working to spread awareness of all these threats to our clients. We offer training programs to our clients at most SBDCs and we are working to expand the coverage to the entire network. In our centers in New York, Delaware, Florida, Texas and others we are developing programs to not only advise and inform our clients but spread the information and training capacity throughout our networks. In Florida, our network is collaborating with Ridge Global, the firm founded by former DHS Secretary Tom Ridge, to develop a series of training videos on cybersecurity. The New York SBDC has developed a cybersecurity planning guide which we are working to disseminate to other states to help them build their capacity. In Michigan, besides training, our network is launching a media campaign day to spread awareness. SBDCs began developing these resources on our own over the last few years. My members recognized that, while they are advising and training their clients on the value of the web as a marketing and sales engine, they also needed to educate them on the dangers and pitfalls of the web.

On top of the organic efforts within the SBDC networks we are now working at the national level to help develop a national small business cyber strategy. Pursuant to section 1841 of the National Defense Authorization Act for 2017 America's SBDCs is working with the Department of Homeland Security (DHS) and the Small

Business Administration (SBA) to develop a strategy to leverage the collective resources of DHS, SBA and the national network of SBDCs to provide the resources, training and assistance small businesses will need.

We will be working share and improve cyber programs, enhance services and raise awareness of the threats. In particular, we want to help develop cost-effective, high-quality tools for small business and a network to share information and analysis on threats.

On behalf of our clients I want to thank the members of this committee for their efforts in getting that language included in the NDAA. The timing could not be more critical, the threats and the awareness of the threats has grown but at the same time so has the confusion. What steps do small businesses need to take? Do they need security software, a cyber specialist, certifications? What tools are effective, what certifications are valid?

SBDCs are developing and training small businesses on that first line of their cyber security needs, the internal focus of basic security practices. Teaching employees about the threats and weaknesses, helping them protect client and customer information. They are also working with small businesses to help them recognize and develop their own strategies and assessments of their needs. My members have developed some excellent education and it will grow stronger but the harder effort is going to be assisting small businesses in dealing with the external demands of cybersecurity.

Commercial customers and big business will have growing demands on the cyber infrastructure of their small business suppliers. What certifications will they demand, what hardware? Who will supply these certifications, and at what cost? If we add federal procurement issues (already a complicated area) how will small businesses cope? I want to divide this area of concern into two sides—commercial business and government business.

On the commercial side, small business faces a real problem. Who is in charge and to whom are they responsible? Last year, the Federal Communications Commission (FCC) stepped into the world of e-commerce and declared Internet Service Providers (ISPs) to be “common carriers”. Now the FCC has decided to hold off on the privacy rule in favor of “harmonization”. Small businesses are left to wonder, “Who is responsible, anyone?”

At America’s SBDC we will be working hard to ensure that our clients have the best possible, most cost-effective tools. At the same time, it would nice to know if anyone further up the “food chain” is to be held accountable. There is a real concern about the trickle down nature of the regulatory framework. While titans like Verizon and Comcast battle Google and Facebook, what level of regulation will be placed on small business?

We know there is a potential for small business to be a back door. Does that mean, in a regulatory framework controlled by internet giants, that the rules will be set by the giants at the expense of the pygmies? We have already seen Google declare that websites without what they consider “adequate security” will be labeled “unsafe”. I do not doubt that http vs. https is serious, but

how many small businesses are either aware of this distinction or aware of what they need to do to be Google compliant?

I expect Google aficionados and techies will call me a Luddite. They would be wrong. I use Chrome and love it. I know what an SSL certificate is. How many small business owners do, or know where they can get the help they need? How much business will a small business lose because they are on eBay and, as of the end of January, eBay wasn't https complaint?

These are the types of trickle-down, large firm favoring regulatory schema about which we should be concerned.

Now I'd like to comment on the government side. The previous administration was proud of their efforts and successes at meeting small business contracting and subcontracting goals. I'm concerned about how weather that success can last. Unfortunately, a lot of the uncertainty we face now is because the previous administration also put out cybersecurity regulations at the very end of their term before anything could really be discussed and tried out. The result is the uncertainty and confusion we see now.

There should be significant concern that federal and state agencies will begin to develop conflicting and potentially contradictory procurement regulations, derived from the best intentions regarding security and privacy, but having a negative effect on small business participation. The Department of Defense has issued cybersecurity amendments to the Defense Acquisition Regulations (DFAR) and the FAR Council issued amendments to the Federal Acquisition Regulations (FAR). Just recently the Department of Homeland Security released three proposed regulations on cybersecurity though they are, I believe being held by the current administration. Those regulations weren't even for classified information; they were for Controlled Unclassified Information (CUI). To date, I have seen only two comments in the Federal Register. I doubt any small business that contracts with DHS is aware of these proposed regulations, and many of our SBDC clients are those affected businesses.

How will all these regulations operate? Can they co-exist? Agencies issue the proposed rules and state they will "harmonize" them with FTC and other efforts, how? Who will "harmonize" them? These regulations have the best and most laudable goals, protecting government data integrity and protecting citizens' privacy. However, the potential costs of compliance for any small business involved in, or wishing to be involved in government contracting could be crippling. Will the standards be set at the convenience of the largest contractors with small businesses left to wonder how they'll be able to comply?

In addition, what will happen to subcontractors? Imagine a one-size fits all cybersecurity protocol that flows down to subcontractors. The potential for small businesses becoming frozen out is very real.

That is why America's SBDCs is glad to be working on this strategy with DHS and SBA now. We want to help head off the confusion and provide training to ensure opportunity is not sacrificed for

cybersecurity. At America's SBDC we believe it important to be at the front of this effort, to develop a set of resources to enable small business participation through assistance and training, rather than having to play "catch up" with small businesses confused by a new regulatory framework.

