

IS MY DATA ON HEALTHCARE.GOV SECURE?

HEARING BEFORE THE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY HOUSE OF REPRESENTATIVES ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2013

Serial No. 113-55

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

86-893PDF

WASHINGTON : 2013

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

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California	EDDIE BERNICE JOHNSON, Texas
RALPH M. HALL, Texas	ZOE LOFGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin	DANIEL LIPINSKI, Illinois
FRANK D. LUCAS, Oklahoma	DONNA F. EDWARDS, Maryland
RANDY NEUGEBAUER, Texas	FREDERICA S. WILSON, Florida
MICHAEL T. McCAUL, Texas	SUZANNE BONAMICI, Oregon
PAUL C. BROUN, Georgia	ERIC SWALWELL, California
STEVEN M. PALAZZO, Mississippi	DAN MAFFEI, New York
MO BROOKS, Alabama	ALAN GRAYSON, Florida
RANDY HULTGREN, Illinois	JOSEPH KENNEDY III, Massachusetts
LARRY BUCSHON, Indiana	SCOTT PETERS, California
STEVE STOCKMAN, Texas	DEREK KILMER, Washington
BILL POSEY, Florida	AMI BERA, California
CYNTHIA LUMMIS, Wyoming	ELIZABETH ESTY, Connecticut
DAVID SCHWEIKERT, Arizona	MARC VEASEY, Texas
THOMAS MASSIE, Kentucky	JULIA BROWNLEY, California
KEVIN CRAMER, North Dakota	MARK TAKANO, California
JIM BRIDENSTINE, Oklahoma	ROBIN KELLY, Illinois
RANDY WEBER, Texas	
CHRIS STEWART, Utah	
CHRIS COLLINS, New York	

CONTENTS

November 19, 2013

Witness List	Page 2
Hearing Charter	3

Opening Statements

Statement by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	6
Written Statement	7
Statement by Representative Eddie Bernice Johnson, Ranking Minority Mem- ber, Committee on Science, Space, and Technology, U.S. House of Rep- resentatives	8
Written Statement	9

Witnesses:

Mr. Morgan Wright, Chief Executive Officer, Crowd Sourced Investigations, LLC	
Oral Statement	11
Written Statement	14
Dr. Fred Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University	
Oral Statement	25
Written Statement	27
Dr. Avi Rubin, Director, Health and Medical Security Laboratory Technical Director, Information Security Institute, Johns Hopkins University (JHU)	
Oral Statement	35
Written Statement	37
Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC	
Oral Statement	41
Written Statement	44
Discussion	65

Appendix I: Answers to Post-Hearing Questions

Mr. Morgan Wright, Chief Executive Officer, Crowd Sourced Investigations, LLC	104
Dr. Fred Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University	112
Dr. Avi Rubin, Director, Health and Medical Security Laboratory Technical Director, Information Security Institute, Johns Hopkins University (JHU) ..	120
Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC	124

Appendix II: Additional Material for the Record

Letter from the Identify Theft Resource Center submitted for the record by Representative Lamar S. Smith, Chairman, Committee on Science, Space, and Technology	132
---	-----

IV

	Page
Centers for Medicare & Medicaid Services memorandum submitted for the record by Representative Larry Bucshon, Committee on Science, Space, and Technology	135

IS MY DATA ON HEALTHCARE.GOV SECURE?

TUESDAY, NOVEMBER 19, 2013

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Committee met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Committee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

Is My Data on Healthcare.gov Secure?

Tuesday, November 19, 2013
10:00 a.m. to 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Morgan Wright, Chief Executive Officer, Crowd Sourced Investigations,
LLC

Dr. Fred Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security,
Southern Methodist University

Dr. Avi Rubin, Director, Health and Medical Security Laboratory Technical
Director, Information Security Institute, Johns Hopkins University (JHU)

Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC

**U.S. House of Representatives
Committee on Science, Space, and Technology**

HEARING CHARTER

Is My Data on Healthcare.gov Secure?

Tuesday, November 19, 2013
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

At 10:00 a.m. on November 19, 2013, the Committee on Science, Space, and Technology will hold a hearing titled “*Is My Data on Healthcare.gov Secure?*” The data passing through the Healthcare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. In order to gain information on potential healthcare coverage through the website, users must input personal contact information, birth dates and social security numbers for all family members, as well as household salary and debt information. Users may also be asked to verify home mortgage and credit card information, place of employment, previous addresses, and whether the person has any physical or mental disabilities. This hearing will explore the threat posed by identity theft to Americans if hackers gained such information through the Healthcare.gov website, assess the security controls in place and its vulnerabilities by cybersecurity experts not involved with the website, and what specific security standards and technical measures should be in place to protect Americans’ privacy and personal information on Healthcare.gov.

Witnesses

- **Mr. Morgan Wright**, Chief Executive Officer, Crowd Sourced Investigations, LLC
- **Dr. Fred Chang**, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University
- **Dr. Avi Rubin**, Director, Health and Medical Security Laboratory Technical Director, Information Security Institute, Johns Hopkins University (JHU)
- **Mr. David Kennedy**, Chief Executive Officer, TrustedSEC, LLC

Overview

The data on Healthcare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies¹ along with state agencies and government contractors. Federal agencies have a duty to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act (FISMA). However, according to documents from the Department of Health and Human Services, the security of the health care website had not been fully tested when it went public last month, and many cybersecurity experts have expressed concern about flaws in the website that put the personal data of Americans using the website at risk to identity theft from cybercriminals/hackers. According to testimony before the Homeland Security Committee, hackers have already tried to attack the Healthcare.gov website.²

Several government agencies within the Science, Space, and Technology Committee's jurisdiction have responsibilities with information security over the Internet. According to the website of the White House Office of Science and Technology Policy,³

The Obama administration and OSTP will develop policies that will:

- **Bring government into the 21st Century:** Establish a Chief Technology Officer position within the Executive Office of the President to ensure that every government branch and agency has the right infrastructure, policies and services for the 21st century
- **Create an Open and Transparent Democracy:** Develop cutting-edge technologies to create a new level of transparency, participation, and collaboration for America's citizens and enhance scientific integrity in government decision-making.
- **Protect America's Cyber Networks:** Initiation of new and powerful protection strategies to ensure that America's cyber network remains safe from espionage and disruption while at the same time increasing the Federal Trade Commission's enforcement budget so it can step up efforts to track down cyber criminals.

Investment in these important technologies cannot be expected to remain strong if there is not an equally strong intellectual property regimen in place to promote innovation, investment and protect the rights of developers. And citizens cannot be expected to embrace these technologies unless they can be adequately assured that private information will be protected.

Under FISMA, the National Institute of Standards and Technology (NIST)—an agency within Department of Commerce—is tasked with providing standards and guidelines for non-Defense-related Federal agencies to use in developing Information Technology (IT) networks.

¹ The seven agencies are: Internal Revenue Service, Social Security Administration, Department of Homeland Security, Department of Defense, Department of Veterans Affairs, Office of Personnel Management and Peace Corps; See Stacy Cowley, "How Obamacare's 'privacy nightmare' database really works," CNN.com, July 24, 2013, available at <http://money.cnn.com/2013/07/23/technology/security/obamacare-privacy>.

² Joe Johns and Stacy Samuel, "Official: Hackers tried repeatedly to attack Obamacare website," CNN.com, November 18, 2013, available at: <http://www.cnn.com/2013/11/13/politics/hackers-attack-obamacare-site/>

³ Office of Science and Technology Policy, Technology & Innovation, available at: <http://www.whitehouse.gov/administration/eop/ostp/divisions/technology>.

The standards and guidelines that NIST issues require the Chief Information Officer (CIO) or Chief Technology Officer (“technology officer”) at each Federal agency to address certain privacy and security standards and document how those standards were applied or modified in the development, fielding and deployment of its IT network.

The first level of inquiry requires the technology officer to develop a system security plan. In developing such a plan, the technology officer must decide what level of security to provide. NIST guidelines provide assistance on the level of security that should be chosen as well as which security requirements correspond with each level. The guidelines outline specific controls that should be considered and the technology officer must consider each type of control and provide an explanation for choosing not to use certain controls.

The second level of inquiry is the information security risk assessment. Once the controls have been implemented, a security assessment should be performed based on NIST guidelines for the assessment of the security controls. The security assessment should determine whether the system and controls are operating as intended, whether the controls are implemented as intended, and whether the controls are supporting privacy policies. The technology officer then is required to provide a report assessing the security of the system.

The package accompanying the authorization to operate will include the security plan, the security assessment, and a plan of action and milestones. The plan of action and milestones are the future plans to continue addressing risk factors and continue monitoring risks. The technology officer for every Federal agency must decide whether to issue an authorization based on these three documents. An authorization to operate may be issued for up to three years, but may be for a shorter period time.

On September 3rd, shortly after an Inspector General IG report to the Center for Medicare and Medicaid Services (CMS) outlined concerns that CMS had missed several key deadlines and would not have time to adequately perform testing for the security of the website, the CMS Chief Information Officer supported moving forward with approval of the website despite indications of numerous issues that could compromise its security. The documents indicate that the system security utilizing the NIST guidelines was identified as a Moderate level rather than a High level.

In addition to the threat from hackers with malicious intent of identity theft, the Healthcare.gov system is also routing personal information about individuals to the wrong people. According to news reports, Mr. Justin Hadley of North Carolina recently downloaded a letter from the Healthcare.gov website that included personal information belonging to Mr. Thomas Dougall of South Carolina. Mr. Dougall contacted the website to rectify the problem, but soon realized they had “no procedure whatsoever to handle security breaches.”⁴ Another case involves a Missouri woman, Ms. Lisa Martinson, who called Healthcare.gov’s customer service after forgetting her password. She was informed that three different people were given

⁴ Sterling Beard, “Healthcare.gov Users Warn of Compromised Personal Information,” *National Review Online*, Nov. 4, 2013, available at <http://www.nationalreview.com/corner/363031/healthcaregov-users-warn-compromised-personal-information-sterling-beard>.