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



Testimony of

James E. Mooney

President & CEO

Chevron Federal Credit Union

on behalf of

The National Association of Federally-Insured Credit Unions

"Small Business Cybersecurity: Federal Resources and Coordination"

Before the

House Small Business Committee

March 8, 2017

**Introduction**

Chairman Chabot, Ranking Member Velázquez and Members of the Committee, thank you for the invitation to appear before you this morning. My name is Jim Mooney and I am testifying today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU). I am the President and CEO of Chevron Federal Credit Union, headquartered in Oakland, California, and also serve as Chair of NAFCU's Cybersecurity and Payments Committee.

Chevron Federal Credit Union is a federally charted credit union serving the employees of Chevron Corporation, Bechtel Corporation, and numerous smaller companies as well as retirees and family members. We serve 107,000 members through 21 branches located in California, Texas, Utah, Louisiana, Mississippi, and Virginia.

As you are aware, NAFCU is the only national organization exclusively representing the interests of the nation's federally-insured credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federally-insured credit unions. It is my privilege to submit the following testimony on behalf of NAFCU, our credit unions and the 100 million members they represent that have been heavily impacted by ongoing data security breaches by no fault of their own. We appreciate the opportunity to speak about how cybersecurity and data security issues impact credit unions.

**Background on Credit Unions**

Historically, credit unions have served a unique function in the delivery of essential financial services to American consumers. Established by an Act of Congress in 1934, the federal credit

union system was created, and has been recognized, as a way to promote thrift and to make financial services available to all Americans, many of whom may otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to meet a precise public need – a niche that credit unions still fill today.

Every credit union, regardless of size, is a cooperative institution organized “for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes.” (12 USC 1752(1)). While over 80 years have passed since the Federal Credit Union Act (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- credit unions remain wholly committed to providing their members with efficient, low-cost, personal financial services; and,
- credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are small businesses themselves, especially when compared to our nation’s mega banks and largest retailers, facing challenges of meeting the products and service needs of their community, while dealing with various laws and regulations.

#### **Credit Unions and Data Security**

Today, my testimony will cover credit union efforts to maintain a successful track record of protecting member information, NAFCU’s work on the cyber and data security front, the impacts

of recent retailer and merchant data breaches on credit unions and consumers, including the financial burdens they have faced, and NAFCU's principles for data security reform and potential legislative next steps to address consumer data threats that exist in the 21<sup>st</sup> century cyber environment.

As members of the committee are well aware, cyber and data crime has reached epic proportions in nearly all sectors of the economy. Symantec's *2016 Internet Security Threat Report* characterized 2015 as a year when "attacks against businesses and nations hit the headlines with such regularity that we've become numb to the sheer volume and acceleration of cyber threats." According to the report, more than 430 million new pieces of malware were created in 2015 and the number of identities exposed in breaches increased by 21 percent from 2014. While large companies across all sectors are still a prime target, 65 percent of all targeted attacks struck small and medium-sized companies last year.

In a recent report by Javelin Strategy & Research, they found that card not present fraud increased by 40% from 2015 to 2016. The author of the report, Al Pascual, head of security, risk, and fraud at Javelin Strategy & Research noted that the jump in fraud was not simply the shift of card present to card not present fraud, but pointed to the online retailers and merchants not maintaining up-to-date security standards. My credit union's experience is consistent with the report's findings: in the four-year period of 2013 to 2016 -- during which we implemented EMV -- our card-related fraud losses tripled, with 2016 losses approaching three-quarters of a million dollars.

With cyber and data crime becoming more and more prevalent the U.S. government is also working to identify malicious actions within their networks. In 2015 the Department of Homeland Security's Office of Cybersecurity and Communication announced that a network monitoring program would fully cover the government by the end of fiscal year 2016 through the Einstein program used to strengthen perimeter defenses and the Continuous Diagnostics and Mitigation program designed to better detect hackers once systems have already been penetrated. In 2015, Senators Tom Carper and Ron Johnson introduced S. 1869, the Federal Cybersecurity Enhancement Act, which included language authorizing the Department of Homeland Security to use the Einstein program on every federal agency's network. Language from the bill was included in the Cybersecurity Act of 2015, which was a Division N of the omnibus passed in December of 2015 and does not sunset till 2022. As the cybersecurity conversation moves forward we believe that it is important for Congress to also explore industry improvements that can and need to be made regarding data security standards.

NAFCU supports comprehensive data and cybersecurity measures to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA). Unfortunately, there is no comprehensive regulatory structure similar to what GLBA put in place for financial institutions for other entities that may handle sensitive personal and financial data.

In today's digital economy, cybersecurity poses a threat to businesses of all sizes, individual consumers, and even national security. From the financial services perspective, cybersecurity and data security are inextricably linked. Securing consumers' personal information and financial

accounts will require the entire payments ecosystem to take an active role in addressing emerging threats, and in turn require all industries to be proactive in protecting consumers' personally identifiable and financial information from the onset.

As will be discussed in my testimony, credit unions have been able to successfully minimize emerging threats and data breaches. Still, consumers unintentionally put themselves at risk every time they use their debit or credit card. Given the magnitude of the many recent data breaches and the sheer number of consumers impacted, policy makers have a clear bipartisan opening to ensure all industries in the payments system have a meaningful federal data safekeeping standard to help prevent further breaches from occurring.

This hearing is an important one as we are at a critical juncture in the cyber and data security discussion on Capitol Hill. On behalf of NAFCU and our member credit unions, I appreciate the opportunity to be here today.

**Financial Institutions and the *Gramm-Leach-Bliley Act***

GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record protecting valuable information since its enactment in 1999. This record of success is why NAFCU believes any future requirements must recognize this existing national standard for financial institutions such as credit unions.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2)

confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records.

Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among credit unions. The best way to move forward and address data breaches is to create a comprehensive regulatory strategy for industries that are not already subject to oversight with the responsibility of protecting consumer data. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

Below, I outline the key elements, requirements and definitions of the GLBA. Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.

- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

*Sensitive Consumer Information*

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log into or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

*Unauthorized Access to Consumer Information*

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response

programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

*Risk Assessment and Controls*

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is applicable for the largest and smallest in the financial services arena. As the committee considers cyber and data security measures, it should be noted that scalability is achievable and that is inaccurate when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information;
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies;
- Train staff to implement the credit union's information security program; and,

- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.”

*Service Providers*

The security guidelines direct every financial institution to require its service providers through contract to implement appropriate measures designed to protect against unauthorized access to, or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

*Response Program*

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers. Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

*Consumer Notice*

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable the institution's members to take steps to protect themselves against the consequences of identity theft.

*Content of Consumer Notice*

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected fraud or identity theft to the institution.

*Delivery of Consumer Notice*

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

**Regulators Oversight of Financial Sector Cybersecurity**

Since the passage of GBLA, financial regulators have developed robust guidance to help institutions develop information security programs and enterprise risk management policies to address data and cybersecurity needs. In addition, financial regulators oversee bank and credit union cybersecurity through periodic examinations designed to assess the risks associated with IT environments of varying size and complexity.

Guidance promulgated by the Federal Financial Institutions Examination Council (FFIEC) has shaped the contents of bank and credit union examinations. In June 2015, the FFIEC publicly announced its Cybersecurity Assessment Tool (CAT), which was influenced in large part by the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), released by the

National Institute of Standards and Technology (“NIST”) in 2014. Both the Framework and the CAT are voluntary tools that credit unions and banks can use to gauge their cybersecurity readiness. The Framework has endowed the CAT with a common lexicon of cybersecurity terminology, which has also influenced the thinking of other financial institution regulators. Furthermore, NCUA has said that its ongoing update of IT examination procedures will adhere to the principles described in the CAT, and other financial regulators have either aligned their cybersecurity standards more closely with the Framework or voiced support for its risk-based approach.

Financial sector cybersecurity has always been a priority for banking and credit union regulators; however, in recent years it has emerged as top issue. NCUA has made cybersecurity a supervisory priority since 2013, and the agency reminded credit unions in 2016 that “technological innovation, the expansion of social networking and growing interconnectivity are fueling fundamental change in cybersecurity procedures and processes.” NCUA forecasts that elevated risk levels may lead to “higher mitigation costs and lower consumer confidence, as well as greater financial and legal risks.” Likewise, other regulators have either announced changes to their own examination procedures as a result of growing technological complexity in the financial sector, or issued new proposals aimed at mitigating unprecedented levels of data security risk.

#### **Government Resources for Managing Data and Cybersecurity Risk**

Credit unions and banks have benefited from the availability of government initiatives aimed at coordinating information sharing, identifying emerging threats, and promoting greater cybersecurity expertise. A NAFCU survey released in October 2016 revealed that members use government resources such as the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center, the U.S. Department of Treasury's Financial Crimes Enforcement Network, NIST's National Vulnerability Database, and the United States Computer Emergency Response Team (US-CERT) to maintain awareness of emerging data security threats and develop stronger cybersecurity standards. To support interagency coordination across these platforms, NAFCU has engaged the Treasury Department Office of Critical Infrastructure Protection and Compliance Policy to suggest areas of improvement and future opportunities for public-private collaboration.

#### **NAFCU's Work in Various Cyber and Data Security Initiatives**

In addition to these government platforms, many credit unions and banks belong to industry-led organizations such as the Financial Services-Information Sharing and Analysis Center (FS-ISAC), of which NAFCU is a member. As data breaches continue to rise and innovations in payments technology make the entire ecosystem more complex for financial institutions and consumers, involvement in these organizations is as critical as ever.

Specific to payments, NAFCU is a member of the *Payments Security Task Force*, a diverse group of participants in the payments industry that is driving a discussion relative to systems security. NAFCU also supports many of the ongoing efforts at the *Financial Services Sector Coordinating Council* (FSSCC) and the *Financial Services Information Sharing and Analysis Center* (FS-ISAC).

These organizations work closely with partners throughout the government creating unique information sharing relationships that allow threat information to be distributed in a timely manner.

Information sharing is a key weapon in credit unions' arsenal against cybercrime. NAFCU has long held that cyber threats could be mitigated with a greater level of collaboration between financial institutions, and the use of public-private partnerships to share information about threats and cybersecurity best practices. To that end, NAFCU has recently collaborated with FS-ISAC to promote awareness of a new information sharing initiative specific to credit unions. FS-ISAC has spoken to NAFCU's Cybersecurity and Payments Committee about its recently launched Credit Union Advisory Council, which allows member credit unions to share critical insights about emerging data security threats, consult model risk assessments, and gain insights on nearly every aspect of cyber risk management. NAFCU believes that interest in FS-ISAC's advisory council, as well as other credit union led information sharing organizations, demonstrates that credit unions are keenly aware of the fast-evolving threat environment that threatens the financial sector.

NAFCU has also aided industry efforts to make data security effective not just for institutions but also for consumers. In November of 2016, FS-ISAC released its "Sheltered Harbor" initiative to improve cybersecurity defense measures for financial institutions. The creation of Sheltered Harbor came as a response from cybersecurity exercises that FS-ISAC members participated in over this past summer. In the case of potential cyber incidents, Sheltered Harbor would allow financial institutions to securely store member account information in data vaults so it can be protected and restored. NAFCU has provided assistance to support the development and maintenance of the Sheltered Harbor program because it understands the critical importance of

cybersecurity. In today's challenging cyber environment it is important that those who have access to significant customer information look for ways to enhance consumer protections.