Chairman SMITH. The Committee on Science, Space, and Technology will come to order. Good morning to everyone. Our hearing today is on the subject of the security of data on the HealthCare.gov website. I am going to recognize myself for an opening statement and then the Ranking Member.

Many Americans are beginning to experience the ill effects of Obamacare. That is because the President's broken promises are piling up. He promised that if you like your health care plan you can keep it. But for millions of Americans, that is not true. He said that the law would make health insurance more affordable. But across the country, Americans are seeing their premiums go up, not down. And when launching HealthCare.gov, the Obama Administration said that the website was safe, secure and open for business. We now know that isn't true either.

The data obtained by HealthCare.gov is one of the largest collections of personal information ever assembled. It links information between seven different Federal agencies and state agencies and government contractors. The website requires users to provide personal information like birth dates, Social Security numbers and household incomes in order to obtain information about potential health coverage. But security experts have expressed concern about flaws in the site that put this personal data at risk and subject users to the threat of identity theft.

The Science Committee oversees the agencies responsible for setting privacy and security policies and standards for the rest of the federal government, the White House Office of Science and Technology Policy and the National Institute for Standards and Technology. The Obama Administration has a responsibility to ensure that the personal and financial data collected by the government is secure. Unfortunately, in their haste to launch the HealthCare.gov website, it appears the Administration cut corners that leaves the site open to hackers and other online criminals. So the question for today's hearing is: Can Americans trust the federal government with their personal information on the HealthCare.gov website?

Today, we are going to hear from witnesses from outside the government who are experts in cybersecurity and hacking websites. Our witnesses will provide their professional assessment of the vulnerabilities that underlie HealthCare.gov. Several vulnerabilities have already been identified, and we know of at least 16 attempts to hack into the system. And I heard this morning that there were another 50. But we can assume that many more security breaches have not been reported.

Here are some real-life examples. Mr. Thomas Dougall of South Carolina received a surprise phone call from a stranger one Friday evening explaining that he had just downloaded a letter off the HealthCare.gov website containing Dougall's personal information. And when Lisa Martinson of Missouri called HealthCare.gov's customer service after forgetting her password, she was told three different people were given access to her account, address and Social Security number.

Also, it turns out that Federal employees called navigators who help users apply for insurance on the HealthCare.gov website have

not received background checks yet they are able to access the personal information of thousands of people.

Many Americans have been the victims of identity theft by computer hackers. Identity theft jeopardizes credit ratings and personal finances. The massive amount of personal information collected by the HealthCare.gov website creates a tempting target for scam artists. These threats to Americans' well-being and financial security should make us question the future of Obamacare. Perhaps it is time to take Obamacare off of life support.

Americans deserve a healthcare system that works and that they can trust. Obamacare is no cure.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF CHAIRMAN LAMAR S. SMITH

Many Americans are beginning to experience the ill effects of Obamacare. That's because the President's broken promises are piling up. He promised that if you like your health care plan you can keep it. But for millions of Americans, that's not true.

He said that the law would make health insurance more affordable. But across the country, Americans are seeing their premiums go up, not down. And when launching HealthCare.gov, the Obama administration said that the website was safe, secure and open for business. We now know that isn't true either.

The data obtained by HealthCare.gov is one of the largest collections of personal information ever assembled. It links information between seven different federal agencies and state agencies and government contractors.

The website requires users to provide personal information like birth dates, social security numbers and household incomes in order to obtain information about potential health coverage. But security experts have expressed concern about flaws in the site that put this personal data at risk and subject users to the threat of identity theft.

The Science Committee oversees the agencies responsible for setting privacy and security policies and standards for the rest of the federal government—the White House Office of Science and Technology Policy and the National Institute for Standards and Technology.

The Obama administration has a responsibility to ensure that the personal and financial data collected by the government is secure. Unfortunately, in their haste to launch the HealthCare.gov website, it appears the administration cut corners that leaves the site open to hackers and other online criminals.

So the question for today's hearing is: Can Americans trust the federal government with their personal information on the HealthCare.gov website?

Today, we're going to hear from witnesses from outside the government who are experts in cybersecurity and hacking websites. Our witnesses will provide their professional assessment of the vulnerabilities that underlie HealthCare.gov.

Several vulnerabilities have already been identified, and we know of at least 16 attempts to hack into the system. And I heard this morning that there were another 50. But we can assume that many more security breaches have not been reported.

Here are some real-life examples. Mr. Thomas Dougall of South Carolina received a surprise phone call from a stranger one Friday evening explaining that he had just downloaded a letter off the HealthCare.gov website containing Dougall's personal information.

And when Lisa Martinson of Missouri called HealthCare.gov's customer service after forgetting her password, she was told three different people were given access to her account, address and social security number.

Also, it turns out that federal employees—called navigators—who help users apply for insurance on the HealthCare.gov website have not received background checks. Yet they are able to access the personal information of thousands of people.

Many Americans have been the victims of identity theft by computer hackers. Identity theft jeopardizes credit ratings and personal finances. The massive amount of personal information collected by the HealthCare.gov website creates a tempting target for scam artists.

These threats to Americans' well-being and financial security should make us question the future of Obamacare. Perhaps it is time to take Obamacare off of life-support.

Americans deserve a healthcare system that works and that they can trust. Obamacare is no cure.

Chairman SMITH. I now recognize the Ranking Member, the gentlewoman from Texas, Ms. Johnson, for her opening statement.

Ms. JOHNSON. Good morning, and thank you very much, Mr. Chairman. Let me welcome our witnesses. I look forward to your testimony today.

In light of the startup problems that have been reported with the HealthCare.gov website, problems that need to get fixed as quickly as possible, some Americans may be concerned about the security of their personal information on the website. I can understand such concerns, because anytime any of us go to the internet, we are vulnerable to those who would attack public and private databases to get access to our information. That said, we have not heard much about security failures at HealthCare.gov. There is one recorded instance where an individual was mistakenly given access to the records of another person. There were initially security issues with the password reset function. The site has also been attacked by hackers in a denial-of-service attack. However, my understanding is that these issues were quickly fixed and the cyber attack was successfully prevented.

The reality is that HealthCare.gov is subject to the same attacks as every other website and every other internet-accessible database. Every Member of this Committee knows that computer vulnerabilities are exploited every day at companies and government offices across the world, leading to the compromise of a wide range of personally sensitive information.

I would like to draw your attention to a graphic that tries to illustrate major security failures of computer systems resulting in personal information being compromised. It is on the screens. As you can see, some of the biggest and most experienced internet firms have suffered attacks, and often the personal information that is accessed goes well beyond identifying information to include credit card and sensitive financial information. Governmental institutions have also seen materials stolen.

Last year, Symantec's annual 2012 Cybercrime Report found that 556 million individuals in 24 countries, including the United States, were victims of one sort of consumer cyber crime or another. This equates to 1.5 million victims every day.

One might conclude that the only way to avoid being vulnerable to such attacks is to not be connected to the internet at all. However, in the 21st century, that is not a reasonable option for most government agencies, businesses or individuals. So, I think we have to be realistic about the ability of any internet-connected database to be completely invulnerable to being compromised. I also think we have to be honest about what information actually will be available to a cyber attacker through HealthCare.gov. In my work as a psychiatric nurse, I saw how patients' medical records were routinely accessed by large numbers of people every day. Several years ago my own electronic medical records were breached, and I received a letter from the UT Southwestern Medical School Hospital in Dallas telling me that.

So how vulnerable are medical records on HealthCare.gov? Some including two of the witnesses invited to testify today have made public claims that the website will have all kinds of sensitive personal medical records in its database. That is simply not true.

HealthCare.gov will not have patient or health care case information about anyone. HealthCare.gov will have the name, date of birth, Social Security number and address of participants, but that information is also potentially available through every insurance company, bank, credit card company and government agency that anyone deals with, and I have already pointed out the data breaches that have occurred and are occurring in these sectors of our economy.

So while there can be legitimate concerns about the privacy in the health care field, HealthCare.gov should not be the case of any exceptional fears in that regard. By saying that, I am not excusing the startup failures to implement the Affordable Care Act website in an effective way nor am I saying security failures are acceptable; they are not. I expect HHS will take every measure available to them to make the site secure and to maintain a high level of security going forward. However, I want everyone to keep the issues of security in perspective, and I hope that none of us will use this hearing to engage in fear-mongering in an effort to destroy participation in the Affordable Care Act. That would be irresponsible and, frankly, cruel. The Americans who most need the Affordable Care Act to work are those that are among the most vulnerable members of our society. Their personal medical data is not at risk on HealthCare.gov. In fact, it can be argued that this Committee's efforts to force sensitive information out of the EPA and Harvard and the American Cancer Society are a bigger threat to patients' privacy than HealthCare.gov.

In closing, I hope that today's hearing will not become a soapbox for growing fear and confusion. Let us stay focused on the facts.

With that, I again want to thank our witnesses and yield back the balance of my time. Thank you.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF RANKING MEMBER EDDIE BERNICE JOHNSON

Good morning, and welcome to our witnesses. I look forward to your testimony.

In light of the startup problems that have been reported with the HealthCare.gov website—problems that need to get fixed as quickly as possible—some Americans may be concerned about the security of their personal information on the website. I can understand such concerns, because anytime any of us go on the internet, we are vulnerable to those who would attack public and private databases to get access to our information.

That said, we have not heard much about security failures at HealthCare.gov. There is one recorded instance where an individual was mistakenly given access to the records of another person. There were initially security issues with the password reset function. The site has also been attacked by hackers in a "denial of service" attack. However, my understanding is that these issues were quickly fixed and the cyber-attack was successfully prevented.

The reality is that HealthCare.gov is subject to the same attacks as every other website and every other internet-accessible data base. Every Member of this Committee knows that computer vulnerabilities are exploited every day at companies and government offices across the world, leading to the compromise of a wide range of personally sensitive information.

I would like to draw your attention to a graphic that tries to illustrate major security failures of computer systems resulting in personal information being compromised.

As you can see, some of the biggest and most experienced internet firms have suffered attacks—and often the personal information that is accessed goes well beyond identifying information to include credit card and sensitive financial information. Governmental institutions have also seen materials stolen.

Last year, Symantec's annual 2012 Cybercrime Report, found that 556 million individuals in 24 countries, including the United States, were victims of one sort of consumer cybercrime or another. This equates to 1.5 million victims every day.

One might conclude that the only way to avoid being vulnerable to such attacks is to not be connected to the internet at all. However, in the 21st century that is not a reasonable option for most government agencies, businesses or individuals. So, I think we have to be realistic about the ability of any internet-connected database to be completely invulnerable to being compromised.

I also think we have to be honest about what information actually will be available to a cyber-attacker through HealthCare.gov. In my work as a psychiatric nurse I saw how patients' medical records were routinely accessed by large numbers of people every day. Several years ago my own electronic medical records were breached and I received a letter informing me about this from the hospital in Dallas.

So how vulnerable are our medical records on HealthCare.gov? Some, including two of the witnesses invited to testify today, have made public claims that the website will have all kinds of sensitive personal medical records in its database. That is simply not true.

HealthCare.gov will not have patient or healthcare case information about anyone. HealthCare.gov will have the name, date of birth, social security number and address of participants, but that information is also potentially available through every insurance company, bank, credit card company and government agency that anyone deals with, and I've already pointed out the data breaches that have occurred and are occurring in those sectors of our economy.

So while there can be legitimate concerns about privacy in the health care field, HealthCare.gov should not be the cause of any exceptional fears in that regard. By saying that, I am not excusing the startup failures to implement the ACA website in an effective way, nor am I saying security failures are acceptable. They are not. I expect HHS will take every measure available to them to make the site secure and to maintain a high level of security going forward. However, I want everyone to keep the issues of security in perspective, and I hope that none of us will use this hearing to engage in fear-mongering in an effort to destroy participation in the ACA. That would be irresponsible and, frankly, cruel. The Americans who most need the ACA to work are those that are among the most vulnerable members of our society.

Their personal medical data is not at risk on HealthCare.gov. In fact, it can be argued that this Committee's efforts to force sensitive information out of EPA, Harvard, and the American Cancer Society are a bigger threat to patient privacy than is HealthCare.gov.

In closing, I hope that today's hearing will not become a soap box for sowing fear and confusion. Let's stay focused on the facts.

With that, I again want to welcome our witnesses, and I yield back the balance of my time.

Chairman SMITH. Thank you.

Our first witness, Mr. Morgan Wright, is the Chief Executive Officer of Crowd Sourced Investigations, LLC. Mr. Wright is a former Kansas State Trooper, officer and detective with almost 18 years of service. He has also worked for the Department of Justice, the intelligence community, the Department of Homeland Security, and State Department. Mr. Wright has taught behavioral analysis interviewing at the National Security Agency. He holds degrees in human resource management and computer information systems from Friends University and is a 2011 graduate of the Executive Leadership and Management program at the University of Notre Dame.

Our second witness, Dr. Fred Chang, is the Bobby B. Lyle Endowed Centennial Distinguished Chair in Cybersecurity and Professor in the Department of Computer Science and Engineering at Southern Methodist University in Dallas, Texas. Dr. Chang brings us today over 30 years of public and private sector cybersecurity knowledge, serving as the Director of Research at the National Security Agency and then in an executive role at the SBC Commu-

nications. Dr. Chang is also a member of the Texas Cybersecurity Education and Economic Development Council, and he has taught at both the University of Texas in San Antonio and the University of Texas in Austin. Dr. Chang received his Bachelor's degree from the University of California-San Diego and his Master's and Ph.D. degrees from the University of Oregon.

Our third witness, Dr. Avi Rubin, is a Professor of Computer Science at Johns Hopkins University and is the Technical Director of their Information Security Institute. He is also President and Co-founder of Independent Security Evaluators, a computer security consulting company. Prior to joining the faculty at Johns Hopkins, Dr. Rubin worked in the Secure Systems Research Department at AT&T Labs Research. Dr. Rubin received his bachelor's, Master's and Ph.D. degrees from the University of Michigan.

Our final witness, Mr. David Kennedy, is the President and CEO of TrustedSEC, LLC. Previously Mr. Kennedy was a Chief Security Officer for a Fortune 1000 company located in over 77 countries with over 18,000 employees. Mr. Kennedy is considered a leader in the security field. He has spoken at many conferences worldwide including Blackhat, Defcon, INFOSEC World, and the Information Security Summit, among others. Mr. Kennedy is the creator of several widely popular open source tools and has coauthored a book on internet security that was number one on Amazon.gov for over six months. Prior to moving to the private sector, Mr. Kennedy worked for the National Security Agency and the United States Marines in cyber warfare and forensics analysis. Mr. Kennedy received his Bachelor's degree from Malone University.

We welcome you all, and Mr. Wright, if you will begin?

**TESTIMONY OF MR. MORGAN WRIGHT,
CHIEF EXECUTIVE OFFICER,
CROWD SOURCED INVESTIGATIONS, LLC**

Mr. WRIGHT. Thank you, Chairman Smith, Ranking Member Johnson and Members of the Committee, I am pleased to be here today. Thank you for allowing me to testify. Again, I am Morgan Wright.

During my testimony, I just want to cover four major areas that we want to provide a high-level overview to: end-to-end security testing, user account creation and registration, cyber squatting and domain name confusion, and the insider threat.

Just to set the stage, because we were talking about the size and scope of HealthCare.gov, it has been reported to have over 500 million lines of code. At the same time, Facebook, who has addressed similar privacy threats and issues, has less than 20 million lines of code running, 772 million daily active users, and 1.2 billion monthly users. So, when we start looking at this, we start looking at the complexities and interdependencies of the current government sites and the potential for disruption, compromise of security of identifiable information, frauds and scams, and I think one of the larger issues is the insider threat. This vast amount of code also means that it becomes very challenging from an industry standpoint and best practices standpoint to give a certification and assurance that the site is secure, especially as it relates to FISMA.

So, in the end-to-end security testing, I think one of the first major issues is the lack and the inability to conduct a complete end-to-end security assessment. Even when the contractors were here and testifying, they said it would take two months to complete this. It is essential when you are dealing with information that you have a top-down view, and in a system this complex, and having worked on major intelligence systems and the number of places we have to go out and touch data, you have to have that top-down view of security. It has to be something that is embedded in everything you do. There are five major types of data: voice, video, data, mobility, and then you apply security around that. That has to be put into it at the beginning.

A recent news article, in fact, on October 30th in the Washington Post stated that—and Ranking Member Johnson, I believe, brought this out—the security flaw with user name and password. The issue that it was not identified and rectified until three weeks after the site was launched is an indication of the lack of comprehensive security controls and awareness of one of the basic functions HealthCare.gov is designed to create, which is that experience, that user account, and the way you secure that is with your password.

There is a document here I would like to have put into the record a little bit later, but it came from Troy Trenkle, who was the CIO at that time of CMS. In the authorization to operate, one of the things he highlighted is that the Federal Facilitated Marketplace has an open high finding in terms of a security issue, but in the finding description, it says the threat and risk potential is limitless. These were the words from the authorization to operate, and the fix date, it is due May 31, 2014, is when this is required to be fixed. And then on the next page, on page 3, there is another finding, and it says it is a high finding but there is no finding description, it has all been redacted out, with a fix date of February 26, 2015. So just from an industry perspective, being on both the public side and the private sector side, there has to be some accountability from a security standpoint, if you go out and you say that the threat and risk potential is limitless. There is a lot of accountability in the private sector from shareholder lawsuits, civil litigation if information like that is found out. And from an industry perspective, it is contravention of what would be considered best practices from a security standpoint.

So the user account creation and registration, this was the second major issue because this is how people access the marketplace. I think one of the issues that caused some of the security concerns was the decision to move the submission of personally identifiable information before you could access the health care information, which meant that a user had to give, as was stated, name, date of birth, Social Security number, address and some other information in order to be able to see the plans. That creates an issue to where now—and I know David will talk about this a little bit later—is that when you start telling people the norm is to give your personally identifiable information, things that identify you before you are allowed to see the marketplace, it would be the equivalent of saying you can't go in and see a car on the car lot and kick the tires until you fill out a credit app and you are approved. This is not the way consumers do business but it creates the potential for fraud

because now you have established a norm for fraudulent sites and deceptive sites to say it is a norm that you give us your personally identifiable information first before we give you access to the rest of the information.

The third issue is about cyber squatting and domain name confusion, and why would this be an issue? As a former law enforcement officer, I can tell you it was tough enough as we started getting into technology to defend one site or do an investigation into one site. One of the articles that came out from the Washington Examiner quoted another cybersecurity expert who said that HealthCare.gov had 221 sites that were attempting to exploit it, and on the state exchanges, there were 499 sites. So from a purely law enforcement standpoint, you have given a lot of ground for people to use and establish the norm that you have to give your personally identifiable information first before you can access it.

And then the very last thing is the insider threat. If you were to assume that HealthCare.gov had reasonable security, it ran reasonably well and it was within acceptable limits, the fact that people who access this information and access the information from the consumers do not undergo at least a background check from a position of public trust, which is already established by OMB standard form 85-P—it is a limited background check to identify people with felonies or certain convictions that would prohibit you from having positions within the government. At least a similar background check like that would expose deficiencies and then you apply rigorous auditing and accounting to that to make sure that you learn from those lessons and prevent future issues. So when dealing with the insider threat, you have to remember, trust is not a control and hope is not a strategy. If anything, Edward Snowden has taught us that no matter how much trust you give somebody, things can still happen.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Wright follows:]

**Testimony of Morgan Wright, CEO, Crowd Sourced Investigations, LLC
Before the House Committee on Science, Space, and Technology**

November 19, 2013

Chairman Smith, Ranking Member Johnson, and members of the Committee:

Thank you for inviting me to testify before you today. I'm Morgan Wright, CEO of a startup called Crowd Sourced Investigations, LLC d/b/a ConnectedToTheCase.com. We are a no-cost resource for federal, state and local law enforcement that uses the power of social media and crowdsourcing to solve crime, return the missing and protect our children.