NAFCU also worked with NIST on the Framework it released in 2014 which has since guided financial institutions of varying size and complexity through the process of reducing cyber risks to critical infrastructure. The recommendations are designed to evolve and will be updated to keep pace with changes in technology and threats.

NAFCU's efforts to gauge credit union cybersecurity readiness indicate that the vast majority of members have taken a proactive approach to managing data security risks and improving operational resilience. A NAFCU survey published October 2016 revealed that 93.7 percent of survey respondents reported that their credit union participates in some form of information sharing to keep pace with cybersecurity threats, and nearly 70 percent of respondents make use of NIST's National Vulnerability Database to track and monitor common vulnerabilities. NAFCU's survey also showed that the percentage of respondents' overall operating budget devoted to IT/cybersecurity has nearly doubled over the past five years. In addition, to address growing cybersecurity risks, a quarter of all respondents have hired a Chief Information Security Officer to manage cybersecurity-related activities. Meanwhile, half of all respondents have a committee specifically devoted to cybersecurity oversight, and an additional 6.3 percent of respondents have added cybersecurity oversight to their board of directors' or supervisory committee's existing duties.

#### **Protecting Consumer Data is Important**

With the increase of massive data security breaches at retailers, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the 2014 Home Depot breach impacting 56 million payment cards, Americans are becoming more aware and more concerned about data security and its impact. A Gallup poll from October 12-October 15, 2014, found that 69 percent of U.S. adults said they frequently or occasionally are concerned about having their credit card information stolen by hackers, while 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year according to an October 2016 Gallup survey. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Since the large Target and Home Depot breaches there have been many others including the most recent breaches at Wendy's and Arby's fast-food chains. The Arby's breach, which was announced just last month, has so far compromised 355,000 customer credit cards and the investigation is still developing. NAFCU-member, Evansville Teachers Federal Credit Union reported that the Arby's breach impacted 5,214 of their card holders. To shut off the member's breached card, cover the reported fraud, and pay for the card reissue it cost Evansville Teachers Federal Credit Union alone a total of \$52,466.10. With the Arby's breach investigation still unfolding and its known impacts on so many financial institutions already, it is unclear how many more credit unions have or will face similar costs.

Data security breaches are more than just an inconvenience to consumers as they wait for their debit and/or credit cards to be reissued. Breaches often result in compromised card information leading to fraud losses, unnecessarily damaged credit ratings, and even identity theft. Symantec's *Internet Security Threat Report* issued in April of 2016 found that individuals' financial

information was exposed in 33% (over 140 million ) of the 429 million records compromised in the 2015 breaches . That percentage is up significantly from 18% in 2013. More than 23% of the US population had their financial identities compromised by a merchant data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data security breaches at our nation's retailers are happening almost every day. A survey of NAFCU member credit unions in February of 2015, found that respondents were alerted to potential breaches an average of 164 times in 2014. Two-thirds of the respondents said that they saw an increase in these alerts from 2013. When credit unions are alerted to breaches, they take action respond and protect their members. The chart below outlines the actions that credit unions took to respond to data breaches in 2014.



Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

Retailers and credit unions are both targets of cyberattacks. The difference, however, is that credit unions have developed and maintained robust internal protections to combat these attacks and are required by federal law and regulation to protect this information as well as notify their members when a breach occurs, putting them at risk. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to \$1 million per day for compliance violations. These extensive requirements and safeguards discussed earlier in my testimony have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999. In contrast, retailers are not required by *any* federal laws or regulations to protect the consumers' data and notify them when it is breached.

A credit union data security program to protect its own system can have many security components, such as:

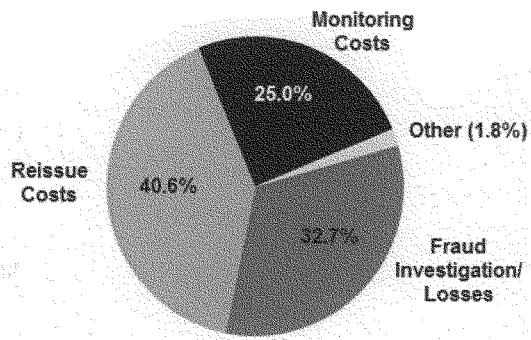
1. Firewall
2. Intrusion Prevention

3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email
12. Encryption
13. End point security

These elements can have a significant cost to the institution. A February, 2015, survey of NAFCU members found that the average respondent credit union spent \$136,000 on data security measures in 2014, which does not even factor in the additional costs that the credit union faced due to data breaches at other entities.

The ramifications of recent data breaches for credit unions and their members have been monumental. The aforementioned survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were \$226,000 on average per credit union. Almost all respondents noted that merchant data breaches lead to increased member-service costs and needs that are not reflected in these direct costs. The three main elements of these costs were card reissuing costs, fraud investigations/losses and account monitoring. The chart on the next page outlines how these various costs from merchant data breaches are broken down.

### Percent of Fraud-Related Costs in 2014



The data breaches in 2014 for the credit union I serve as President and CEO, Chevron Federal Credit Union, were estimated to have cost us \$294,804. From 2013 through 2016 data breaches have cost my credit union an estimated total of \$833,000 in member notification and card resissue expenses. This does not even include the actual fraud losses. These costs are almost double what Chevron Federal Credit Union pays to annually for information security systems and services, which does not include the costs of our three-person IT Information Security team.