I am providing this written testimony pursuant to your invitation to testify. I will describe my professional career, my work with information and network security, my understanding of both the technical and human threats to Healthcare.gov, the privacy issues with the collection of personally identifiable information and my opinion of the issues facing the continued deployment of the site.

Analysis of Healthcare.gov: Threats, Vulnerabilities and Best Practices

It has been widely reported that Healthcare.gov has over 500 million lines of computer code. The number of daily unique visitors to the website since October 1, 2013 has trended down, reported to be no more than 500,000¹. Many visits resulted in a website that was not functional. In contrast, Facebook is reported to have less than 20 million lines of code with 727 million daily active users in September 2013. This is based on 1.2 billion monthly active users.²

The complexities and interdependencies of the current government site create significant opportunities for disruption of service, compromise of the security and

¹ <http://consumer.healthday.com/public-health-information-30/misc-insurance-news-424/website-contractor-to-lead->

² <http://newsroom.fb.com/Key-Facts>

privacy of personally identifiable information (PII), frauds and scams and insider threats. The vast amount of code also means applying industry-standard security practices, along with federally mandated Federal Information Management Security Information Act (FISMA) requirements, is a task that can have no real chance of success at present.

During my written testimony I will cover four major topics:

- End-To-End Security Testing
- User Account Creation and Registration
- Cybersquatting and Domain Name Confusion
- The Insider Threat

End-To-End Security Testing

The first major issue is the lack of, and inability to conduct, an end-to-end security test on the production system. The number of contractors and absence of an apparent overall security lead indicates no one was in possession of a comprehensive, top-down view of the full security posture.³ For a system dealing with what will be one of the largest collections of PII, and certain to be the target of malicious attacks and intrusions, the lack of a clearly defined and qualified security lead is inconsistent with accepted practices.

A recent article in the Washington Post stated that the “Healthcare.gov site had a glaring security flaw that wasn’t patched until last week.”⁴ This flaw dealt with the management of user names and passwords – a key component in protecting the privacy and security of PII. A private security researcher discovered the flaw, which according to the article “...would have allowed an attacker to take over a customer’s whole account in the insurance hub.” To have discovered this major deficiency after

³ <http://bigstory.ap.org/article/govt-document-health-site-posed-security-risk>

⁴ <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/30/healthcare-gov-had-a-glaring-security-flaw-that-wasnt-patched-until-last-week/>

launch only reinforces the conclusion that the site lacks both the proper security controls and comprehensive security test plan.

The GAO recently released a report on the changes to FISMA⁵ and the result of reviews of government agencies subject to FISMA. GAO noted a significant increase in security incidents (from 42,854 in 2011 to 48,562 in 2012), with security management weakness as the top deficiency in general control areas. The common recommendations from this report should have formed the basis of a starting point to ensure the most likely vulnerabilities were addressed, including protecting user names and passwords.

The lack of end-to-end testing was also documented in questioning by Rep. Mike Rogers of Secretary Kathleen Sebelius⁶ on October 30, 2013. Based on the testimony of Secretary Sebelius as to the process of applying almost daily hot fixes and patches, it would be highly unlikely that the required remediation can occur anytime soon. This information was documented in a memo⁷ from Tony Trenkle dated September 3, 2013. While the memo issues an Authorization To Operate (ATO), it does outline significant security issues on Page 2 of the Authorization Decision attachment. The 'Finding' column indicates the Federal Facilitated Marketplace (FFM) has an open high finding. Because the document is redacted, the only text readable under 'Finding Description' column says, "...the threat and risk potential is limitless." It gives until May 31, 2014 – eight months after the launch of Healthcare.gov – to fix the issue.

This is completely unacceptable from an industry perspective, and is in extreme contravention of security best practices. Only in the government could such a gaping hole be allowed to exist without fear of consequence. This shows a lack of understanding for the consequences to consumers and the protection of their PII. It

⁵ http://csrc.nist.gov/groups/SMA/isab/documents/minutes/2013-02/isab_feb2013_gaos-view-of-fisma_alawrence.pdf

⁶ <http://www.youtube.com/watch?v=y2-SeXEoaBU>

⁷ http://media.cmgdigital.com/shared/news/documents/2013/11/12/health_care_security.pdf

also creates massive opportunity for fraud, scams, deceptive trade practices, identity theft and more. Much of this is playing out right now.

User Account Creation and Registration

The second major issue was the decision to require users to create an account and register before being able to view available plans. This required consumers to provide PII before making a buying decision and is the polar opposite of how consumers buy in the private sector⁸. The lack of effective security controls, combined with the requirement to provide PII up front, has created the conditions for massive fraud and hacking.

This policy change created a series of cascading consequences guaranteeing that PII could not be secured. In addition, it meant that hackers and malicious actors could create fraudulent websites, scams and concoct deceptive practices because it was the 'norm' to provide PII up front. Visit any reputable online consumer site. The goal is to get users to create an account with the minimum amount of information needed, in order to provide an enjoyable experience. Consumers should not be held hostage to their PII.

Another outcome of changing the policy was the complexity in rewriting what was already an unsustainable amount of code and the impact on website efficiency. Had the policy remained to only provide PII when it was absolutely necessary to complete a financial transaction, it is quite probable many of the security issues would not have arisen.

A rule of thumb in addressing issues before a system goes live states that if it costs \$1 to fix the problem 'before' launch, it will cost \$100 to fix the same problem 'after' launch. Once real users and transactions are on the production system, the complexity to fix a problem is orders of magnitude greater. This has to do with all the

⁸ <http://www.forbes.com/sites/theapothecary/2013/10/14/obamacares-website-is-crashing-because-it-doesnt-want-you-to-know-health-plans-true-costs/>

additional effort, planning, contingency planning, resource allocation (including hardware, software and human capital) that must be accounted for in order to keep the system operational and functional.

With the policy change, the massive interdependencies between all the systems that must be checked before the user can log in means that if one critical system has an issue, it affects and can expose PII as an unintended consequence. This reflects an government approach to the consumer marketplace, and does not reflect the normal, best practices of the online consumer market space.

Cybersquatting and Domain Name Confusion

A third major issue is the registration of similar, misspelled or deceptive domain names, also known as cybersquatting. A recent article from the Washington Examiner⁹ quoted a cybersecurity expert who had identified 221 websites that appeared to exploit Healthcare.gov, and another 499 that also exploited the websites of state exchanges.

For example, when a consumer types in www.microsoft.com, they believe they will be visiting that site. To prevent confusion, and protect the relationship between the company and the consumer, Microsoft has also registered misspellings such as www.microsfot.com. Even if the consumer 'fat fingers' the typing of the domain, Microsoft has protected the trusted relationship and the possible financial transactions with the consumer.

The reason this is so important to manage from the beginning, and why it relates to web site security, is that consumers who mistakenly create an account on a deceptive site can expose themselves to identity theft and account takeover on the actual site they intended to register with. The other reason is for law enforcement and the eventual responsibility to investigate criminal activity.

⁹ <http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare.gov-state-exchanges/article/2537691>

With the 499 web sites at the state level, and 221 at the federal level, but not preempting the registration of domain names and preventing cybersquatting and associated activities, it becomes extremely challenging to investigate these cases with already limited resources. This means criminal activity has the opportunity to proliferate unabated for a significant amount of time. Unfortunately the government may become an unwitting accomplice to the most personal of crimes – identity theft.

In addition, the current Healthcare.gov site contains no information that is readily available or easily discoverable by consumers that educates and informs them about how to make sure they are engaging with an authenticated site and service. For example, financial institutions have gone to great lengths to educate their customers about how to spot phishing¹⁰ emails and prevent fraud. No such education material is present on Healthcare.gov.

The Insider Threat

If you were to assume that the security of Healthcare.gov was reasonable, that the functionality was within acceptable limits and fraudulent websites were at a minimum, the most troubling aspect would be the lack of a personnel policy that required background checks for individuals with access to PII or sensitive information systems.

During testimony on November 6th, 2013, Secretary Sebelius admitted that convicted felons could be hired as ‘Navigators’ and that no federal policy existed to require background checks. Currently, positions of public trust for the federal government require the completion of Standard Form 85P¹¹ (SF85P). At a minimum, the completion of the SF85P would identify those individuals who should be disqualified from accessing PII or sensitive information systems.

¹⁰ <http://www.consumer.ftc.gov/articles/0003-phishing>

¹¹ https://www.opm.gov/forms/pdf_fill/sf85p.pdf

When dealing with the insider threat, it must be understood that trust is not a control. The mere fact of a background check does not automatically ensure trust will endure. Aggressive auditing should be implemented to deter improper activity and identify procedural weaknesses that could contribute to misconduct, and continuous training should be delivered to the work force and monitored for satisfactory compliance.

Professional Background and Experience

My professional career includes over 17 years of service in state and local law enforcement as a city officer, state trooper and detective. During this time I developed expertise in behavioral analysis interviewing, interview and interrogation and the investigation and analysis of computer crime including internet investigations.

I have provided instruction on the investigation and analysis of computer crime to over 2000 federal, state and local law enforcement officers as a Board Member of the International Association of Computer Investigative Specialists (IACIS). I have been qualified as an expert witness and as a Certified Forensic Computer Examiner in federal and state court. In addition, I provided in-service training to the FBI Computer Analysis Response Team (CART) on the investigation of computer intrusions.

As an instructor in behavioral analysis interviewing I have trained federal, state and local law enforcement including a course at the National Security Agency to personnel conducting damage assessment from significant espionage cases. This blend of technology and behavioral experience has been an integral part of my career in understanding the application of security and privacy to information systems.

For the last 14 years, I have held positions in companies who specialized in systems integration, defense, intelligence, justice, consulting, advanced technology and broadband communications. I have degrees in Computer Information Systems and Human Resource Management.

In 1999 I was the Director of the Rapid Emergency Action Crisis Team (REACT) at Global Integrity Corporation, a subsidiary of SAIC. We created the model for sharing cyber threat data that became the framework for the Information Sharing Analysis Centers (ISAC's) established under Presidential Decision Directive 63. The first ISAC was developed for the financial services industry and went active in October 1999.