Another cost, though difficult to measure: members often do not know that their compromised cards are due to a specific data breach. The card networks do not identify the compromise sources in their card alerts. Therefore, credit union staffs typically can only inform affected members that their cards may be compromised, not the source of the compromise. For all the members know, the source of the problem may be the credit union itself. This undoubtedly can have an unjustified but damaging effect on their confidence in their credit union.

Additionally, one of the residual effects that goes largely unnoticed is the impact that the reissuance of a card has on the neural network of a credit union. This is a credit union's own fraud detection system. Some of the components of the system are payment patterns and history of card usage, as is the case with most neural networks. Every time a credit union has to reissue a card, the pattern and history for that member is erased and it starts over. This increases the chance that the member will make a purchase that is perfectly acceptable, but get denied because the network does not recognize that what they are doing is perfectly normal. This is especially true for credit union members who travel.

Unfortunately, credit unions often never see any reimbursement for their costs associated with the majority of data breaches. Even when there are recoupment opportunities, such as the recent Target settlement with MasterCard, it is usually only pennies on the dollar in terms of the real costs and losses incurred. Meanwhile, big box retailers that were negligent in recent data security breaches are posting record profits. A 2015 Columbia University review of financial statements of merchants such as Target and Home Depot reveals that retailers barely notice a financial hit from massive data breaches, and breach costs were less than one-tenth of one percent of these giant retailers 2014 annual sales.

Payment networks are critical partners to credit unions in ensuring credit union members have the credit and debit card programs they need and demand. Collectively, the networks have worked together to standardize the Payment Card Industry (PCI) Data Security Standard designed to provide merchants and retailers with a framework of specifications, tools, measurements and support resources to ensure the safe handling of cardholder information. While NAFCU

appreciates the positive progress is this regard, credit unions and other issuers are still seeing steep losses in the wake of retailer and merchant data breaches and would like to see the networks do everything they can to make reimbursement in the wake of fraud stemming from a data breach more equitable. As discussed, NAFCU believes the negligent entity should be wholly responsible for such damages.

#### **NAFCU's Key Data Security Principles**

NAFCU has long been active on the data security front, and was the first financial services trade association to call for Congressional action in the wake of the 2013 data breach at Target. Recognizing that a legislative solution is a complex issue, NAFCU's Board of Directors has also established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *GLBA*.
- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

#### **Preventing Future Breaches**

NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for retailers and merchants akin to what credit unions already comply with under the GLBA.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that financial institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach.

While some have said that voluntary industry standards should be the solution, the *Verizon 2015 Payment Card Industry Compliance Report* found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the 10 year study, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves retailers and merchants, and therefore consumers, more vulnerable to breaches.

In addition, the report finds that the use of EMV cards ("chip cards") in other countries has not been a silver bullet solution to preventing fraudulent activity, but merely displaces it. The report shows that once EMV use increases, criminals shift their focus to card not present transactions, such as online shopping. While some argued for the "chip card" solution, the reality is that it is not a panacea and does not replace a sound data security standard.

One basic but important concept to point out with regard to almost all cyber and data threats is that a breach may never come to fruition if an entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data

in their systems. Enforcement of prohibition on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

#### **Legislative Solutions**

NAFCU believes that the best legislative solution on the issue of data security is the bipartisan legislation that was introduced in the 114<sup>th</sup> Congress by Senators Roy Blunt and Tom Carper and Congressman Randy Neugebauer. The legislation, S. 961/H.R. 2205, the *Data Security Act of 2015*, would have set a national data security standard that recognized those who already have one under the GLBA. We supported these bills and would urge for reintroduction in both the Senate and the House.

As the committee is aware, the cyber and data security discussions cross the jurisdiction of several Congressional committees. Given the daunting task of making meaningful reform in these areas, NAFCU would like to encourage congressional leadership to create a bipartisan and bicameral working group to find a legislative path forward to help better protect consumers from ongoing data breaches.

#### **Conclusion**

Cyber and data security, ensuring member safety, and how to incentivize and emphasize data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. Given the breadth and scope of many recent retailer and merchant data breaches, we have reached a tipping point in the public dialogue about how to tackle these issues. NAFCU member

credit unions and the 106 million credit union members across the country are looking to Congress to continue work on cyber and data security issues and move forward with legislation that will make a meaningful difference to consumers. It is time to level the playing field and require equal data security treatment to all those who collect and store personally identifiable and financial data.

Consumers will only be protected when every sector of industry is subject to robust federal data safekeeping standards that are enforced by corresponding regulatory agencies. It is with this in mind that NAFCU urges Congress to modernize data security laws to reflect the complexity of the current environment and insist that retailers and merchants adhere to a strong federal standard in this regard.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.

**Statements for the Small Business Committee Record****Congressman Adriano Espaillat (NY-13)****March 8, 2017**

Thank you Chairman Steve Chabot and Ranking Member Nydia Velazquez for holding this timely briefing before our committee.

I have the distinguished honor of also sitting on the Foreign Affairs Committee, where this week, we will be discussing Russia's interference in the U.S. election, as well as their use of propaganda and fake news to influence policy. So, you will imagine, it came as no surprise to me when I read that in its 2011 report, the Office of the National Counter Intelligence Executive conveyed that "tens of billions of dollars in trade secrets, intellectual property, and technology are stolen each year from computer systems in the federal government, corporations, and academic institutions" – and they identified China and Russia as the two largest participants in cyber espionage.

1. Should Congress have a separate independent investigation of Russia, solely focused on cyberattacks, and their impacts on American businesses? If so, what additional information do you think we will learn?