My team led the investigation and development of information indicating the probability of a massive denial of service attack back in February of 2000. We had been sharing this information with our financial services clients, and on February 7, 2000 I issued a press release which stated "DDOS attacks constitute one of the single greatest threats facing businesses involved in electronic and business-to-business commerce because an attack can completely shut down a Web site," said **Morgan Wright**, director of **Global REACT Services for Global Integrity**."

That same day, February 7th, the largest computer event ever known at that time – a full blown Distributed Denial of Service attacks (DDoS) - was in full force taking down Yahoo, CNN, eBay, Dell and Amazon. As a result, our company was asked to testify before a Subcommittee of The Committee on Appropriations, United States Senate¹².

In addition, my team also developed threat data on an impending event that became known as the "ILOVEYOU" virus. We had released information at 3:00 AM on May 4th, 2000 to our clients advising them of the probability of a significant computer event and provided guidance and potential countermeasures. The FBI did not release a similar warning until 11:00 AM the same day.

Again, our company was asked to testify¹³ about this event, this time before the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform, House of Representatives. The ILOVEYOU virus

¹² <http://www.gpo.gov/fdsys/pkg/CHRG-106shrg63940/html/CHRG-106shrg63940.htm>

¹³ <http://www.gpo.gov/fdsys/pkg/CHRG-106hhrg72361/html/CHRG-106hhrg72361.htm>

caused an estimated \$8 billion in damages and rendered the Department of Health and Human Services 'incapable of responding to a biological disaster'.

The work I directed with my team was the subject of over 17 separate Government Accounting Office (GAO) reports that highlighted the success of early threat identification and analysis. Of paramount importance were the privacy, safety and security of mission critical data.

I subsequently worked on complex information and intelligence sharing systems involving classified, sensitive but unclassified and unclassified information from 2001 to 2004. I provided the law enforcement and intelligence subject matter expertise for these programs, along with cybersecurity and privacy consulting. These programs included: Technology Exploration Development, Counterintelligence Field Activity, Joint Counterintelligence Group; Consolidation of The Terrorist Watch Lists, and; Concept of Operations – System of Services, Law Enforcement Information Sharing Program (LEISP), Department of Justice (now called OneDOJ).

During this time I became an instructor for the US State Department, Diplomatic Security Service, Antiterrorism Assistance Program. I delivered briefings called 'Unclassified Executive Seminar on Cyberterrorism' to organizations in Pakistan and Turkey. These briefings covered threats against critical infrastructure.

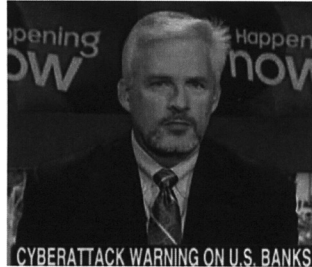
Beginning in 2004, I was the Global Industry Solutions Manager for Public Safety and Homeland Security at Cisco Systems. My responsibility was to deliver advanced technology solutions that utilized voice, video, data, mobility and security. Our portfolio included mission critical systems such as inbound 9-1-1, rapidly deployable emergency communications, law enforcement information and intelligence systems, government intelligence systems, critical infrastructure protection technologies and security and safety solutions.

A core tenet of our architectures for public safety was the inclusion and embedding of security. Based on thousands of government customers around the world at all levels, security was fine tuned to become an enabler of business and government and not an impediment.

In 2010 I took a position as Vice President of Global Public Safety, End To End Long Term Evolution (LTE) at Alcatel-Lucent. We were developing the broadband technology to be used under what is now called FirstNet. Working with my team and a team of distinguished engineers from Bell Labs, we addressed the creation of a national blueprint for this public safety network. The security and resilience of this network was core to the mission of deploying a nationwide solution.

In 2012 I served as the Senior Law Enforcement Advisor at the Republican National Convention for a consortium of companies that included Cisco, Raytheon and Nokia Siemens. We delivered a private broadband network to support the deployment of over 1,000 law enforcement and security forces. I provided the overall approach, concept of operations and mission requirements. Our design had security of the network, devices and applications as the primary requirement.

In our meetings with the US Secret Service and FBI, our group had to provide demonstrations of the technology to ensure we met the security requirements needed to support over 50 federal, military, state and local law enforcement agencies. We had to further ensure that no sensitive information or devices would be compromised even as we were the target of very technically advanced protesters.



Morgan Wright is the CEO of Crowd Sourced Investigations, LLC, d/b/a Connected To The Case. He is currently an analyst for Fox News Channel and Fox Business Network on issues of cyberterrorism and cybercrime, having provided analysis on major events such as the Elizabeth Smart kidnapping, the capture of Osama Bin Laden and the Flame Virus/Stuxnet Worm. Morgan's expertise was also sought out by CNN to review the technology aspects of the latest James Bond movie "Skyfall".

Previously Morgan was the Global Vice President for Public Safety 4G/LTE for Alcatel-Lucent, and was responsible for the development and market strategy for a \$1.7B addressable opportunity. Under his leadership, Alcatel-Lucent secured wins valued in excess of \$165M in the first 18 months, with several market 'firsts'. Morgan was also the Global Industry Solution Manager for Public Safety and Homeland Security at Cisco. Morgan received two Frost and Sullivan industry awards for Technology Leadership in Public Safety and Government Solution of the Year.

Prior to Cisco, Morgan held key technology and consulting leadership positions at BearingPoint, Unisys and SAIC on a variety of programs ranging from intelligence and information sharing to cybersecurity. Many of the programs achieved revenues in excess of \$500M.

Morgan's career also includes 17 years in state and local law enforcement as a highly decorated city officer, state trooper and detective. He is a member of the International Association of Chiefs of Police (IACP) Community Policing Section and most recently served as the Senior Advisor for Law Enforcement at the Republican National Convention. While serving in law enforcement, Morgan was awarded the Kanas Governor's Award for Valor, Gold Award for Valor, Attorney General Good Life Award, Gold Meritorious Service Award, Bronze Award of Valor, Bronze Award of Merit and the Meritorious Service Award. Morgan has also served as a member of the Board of Directors of several non-profits related to public safety and law enforcement.

Morgan has previously made appearances on CNN, ABC Nightline, PBS, NPR and over fifty various print media as an expert on cybercrime, cyberterrorism and computer intrusions. He is the author of two chapters in the 4th Edition Computer Security Handbook (Wiley and Sons) on 'Working With Law Enforcement' and 'Cyberspace Law and Computer Forensics'.

Morgan holds degrees in Computer Information Systems and Human Resource Management from Friends University and is a graduate of the Executive Leadership and Management Program, Mendoza College of Business, University of Notre Dame.

Chairman SMITH. Thank you, Mr. Wright. You got a lot into five minutes there.

Dr. Chang.

**TESTIMONY OF DR. FRED CHANG,
BOBBY B. LYLE CENTENNIAL
DISTINGUISHED CHAIR IN CYBER SECURITY,
SOUTHERN METHODIST UNIVERSITY**

Dr. CHANG. Chairman Smith, Ranking Member Johnson and Members of the Committee, thank you for the opportunity to testify before you today. As Chairman Smith mentioned, my name is Frederick R. Chang. I am the Bobby B. Lyle Centennial Distinguished Chair in Cybersecurity, Professor in the Computer Science and Engineering Department, and Senior Fellow in the Tower Center for Political Studies at SMU in Dallas, Texas.

On the backdrop of the 25th anniversary of the internet worm of 1988, which caused a major disruption on the internet in its day, let me start by saying that when considering the volume and sensitive data associated with HealthCare.gov, it would be unwise to underestimate the motivation, patience and creativity of today's cyber adversaries. They will find seams in the system. They will change the rules. They will attack you in ways that you won't expect, and I will return to this theme at the end of my oral comments.

In my written testimony, I pointed out three types of risk that I see, and I will describe these briefly now. In the near term, I think there is a large risk from bogus websites because there is not one single website for people to use, there will be confusion, and adversaries will take advantage of this confusion. I believe there will be people who will launch a search from a search engine and they will see many choices. I would invite you to try that, by the way. It is pretty instructive. Additionally, people will make typos when entering a web address, and this will lead them to the wrong site or they will receive spam emails taking advantage of the launch of the new Affordable Care Act. I read one report indicating that over 700 fake websites had been set within the first few weeks of the October 1st launch. If you combine that volume with the fact that people may be more likely than normal to enter sensitive information over the web because it has to do with health insurance coverage, you get especially concerned about the potential for loss of sensitive information. It is difficult to know how much traffic these bogus websites will siphon off from authentic websites, but I saw one estimate that was disturbingly high.

The second risk concerns the inherent risk in delivering applications over the web. There are a plethora of security risks facing any organization, public or private, as they contemplate delivery of an application over the web. The web was originally designed for the delivery of static read-only pages. Today, of course, we perform a wide array of interactive services over the web from buying books, videos and pet food to checking in for our airline flights and so much more. The convenience and business benefits are clear. It is really hard to imagine not using the web this way. Unfortunately, the convenience and benefits come at a price, and that price is security. The security risks constantly change and the top risks

have been well chronicled in the field. I did not do any form of security analysis myself personally on HealthCare.gov but I did read some posts where people had done some unobtrusive passive analysis, and concerns were raised, and I think David is going to have some more to say about that shortly.

The final risk that I mention in my written testimony was the risk from complexity. Many in the security field have noted that complexity is the enemy of security. As we ask for more and more functionality and capability from our software applications, the technologists and software developers are only happy to oblige. The result is more complexity including more defects and seams, and the attackers will try to exploit these. I am not an expert in health insurance exchanges but as I looked at the many sensitive back-end databases that are being accessed as a result of HealthCare.gov and thought about the many interactions, increased traffic load, the increased accesses, I believe that one can rightfully be concerned about the possibility of increased malevolent activity.

My wife asked me this weekend why haven't the hackers already launched the big one on HealthCare.gov. She thought that now might be the perfect time as the website was in startup mode. There was a hearing by the Homeland Security Committee chaired by Congressman McCaul in which it was reported that about 16 cyber attacks had been detected against HealthCare.gov. I don't have any detail on those attacks, but regarding my wife's question about the big one, I answered it the same way I mentioned in my opening remarks. It would be unwise to underestimate our adversaries in cyberspace. They are smart, they are creative. They will look for seams to exploit. They will change the rules, and importantly, they will be patient.

Thank you for your attention, and I look forward to your questions.

[The prepared statement of Dr. Chang follows:]

Written Testimony of

Dr. Frederick R. Chang

Bobby B. Lyle Centennial Distinguished Chair in Cyber Security

Southern Methodist University

Before the

Committee on Science, Space and Technology

U.S. House of Representatives

Hearing on

"Is Your Data on the Healthcare.gov Website Secure?"

November 19, 2013

Chairman Smith, Ranking Member Johnson, Members of the Committee, thank you for the opportunity to testify before you in today's hearing on the topic of data security and the new healthcare.gov website. My name is Frederick R. Chang and I consider it an honor and a privilege to come before this Committee again. I have very recently made a return to academia and I am now the Bobby B. Lyle Centennial Distinguished Chair in Cyber Security and Professor in the Department of Computer Science and Engineering at Southern Methodist University in Dallas, Texas. I am also a Senior Fellow in SMU's John G. Tower Center for Political Studies, an Adjunct Professor in the LBJ School for Public Affairs and a Distinguished Scholar in the Robert S. Strauss Center for International Security and Law at the University of Texas at Austin. In prior positions, I have served at the National Security Agency (as Director of Research); in academia (at

The University of Texas at San Antonio and at The University of Texas at Austin); and in the private sector (at 21CT, Inc., SBC Communications, Pacific Bell, and Bell Laboratories). I would also mention that I have served as a member of the CSIS Commission on Cybersecurity for the 44th Presidency and I am currently a member of the Texas Cybersecurity, Education, and Economic Development Council.

Regarding SMU, it is a nationally ranked private university in Dallas founded 100 years ago. The university enrolls nearly 11,000 students - including about 4,600 graduate students - who all benefit from the academic opportunities and international reach of seven degree-granting schools. SMU is recognized by the Carnegie Foundation as a university with "high research activity," which ranges across disciplines from particle physics at the Large Hadron Collider at CERN, to geothermal energy, to the science of human speed, to cyber security through the Bobby Lyle School of Engineering.

A brief historical observation

As we meet today to talk about Internet data security and healthcare.gov, I think it is an interesting coincidence that this hearing is being held in the same month that we observe the 25th anniversary of the Internet worm of November 1988 (also known as the Morris worm). It was the first worm to receive widespread media attention as it caused a major disruption on the Internet in its day. Today, our opponents in cyberspace are intelligent, seam-seeking, shape-shifting adversaries, that have an uncanny ability to penetrate and evade cyber defenses and compromise the targeted system. I am very pleased to be part of a discussion that will explore ideas that may serve to enhance the security of a web application that will be accessed by so many Americans.

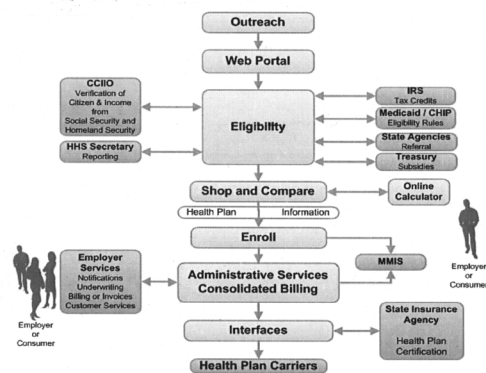
Complexity Risk

When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security. This is a point that has been made often about cybersecurity in a variety of contexts including, technology, coding and policy (1, 2, 3).

The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries.

This is a difficult dilemma. We want more functionality and capability in our software applications but the price we pay is added complexity which results in a corresponding increase in security vulnerabilities.

As I was preparing for this hearing, I came across a number of articles that commented on the size, functionality and complexity of what was being accomplished as part of healthcare.gov. I even came across a graphic from Xerox published in the Washington Post dated October 9, 2013 (4) and in the hope that a diagram is worth a thousand words, here it is:



In displaying this diagram, I don't intend to describe it, but rather use it to give a sense for the application's complexity. I would observe though that to get a quote for health insurance, the task of the "back end" software seems especially complex and challenging. As I understand it, the system needs to access servers and databases at the

Internal Revenue Service, Medicaid/Children's Health Insurance Program, various state agencies, Treasury, the Social Security Administration, the Department of Homeland Security, and Health and Human Services. It also needs to connect to all the health plan carriers to get pre-subsidy pricing. All this input is fed into the on-line calculator for display to the end user.

While we are on the subject of the back end, I would also make a point about the back end databases that are listed in the top half of the diagram. These databases obviously contain a tremendous amount of sensitive information and as a result would be attractive targets for attackers. The new services that are being introduced are

increasing the access channels into these sensitive databases and as a result the size of the “attack surface” has increased. I believe that this increased attack surface is a risk worth mentioning.

Web Applications Risk

Over the past many years we’ve all grown accustomed to conducting business over the web: buying books, videos, airline tickets and so much more. The convenience and business benefits of conducting transactions via applications that run over the web are clear. For some, it might be getting hard to remember a time when we didn’t use these web applications to conduct business. But with the convenience and benefits come security risks. The web was originally designed to display static, read-only pages, and as a result there was little intrinsic security. Some web security technologies were added later, and while things are improving somewhat, the majority of websites have security vulnerabilities today (5). We’ve known for some time now about the security risks associated with websites and indeed they have been analyzed, cataloged and rank ordered by an open-source, non-profit organization known as the Open Web Application Security Project (OWASP). For about the past decade or so they have been publishing the top 10 web application security risks and a 2013 list has recent been published (6). If you look through this reference you’ll read about items like: injection flaws, cross-site scripting, cross-site request forgery and more. Without going into the details, I’d just mention that these risks are of concern as they could lead to attackers querying or compromising the website with the goal of obtaining sensitive information.

I have not performed any analysis personally to determine whether these risks (and related risks) are present on the healthcare.gov website, but there have been some web posts based on unobtrusive, passive analysis that have raised some concerns along these lines (e.g., 7, 8). I understand that improvements to the website are on-going, so some of these concerns may have been addressed since they were reported.

Risk from bogus websites

The arrival of the new healthcare.gov website was accompanied by an array of fake websites that are designed to capture sensitive information that users enter into that fake website, believing that it is authentic. The information could then be used for purposes of identity theft. There was one report that mentioned that within the first few weeks of the introduction of healthcare.gov, over 700 fake websites had sprung up (9). I believe that this is a substantial threat vector, and others have observed this as well (10). Indeed, one need only to look at the results from fraudulent tax returns in the U.S. due to identity theft to conclude that considerable concern is warranted (11).

The fact that there is not one single place to sign up for health care coverage will lead to confusion by the public. There is the main federal site, individual state sites, as well as legitimate third party sites. As I understand it, there is no official designation or marking that a consumer can use to determine whether they are on the correct site or not. As people seek to register for health care coverage they may find that there are a dizzying array of websites to select from. When it comes to typing in information like a social security number into a web form, many people might be cautious about doing so, but given that it has to do with health insurance coverage people might be more inclined to do so (particularly if they think the request is coming from a legitimate website). These two factors could combine to create a ripe circumstance for personal information to get into the wrong hands. It is difficult to estimate how much traffic these fake websites will siphon off, but it could be significant (12).

A variant of the above scam would be for a bogus website to trick a user into downloading a piece of malware ("malware" is a catch-all term that refers to malicious software that may take the form of a virus, a worm, a trojan horse, a keylogger and the like). That malware could cause the user's computer to become part of a botnet or could capture keystrokes representing sensitive personal information leading to identity theft. A related variant would be that custom malware gets written specifically for the purpose of capturing information being entered into a health insurance exchange website, similar to what has happened in the context of on-line banking (e.g., Zeus malware).

Countermeasures

Ideally, security is built into an application from the very beginning rather than having it “bolted on” afterwards. Many in the security field have emphasized this point (e.g., 13). With the rise in cyber attacks, the “breach then fix” model is becoming untenable. Data breaches are harmful to its victims, time-consuming and costly to repair, damaging to enterprise reputation, and more. An application can’t be perfectly secure, but there are proactive things that can be done to reduce the risk of a successful attack. Let me mention a few such items here. Security should be integral to the application design (e.g., think like an attacker, secure the weakest link, fail securely). Security should be part of the software development lifecycle. Secure coding practices should be employed – in fact there are now published lists of top programming errors that coders make that lead to security problems (14). I previously mentioned the OWASP Top 10 Web Application Security Risks initiative and each of those risks are listed along with, among other things, secure coding countermeasures. Security penetration testing should be routine and continuous – before and after the system goes operational. Indeed I know of one company that uses a third-party service to conduct quarterly, unscheduled penetration tests after the application has been fielded, understanding that cyber adversaries will constantly adapt and modify their attacks.

As it relates to consumers, when the topic of “Internet security” comes up, it is easy to begin thinking about traditional technologies like network firewalls and anti-virus software. And while those technologies are certainly valuable and should be used, they won’t help much when it comes to most of the web application security risks that have been discussed. Regarding the risk of bogus websites, it is very important for consumers to understand that they need to be absolutely certain that they are accessing the correct health insurance exchange website. As I mentioned earlier, there are already many, many fake websites, and to the extent that users are confused about where to go, they may be lured to the wrong place. Users should start their search for coverage on the actual healthcare.gov website and not via a search engine.