**I defer to my colleagues in the national security and criminal law enforcement communities on this issue. The FTC's main role in cybersecurity is to encourage businesses to shore up their defenses to protect against attacks, educate consumers on good security practices, and mitigate any harms.**

Small businesses in my District often struggle just to install Wi-Fi, and I imagine that like business across the country, the costs of cybersecurity attacks are often more costly.

So my questions are for the panel:

1. What can the federal government do to help offset some of these cost burdens?

**We can help small businesses by providing them with resources on how to protect themselves and their customers from cybersecurity threats. In today's world, consumers and small businesses are at risk of a variety of harms from cyberattacks. For example, there are increasing concerns about ransomware, where a malicious actor can hold a company's data and hardware hostage in exchange for payment. Because the costs of a successful attack can be exorbitant, it makes sense for companies to invest in reasonable cybersecurity protection on the front end, to reduce the chances of such an attack in the first place. Many of the most basic but sometimes neglected steps are cost-effective.**

**The FTC has developed free, user-friendly education materials to help companies of all sizes improve their security practices. For example, the FTC offers guidance to assist businesses in designing and implementing information security programs, as well as**

guidance describing immediate steps companies should take when they experience a data breach. The FTC has also educated businesses about threats like ransomware and phishing, and developed guidance for specific industries such as the Internet of Things device manufacturers and mobile app developers. All of these materials are available on our website. We encourage Members of Congress to link to these materials and further distribute them to their constituents.

2. How can the federal government best balance civil liberties protections with information sharing, and the ability to help protect small businesses from cyber-attacks?

I believe there should be coordinated information sharing on cybersecurity between government and industry, and among industry participants, to identify risks, threat vectors, and actual incidents. Such sharing provides stakeholders with valuable information so that they can adjust their security programs in light of known risks. To this end, I have supported the creation of industry-specific Information Sharing and Analysis Centers (ISACs) to enable industry members to pool information about security threats and defenses so that they can prepare for new kinds of attacks and quickly address potential vulnerabilities. To be most effective, ISACs may receive information from, and share information with, relevant government agencies. Because some private entities may have been hesitant to share information with competitors due to antitrust concerns, the FTC and DOJ issued an Antitrust Policy Statement on Sharing of Cybersecurity Information in 2014, which noted that antitrust law should not be a “roadblock to legitimate cybersecurity information sharing.” [https://www.ftc.gov/system/files/documents/public\\_statements/297681/140410ftcdojcyberthreatstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf). I continue to believe that this kind of information sharing is valuable, and support ISACs and other tools to assist small businesses in identifying and responding to cyber risks.

Statements for the Small Business Committee Record Congressman  
Adriano Espaillat (NY-13)  
March 8, 2017

Thank you Chairman Steve Chabot and Ranking Member Nydia Velazquez for holding this timely briefly before our committee.

I have the distinguished honor of also sitting on the Foreign Affairs Committee, where this week, we will be discussing Russia's interference in the U.S. election, as well as their use of propaganda and fake news to influence policy. So, you will imagine, it came as no surprise to me when I read that in its 2011 report, the Office of the National Counter Intelligence Executive conveyed that "tens of billions of dollars in trade secrets, intellectual property, and technology are stolen each year from computer systems in the federal government, corporations, and academic institutions" – and they identified China and Russia as the two largest participants in cyber espionage.

- 1. Should Congress have a separate independent investigation of Russia, solely focused on cyberattacks, and their impacts on American businesses? If so, what additional information do you think we will learn?**

**NIST Response:**

NIST is a non-regulatory, non-oversight agency with the principal mission of advancing measurement science. NIST provides technical guidance and specifications for cybersecurity. Whether to have a "separate independent investigation of Russia" focused on cyberattacks is a decision for Congress and its authorized committees to make, and therefore outside the scope of NIST's mission.

Small businesses in my District often struggle just to install Wi-Fi, and I imagine that like business across the country, the costs of cybersecurity are often too much to burden. However, we also know that the aftermath of cybersecurity attacks are often more costly.

So my questions are for the panel:

- 1. What can the federal government do to help offset some of these cost burdens?**

**NIST Response:**

Small businesses are more innovative, agile, and productive than ever, thanks to the capabilities delivered by information technology (IT), but the IT security challenge for small businesses looms larger than ever. Many small businesses have limited resources and budgets. Small businesses will benefit from practical information security training and solutions that enable them to cost-effectively manage information security risks.

NIST develops and disseminates cybersecurity standards, and resources that are accessible and usable by small businesses to help them understand and manage cybersecurity risks to their enterprises. These resources include guidelines and example solutions of how organizations of varying sizes, types, and cybersecurity capabilities can understand, prioritize, implement, and maintain practical cybersecurity approaches and solutions to make their enterprises more secure.

Examples include the recently updated NIST Small Business Information Security Guideline, the Cybersecurity Framework, and example implementations – developed at NIST’s National Cybersecurity Center of Excellence – that organizations can replicate to address specific real-world cybersecurity challenges. These resources provide understandable approaches that help small businesses establish and improve their cybersecurity programs, and express their cybersecurity requirements to external service providers.

NIST also collaborates with other government agencies and with industry to understand cybersecurity challenges impacting small businesses and provides training and other resources to help small business understand and manage cybersecurity risks.

- 2. How can the federal government best balance civil liberties protections with information sharing, and the ability to help protect small businesses from cyber-attacks?**

**NIST Response:**

One way in which the Federal Government can help to optimize information sharing is

by using standard information-sharing formats. Using standardized formats allows users to pre-select the types of information to be shared and minimizes the potential for sharing information that is not actually needed for a cybersecurity purpose. Standardizing information formats can also decrease the burden on small businesses by reducing the time and expertise needed for assessing which information is important for cybersecurity, and which information need not be shared. Standardized formats can help small businesses receive information that is already filtered. Small businesses can also follow the guidance for entering information in a standardized format designed to protect privacy.