Science of cybersecurity

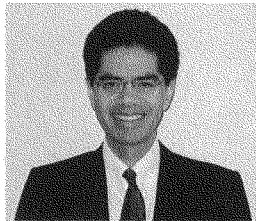
As I was preparing for today's hearing, I was reminded on a few occasions of my previous appearance before this Committee earlier this year on the topic of cybersecurity research and development. I spoke of the need for a science of cybersecurity. In our desire to move from reactively responding to cyber intrusions to proactively getting ahead of the problem we are limited by a lack of rich and reliable sources of data; solid, well-honed metrics; a deep research base providing understanding of the social science (e.g., economics, psychology) issues and consequences; laws or principles from which we can make reliable predictions about relevant cyber phenomena – and so much more. As we talk about important shorter term measures that can be taken to improve the security of healthcare.gov, there are myriad longer term issues that need to be addressed as well. At the beginning of my remarks, I mentioned Internet security issues dating back to 25 years ago. When it comes to cybersecurity, the problem is not going to go away anytime soon. Creating a cybersecurity science will be of critical importance to us in the long struggle ahead.

Thank you again for allowing me the opportunity to be here today. I look forward to your questions.

References

1. Schneier, B. (2000). Crypto-Gram Newsletter, March 15, 2000, Software Complexity and Security. <https://www.schneier.com/crypto-gram-0003.html#8>
2. McGraw, G. (2006). *Software Security: Building security in*. Addison Wesley, Boston, MA.
3. Geer, D.E. (2008). Complexity is the enemy. IEEE Security & Privacy, vol. 6 (6), pp. 88.
4. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/heres-everything-you-need-to-know-about-obamacares-error-plagued-web-sites/>
5. <http://www.darkreading.com/vulnerability/websites-harbor-fewer-flaws-but-most-hav/240154118>
6. https://www.owasp.org/index.php/Top_10_2013-Top_10
7. <http://blog.isthereaproblemhere.com/search/label/Healthcare.gov+Security>
8. <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Healthcare-gov-Affordable-Care-should-be-Secure-Care/ba-p/6227015>
9. <http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare-gov-state-exchanges/article/2537691>
10. <http://blog.trendmicro.com/coming-risk-scam-obamacare-sites/?sf17662278=1>
11. Anderson, R., et al (2012). *Measuring the cost of cybercrime*. In 11th Workshop on the Economics of Information Security, Berlin, Germany, June 2012.
12. <http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare-gov-state-exchanges/article/2537691>
13. G. McGraw, "Software security", IEEE Security & Privacy, vol. 2 (2), 2004, pp.80-83.
14. <http://www.sans.org/top25-software-errors/>

Frederick R. Chang – Brief Bio



Frederick R. Chang is the Bobby B. Lyle Endowed Centennial Distinguished Chair in Cyber Security and Professor in the Department of Computer Science and Engineering in SMU's Lyle School of Engineering. He is also a Senior Fellow in the John Goodwin Tower Center for Political Studies in SMU's Dedman College as well as a Distinguished Scholar in the Robert S. Strauss Center for International Security and Law at the University of Texas at Austin. He has been Professor

and AT&T Distinguished Chair in Infrastructure Assurance and Security at the University of Texas at San Antonio and he was at the University of Texas at Austin as an Associate Dean in the College of Natural Sciences and Director of the Center for Information Assurance and Security. He is the former Director of Research at the National Security Agency. In the private sector he was most recently the President and Chief Operating Officer of 21CT, Inc., an advanced intelligence analytics solutions company. Earlier, he was with SBC Communications where he held a variety of executive positions including, President - Technology Strategy, SBC Communications; President & CEO, SBC Technology Resources, Inc.; and Vice President, Network Engineering and Planning, SBC Advanced Solutions, Inc. He began his professional career at Bell Laboratories.

Dr. Chang has been awarded the National Security Agency Director's Distinguished Service Medal. He has served as a member of the Commission on Cyber Security for the 44th Presidency, and as a member of the Computer Science and Telecommunications Board of the National Academies. He is also a member of the Texas Cybersecurity, Education, and Economic Development Council. He received his B.A. degree from the University of California, San Diego and his M.A. and Ph.D. degrees from the University of Oregon. He has also completed the Program for Senior Executives at the Sloan School of Management at the Massachusetts Institute of Technology. He is the lead inventor on two U.S. patents (U.S. patent numbers 7272645 and 7633951) and he appeared in the televised National Geographic documentary, Inside the NSA: America's Cyber Secrets. He recently served as an expert witness at a hearing on cybersecurity research and development convened by the U.S. House of Representatives Committee on Science, Space and Technology -- subcommittees on Technology and Research.

Chairman SMITH. Thank you, Dr. Chang.
Dr. Rubin.

**TESTIMONY OF DR. AVI RUBIN,
DIRECTOR, HEALTH AND MEDICAL SECURITY
LABORATORY TECHNICAL DIRECTOR,
INFORMATION SECURITY INSTITUTE,
JOHNS HOPKINS UNIVERSITY (JHU)**

Dr. RUBIN. Chairman Smith, Ranking Member Johnson and Members of the Committee, good morning, and thank you for the opportunity to speak to you today. My name is Avi Rubin, and I am a Computer Science Professor at Johns Hopkins University. I am the Technical Director of the Johns Hopkins Information Security Institute, and I direct the Health and Medical Security Lab at Johns Hopkins.

I was asked to comment to you today on general security issues for large web installations and specifically about security issues that could affect a site such as HealthCare.gov. As we all know from reading the press, HealthCare.gov got off to a rocky start, and as a software engineer, it is not surprising to me that this happened. When we think about large systems and rolling out a large software system, the way this is typically done by companies such as Google and Amazon and other companies that roll out large software services, they roll it out in a small way to some controlled number of users. They identify bugs and problems with the system. They fix those. They get the system stable, and then they scale it up to a larger number of users. Once again they discover that now there are all kinds of new problems based on the bigger scale. Why would that be? Because of increased communication requirements, storage and what we might call race conditions that happen when you have a lot more users than you had before. And so then someone rolling out a large software package will roll it out to more users, get it stable and keep rolling it out. It is not very common to roll out a huge system with a ton of users on one day, and so it wasn't surprising to me that there were a lot of problems when this was initially rolled out.

Another thing is that when a project gets—a software project gets behind schedule, it is not very easy to recover from that. You might think well, just add more developers to it, but in software engineering, it is well understood that when you add additional programmers to a late software project, you often make it later. In HealthCare.gov, there are many interoperating components and links to many different systems including the IRS, the Social Security Administration, Department of Homeland Security, Experian, state exchanges and many more, and we know, as was stated earlier, that the more complex a system, the more vulnerabilities there will be, the more interfaces there are the greater likelihood of problems.

We also know, and it has been stated, that there are great risks to high-profile websites. We hear breaches reported in the major media all the time, and the attackers are growing in their creativity, sophistication, talent and resources. In fact, just last week

there was a report of a denial-of-service attack against HealthCare.gov.

Maintaining a secure website is not easy, especially if it manages sensitive information, if it requires ongoing maintenance, keeping up with vendor patches, requiring highly skilled administrators, reporting mechanisms for reporting incidents, contingency plans, and the list goes on. I provided a list, a longer list in my written testimony. And all of that said, the industry—the computer industry has many success stories. There are large, complex websites that have no major breaches that I know of. Examples of these are the airline reservation system, which manages a very complex array of interdependencies, and even other sites like Orbitz and Travelocity, which have to tap into those airline reservation systems. Large social sites—Facebook and LinkedIn—they got attacked all of the time and yet there hasn't been, to my knowledge, a major compromise of these top sites that in a wholesale manner exposed all the private information of the users. We have Amazon.com, a shopping site. And while no system is perfect, there are best practices in the industry that work well for the most part. In my written testimony, I provided a list of best practices and recommendations for the HealthCare.gov website. I don't have time in my oral testimony to go into them but to summarize what they are about, I suggest a few of the security annually by outside experts, focusing on the interfaces among the components and across systems, reviewing authentication mechanisms, checking for known standard vulnerabilities such as SQL injection attacks, sanitization of user inputs, cross-site scripting, and we have a long list of technical things to look for.

Data at rest should be encrypted, and the keys should be managed carefully just like all of those sites that I mentioned do. There should be mandatory incident reporting and contingency plans in place for every possible conceivable scenario. The list of recommendations that I have submitted is partial, but I believe that with the proper administration and the proper expertise, a website such as HealthCare.gov can be deployed in a practical manner.

Thank you for the opportunity to speak with you today, and I look forward to addressing your questions in the Q&A.

[The prepared statement of Dr. Rubin follows:]

Testimony before the US House Committee on Science, Space, and Technology.
November 19, 2013
Rayburn House Office Building, Room 2318
Aviel D. Rubin, Ph.D.

My name is Avi Rubin, and I am Professor of Computer Science at Johns Hopkins University and a former Fulbright Scholar. I am also Technical Director of the Information Security Institute and Director of the Health and Medical Security (HMS) Lab at Johns Hopkins. I have been working in IT Security since 1992, and my Ph.D. was in the area of network security and applied cryptography. Before coming to Johns Hopkins almost 11 years ago, I spent 9 years working in the Bell systems research labs on security issues including Web security, data privacy, and general IT security. I am author or co-author of five books on the subject.

I am currently advising six Ph.D. students and over a dozen undergraduates, and my lab is funded by the Office of the National Coordinator for health information technology and by the National Science Foundation. My grants target healthcare IT and electronic medical records security. My sponsored work does not relate in any way to the HealthCare.gov site or any other government system in production.

From 2005 to 2011 I ran a software security consulting company that evaluated the security of systems, including large Web deployments and backend databases.

I have been asked to comment on security issues for large Web installations in general, and to address, specifically, security issues that need to be considered for the HealthCare.gov Web site.

My understanding is that among other things, HealthCare.gov collects some sensitive information from users to assess their eligibility. The site communicates with databases held by the IRS, DHS, and SSA to verify eligibility for federal subsidies and with third-party non-governmental entities like Experian to verify patients' identities. HealthCare.gov does not collect nor store Electronic Medical Records, but it does collect whatever personal information is needed for enrollment. This information, in the wrong hands, could potentially be used for identity theft attacks.