NIST has participated in an interagency process to develop technical specifications for the format and exchange of cyber threat information using the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) that help organizations share information while protecting privacy.

STEVE CHABOT, Ohio  
Chairman

NYDIA M. VELAZQUEZ, New York  
Ranking Member

## Congress of the United States

U.S. House of Representatives  
Committee on Small Business  
2561 Rayburn House Office Building  
Washington, DC 20515-0715

March 15, 2017

### VIA E-MAIL

Mr. C. E. Rowe  
President & CEO  
America's Small Business Development Centers (SBDC)  
8990 Burke Lake Rd  
Burke, VA 22015

Dear Mr. Rowe:

In order to have a complete record for the hearing titled, "Small Business Cybersecurity: Federal Resources and Coordination," held on March 8, 2017, the following questions are being submitted by Representative Espaillat for your response.

Please provide your response to all questions by April 8, 2017, to the attention of the Committee's clerk, Delia Barr, at [Delia.Barr@mail.house.gov](mailto:Delia.Barr@mail.house.gov), for inclusion in the hearing record. In addition, please send your response to Deputy Staff Director (Democratic Staff) Melissa Jung, at [Melissa.Jung@mail.house.gov](mailto:Melissa.Jung@mail.house.gov).

Thank you for your participation and your timely reply.

Sincerely,

Steve Chabot  
Chairman

## Statements for the Small Business Committee Record

Congressman Adriano Espaillat (NY-13)

March 8, 2017

Thank you Chairman Steve Chabot and Ranking Member Nydia Velazquez for holding this timely brief before our committee.

I have the distinguished honor of also sitting on the Foreign Affairs Committee, where this week, we will be discussing Russia's interference in the U.S. election, as well as their use of propaganda and fake news to influence policy. So, you will imagine, it came as no surprise to me when I read that in its 2011 report, the Office of the National Counter Intelligence Executive conveyed that "tens of billions of dollars in trade secrets, intellectual property, and technology are stolen each year from computer systems in the federal government, corporations, and academic institutions" – and they identified China and Russia as the two largest participants in cyber espionage.

1. Should Congress have a separate independent investigation of Russia, solely focused on cyberattacks, and their impacts on American businesses? If so, what additional information do you think we will learn?  
*If Congress is going to investigate cybercrime and not look at all the potential malefactors then it is not a worthwhile effort. Every attack, no matter where it originates should be a concern. This is because so many avenues and methods for cyberattacks can be copied and used as disguises.*  
*A larger investigation would teach us that the world-wide threat is a real national economic security issue, and not limited to one nation's actions.*

Small businesses in my District often struggle just to install Wi-Fi, and I imagine that like business across the country, the costs of cybersecurity are often too much to burden. However, we also know that the aftermath of cybersecurity attacks are often more costly.

So my questions are for the panel:

1. What can the federal government do to help offset some of these cost burdens?  
*Many of the best measures for protecting assets are not costly at all, they are simple common sense actions. The federal government should concentrate on a broader availability of existing resources and training. I was interested to hear that NIST and the FCC regularly produce educational*

*material but it is not widely disseminated. Better coordination between the agencies and better distribution of their resources would be a solid first step.*

2. How can the federal government best balance civil liberties protections with information sharing, and the ability to help protect small businesses from cyber-attacks?

*The best way to protect civil liberties is for the federal government to restrain its overcollection of personally identifiable information. Too many governmental entities request, require and store vital information from business owners and then fail to safeguard it. While a small business owner may be able to shield information from competitors, vendors or malefactors they are often forced to give it to the government.*

*As for a free and open internet, the best protection is not restricting access but informing citizens. Helping citizens understand encryption and technology is far preferable to government intervention with its propensity to be abused by human frailty.*

Mooney responses for Questions for the Small Business Committee Record  
Congressman Adriano Espaillat (NY-13)  
March 8, 2017

1. Should Congress have a separate independent investigation of Russia, solely focused on cyberattacks, and their impacts on American businesses? If so, what additional information do you think we will learn?

- 1) Any decisions regarding investigations on cyberattacks from/by Russia should be determined by Congress. Neither I nor NAFCU have a position or comment on the issue. What we do observe is that cyberattacks against consumers and businesses come from criminals domestically and from around the world. We believe that there should be a strong national data security standard in place to deal with all such cyberattacks.

Small businesses in my District often struggle just to install Wi-Fi, and I imagine that like business across the country, the costs of cybersecurity are often too much to burden. However, we also know that the aftermath of cybersecurity attacks are often more costly.

So my questions are for the panel:

- 1) What can the federal government do to help offset some of these cost burdens?
  - 1) First and foremost, data and cyber security is the responsibility of every entity that handles sensitive consumer information across the payments ecosystem. With this in mind, I believe that a scalable and flexible standard like the Gramm-Leach-Bliley Act is essential to prevent many of the data breaches that have become all too common. Implementing a strong national standard for data security should complement any national cyber security framework. There are simple and straightforward steps that businesses of any size can take with nominal costs to greatly improve data security. Some of these are: using and regularly updating anti-virus software, use of strong passwords and securing of technology, and vetting vendor security standards.

In addition, Congress and federal regulators should also pair action on cybersecurity with the elimination of redundant and unnecessary regulations in other areas. While government should respond to areas of clear necessity, as is the case with cyber and data security, it is obvious that "regulation for regulation's sake" does not work. Such a mindset has created an environment that has ultimately hurt Main Street. If overly burdensome regulations are rolled back where they are unnecessary, then small businesses and credit unions will have more resources available to hire employees, serve consumers, improve their communities, and defend against cyber threats.

2. How can the federal government best balance civil liberties protections with information sharing, and the ability to help protect small businesses from cyber-attacks?

- 2) One of the biggest issues with information sharing is that, currently, there is no federal requirement for any breached entity to disclose a breach of their systems, much less notify the individual whose personally identifiable or financial information was compromised. Additionally, a financial institution is not allowed to disclose the source of a breach if they take precautionary security measures such as replacing cards – this often gives the impression to consumers that it was the financial institution that was breached and poses for such institutions a significant and undeserved reputational risk. Any consumers whose sensitive data has been compromised have the right to know the identity of the breached entity so they can decide for themselves whether they want to continue to do business with that entity. The current system is unfair to consumers and deprives them of informed consent.



March 8, 2017

## Countering Cyber Risk for Community Banks and Their Small Business Partners

On behalf of the more than 5,800 community banks represented by ICBA, we thank Chairman Chabot and Ranking Member Velazquez for convening today's hearing entitled: "Small Business Cybersecurity: Federal Resources and Coordination." This is a critical topic for community banks both as small businesses that hold sensitive customer data and as the primary lenders to small businesses. Community banks have a vested interest in small-business cybersecurity and prosperity. ICBA is pleased to have this opportunity to offer this statement for the record.

### **The Community Bank-Small Business Partnership**

America's community banks are prolific small business lenders, playing an outsized role in funding small businesses and the jobs they create. While community banks represent 17 percent of all U.S. bank assets, they make more than half of all small business loans. Small businesses create nearly two-thirds of all new jobs in the United States and account for more than half of all employment.

### **Community Banks and Cybersecurity**

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service, and cybersecurity is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their individual data and critical systems.

Community banks adhere to existing law, regulation and guidance for protecting both bank and customer data. For example, the Federal Financial Institutions Examination Council ("FFIEC") Information Technology Examination Handbook ("IT Handbook") provides guidance and is the standard by which banks are examined based on operational resiliency, scope, risk, and complexity with regard to cybersecurity. All community banks are examined and supervised to ensure they comply with the requirements of the IT Handbook.

One of these requirements is to conduct a risk assessment. This is critical to any business entity that operates in today's modern technological environment. Risk assessments can be done by employing a variety of tools, frameworks, and assessments. Many of these have been developed by the private sector and include the Control Objectives for Information and Related Technology

*Our Mission: Community Banks.®*

1615 L Street NW, Suite 900, Washington, DC 20036 ■ 202-659-8111 ■ Fax 202-659-9216 ■ [www.icba.org](http://www.icba.org)

("COBIT") and the SANS CIC Critical Security Controls. Others have been introduced for voluntary use by community banks, such as the FFIEC Cybersecurity Assessment Tool ("CAT"). There is also the NIST Cybersecurity Framework. With the exception of the IT Handbook, all of these tools, frameworks, and assessments are voluntary, and it is critical to community banks that they remain so.

It is not uncommon for community banks to employ parts of various voluntary frameworks, tools, and assessments to create a tailored cybersecurity program for their institution, based on the banks' risk, size, and scope. ICBA believes both Congress and the federal banking agencies should recognize this flexible approach to cybersecurity, and any new legislation or regulation must preserve this approach.

#### **Data Security**

Data breaches at national retail chains and elsewhere have the potential to jeopardize consumers' financial integrity and confidence in the payments system. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice and legal and regulatory requirements. Safeguarding customer information is central to maintaining public trust and retaining customers. However, bad actors will continue to look for weaknesses in the payments and information systems in various industries, and breaches will occur. ICBA supports the following to mitigate losses in the event of a breach:

- All participants in the payments system, including merchants, and all entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards.
- ICBA supports a national data security breach and notification standard to replace the current patchwork of state laws.
- Community banks should be notified of a potential and/or actual breach as expeditiously as possible in order to mitigate losses.
- The costs of data breaches should ultimately be borne by the party that incurs the breach. Barring a shift in liability to the breached entity, community banks should continue to be able to access various cost recovery options after a breach.
- Banks, card networks, and financial technology companies must continue to freely innovate to effectively protect consumer data and confidence.
- ICBA strongly supports ongoing regulatory efforts and existing, voluntary, public-private partnerships to address the growing threat of cyber-attacks.
- ICBA supports stronger data security standards for regulatory agencies and staff.

*One Mission. Community Banks.<sup>®</sup>*

1615 L Street NW, Suite 900, Washington, DC 20036 • 202-659-8111 • Fax 202-659-9216 • [www.icba.org](http://www.icba.org)

**Payment Security**

Payment card system stakeholders, including networks, merchants, card issuers, and cardholders, are concerned about growing security risks and the shift to more sophisticated and secure technology such as chip, tokenization, and end-to-end encryption. While chip cards, with or without PINs, are a step in the right direction in terms of data security, they are not a panacea. None of the major, recent data breaches at U.S. retailers were caused by customers using payment cards without PINs, and none of these breaches would have been prevented by customers using cards with PINs.

Re-engineering a payments system is not an easy task as there are many players that need to collaborate, from the card networks and processors to the bank issuers and merchants. ICBA is actively participating in this migration by conveying the community bank perspective to all stakeholders and communicating the implications of these changes to community banks and their customers.

**Closing**

Thank you again for convening this hearing and raising the profile of a critical topic for community banks and the small businesses they partner with. ICBA looks forward to continuing to work with the committee in our combined effort to better coordinate cybersecurity efforts, promote payments security, and protect against costly and damaging data breaches.

*One Mission. Community Banks.<sup>®</sup>*

1615 L Street NW, Suite 900, Washington, DC 20036 ■ 202-659-8111 ■ Fax 202-659-9216 ■ [www.icba.org](http://www.icba.org)