There have been many highly publicized breaches of large online systems where credit card information, social security numbers, and user passwords have been exposed. Some of the more notable ones involved Heartland Payment Systems, TJ Maxx, and most recently Adobe. Rarely does a week go by without a major media story about a new data breach. Anytime valuable, sensitive information is managed through a user-facing Web interface, there is a risk of exposure, and attackers are constantly growing in sophistication, creativity and resources. As one of the largest and most complex undertakings in the online space, HealthCare.gov faces the same security challenges as other online sites such as airline reservation systems, online banks and retailers, and large social media sites.

It has been widely publicized that HealthCare.gov has had a rocky deployment. To a software engineer, this is not surprising. The system is very large, and it interoperates with many different Web sites and back end systems. The success of HealthCare.gov depends not only on the software and servers that run the front end of the site, but also on every one of the organizations with which it shares data on the back end. Furthermore, HealthCare.gov was deployed with a hard deadline for going live, and there were indications that the system was not ready, as the deadline approached.

When software systems run behind schedule, the temptation is to increase the manpower to try to catch up. However, it is a well-known mantra in software engineering that adding people to a late software project is likely to make it later. A famous book by the software pioneer Dr. Fred Brooks titled The Mythical Man-Month captures this idea, and is considered one of the all time classic books on the development and deployment of large software products. Once a project falls behind schedule, sticking to a hard deadline can result in a faulty system that is not properly tested. Furthermore, systems that may appear to work well in the lab, often fail when scaled up to a large number of users in the field. Stress testing a large-scale system requires simulating the actual environment in which the software will run when hundreds of thousands of users simultaneously access it. Such simulations often do not properly test the system under a realistic load.

The issue of scale is an important one. Most large, consumer-facing Web-based rollouts happen in phases. For example when Google introduces a new service, they initially offer it to a select group of users. As bugs are ironed out and problems are resolved, the new functionality is enabled for more users. It is an iterative process, and there are always issues to resolve. One of the biggest mistakes of HealthCare.gov was the decision to roll it out all on one day. That is not the way large systems go live in practice.

One of the basic principles of security is that a system's security is inversely proportional to its complexity; that is, the more complex a system is, the more numerous vulnerabilities in that system will be. In other words, "Keep it simple" is the best advice. When a system must be complex by its nature, such as is the case for HealthCare.gov, then a good way to address security in the design is to focus on well-defined interfaces among components. This is part of building in security from the beginning.

One cannot build a system and add security later any more than you can construct a building and then add the plumbing and duct work afterwards. That said, in practice, software systems evolve, and as a system changes, new security considerations arise. In practice, systems require some post-production "bolting on" of security features and retrofitting security solutions despite any efforts to build security in at the outset. Ongoing vigilance and response are needed to properly maintain a secure Web installation.

I have followed news reports of some security problems with HealthCare.gov. As far as I can tell, so far all of the security problems that have been publicized were easy to fix and have been remedied. Assessing whether there are any deep, architectural security flaws will require an in-depth design review by security specialists. In the meantime, I have several recommendations that I list at the end of this testimony on how to maximize the security of HealthCare.gov.

Maintaining a secure Web site is not easy and requires ongoing maintenance, administration and expertise. That said, there are many Web sites that operate successfully and which have not, to my knowledge, suffered any significant breaches. Given the large number of interoperating systems and the sensitivity of the data that it handles, I classify HealthCare.gov as a high-maintenance system from a security perspective. It cannot be deployed and left alone. High quality system administrators are needed to keep up with software patches from vendors, to respond to incidents, and to monitor the systems for suspicious incidents. A contingency plan should be developed for every conceivable incident, and a reporting system should be put in place so that responses can occur in a timely fashion.

I believe that if security best practices are adhered to, if the system was architected with proper security and well designed interfaces on the back end, and if my recommendations below are followed, that it is possible for a site with the objectives of HealthCare.gov to achieve the same level of security as some of the well-known popular Web sites that people use regularly on the Internet to shop, bank, book travel, keep up with their friends, and otherwise manage their lives. There will always be the potential for security incidents, but the risks can be minimized with proper design, management and administration.

Here are my recommendations for securing HealthCare.gov:

- Outside, independent experts should review the security of the system annually, including design review, code review and red team exercises
- Security reviews should focus on the interfaces among the components and across systems.
- User authentication mechanisms should be reviewed, and two-factor authentication should be employed wherever practical.
- Security reviews should check for known standard vulnerabilities such as SQL injection attacks, sanitization of user inputs, Cross Site Scripting vulnerabilities, and other standard checks.
- Data at rest should be encrypted, and keys should be cleared from memory when they are not in use.
- Implement mandatory incident reporting, even of suspected and unconfirmed incidents, and contingency plans should be designed for conceivable scenarios.

The opinions expressed herein are my own and do not necessarily reflect the views of The Johns Hopkins University. Thank you for the opportunity to testify before this committee, and I look forward to answering your questions.

Dr. Aviel D. Rubin

Dr. Aviel D. Rubin is Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins, Rubin was a research scientist at AT&T Labs. Rubin has testified before the U.S. House and Senate on multiple occasions, and he is author of several books including *Brave New Ballot* (Random House, 2006) *Firewalls and Internet Security*, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), *White-Hat Security Arsenal* (Addison Wesley, 2001), and *Web Security Sourcebook* (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is Associate Editor of *IEEE Transactions on Information Forensics and Security*, Associate Editor of *Communications of the ACM (CACM)*, and an Advisory Board member of Springer's *Information Security and Cryptography Book Series*. Dr. Rubin spent the 2010-2011 academic year as a Fulbright Scholar at Tel Aviv University. In January, 2004 *Baltimore Magazine* named Rubin a Baltimorean of the Year for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award. Rubin has a B.S. ('89), M.S.E ('91), and Ph.D. ('94) from the University of Michigan.

Chairman SMITH. Thank you, Dr. Rubin.
Mr. Kennedy.

**TESTIMONY OF MR. DAVID KENNEDY,
CHIEF EXECUTIVE OFFICER,
TRUSTEDSEC, LLC**

Mr. KENNEDY. Thank you, Mr. Chairman and Members of the Committee. I appreciate your time today.

Just to give you a brief background of my history, because I think it will parlay into the security issues that we identified with HealthCare.gov. We work with customers, large and small, everything from Fortune 10 to Fortune 500 or Fortune 1000 companies all the time, and we do security assessments where we basically break into computer sites all the time as hackers. So I am a hacker on the good side, a white-hat hacker, in those terms. So we break into websites all the time to identify risks and exposure. We do it for government sites, we do it for private sector sites all the time. And if you look at the security industry, it has evolved significantly over the past ten years. We didn't have dedicated security conferences, folks that are dedicated to protecting infrastructure and security. Technology has advanced so far and so fast that we are really trying to still grasp our hands around how to actually do it the right way, but there are things in place to do it the right way and to make it right, and so there are companies that have successfully deployed websites without any major security exposures. There are websites out there that aren't necessarily unhackable but they are very difficult to break into, and we are hackers who break into them all the time and it becomes very difficult for us. And the purpose of security isn't to say hey, we are 100 percent unpenetrable all the time but can we detect the hackers in the very early stages of their lifecycle of the attack, monitor that and prevent the attacks from happening, and none of those are clearly being done on the HealthCare.gov websites and all of its sub-websites themselves.

What we did—and again, this is purely from a reconnaissance perspective. We did not hack into the site in any way, shape or form. We are not authorized to hack into the website in any way, shape or form. But just by looking at the website, we can see that there is just fundamental security principles that are not being followed, things that are basic in nature that any security tester like my myself or anybody that we hire to test these sites would actually test for prior to it being released, and these are things that could actually compromise sensitive information for people that have registered for the website and actually compromise the entire site itself and everything around it.

One thing to also mention is that not only is there Social Security numbers and information in there that was mentioned but also there is tight integration into state exchanges, the IRS, DHS and third parties like Experian. So the infrastructure itself has trust factors to multiple different areas that it pulls and feeds information from, so not only is HealthCare.gov at risk but you also have the infrastructure that it was built off of that is at risk as well, which happens to be a lot of those different areas.

And so if you read the written testimony that I placed into there, I think we identified around 17 different direct exposures. A lot of those have been addressed. We reported them, and they have been addressed. Some of them have not been, and they have not been included in the report. We are very keen on what is called responsible disclosure and not putting anything at harm when we do these type of things, but there are critical flaws, there are critical exposures right now that are currently on the website that hackers could use to extract sensitive information. I am actually going to demonstrate one that has already been addressed and fixed and one that I cannot demonstrate because it would release sensitive information for U.S. citizens.

So I would like to flip to the actual screen here, and you can actually see the actual attack itself, and this attack and this actual demonstration I am going to show was actually shown from an independent researcher named Gillis Jones, who identified this exposure on `finder.HealthCare.gov`. I want to show you different things. There is multiple sites that support the infrastructure. You have `chat.HealthCare.gov`, `data.HealthCare.gov`, `finder.HealthCare.gov`. These are all components that make up everything that is `HealthCare.gov`. It pulls from different areas, different functionality, different features. They all make up what we consider `HealthCare.gov`. In this case here, if you notice on the right-hand side, and it is a little hard to see, but what we do here is, if we can send an email to anybody that is registered for the website and we can actually extract a lot of that information. As soon as they click this link, and you will see here, as soon as they click this link, it will automatically redirect them back to a malicious website where they actually hack the computer, and this website itself is legitimate. It is `finder.HealthCare.gov`. It is the website that folks go to. It looks legitimate. It is registered by the government. It is a federal government site. And as soon as somebody goes to this website and clicks on it, you notice here, we are going to go to that website and we are going to log in to it, and as soon as you log in to it, a banner pops up that looks just like `HealthCare.gov`. We get a little warning here that says `HealthCare.gov` enrollment. Now, for folks that have actually been on the website, you know that this isn't legitimate. This doesn't necessarily happen when it pops up like this. The individuals going to the website wouldn't know this. And as soon as they click "run," it actually hacks their entire computer. It escapes antivirus preventative technologies. It doesn't get detected by anything. And from there we can actually enable their web cam, monitor their web cam, listen to their microphone, steal passwords. Anything that they do on their computer, we now have full access to. And here I am on the hacker computer, and you can actually see—I can see the person's display here. You can see everything that is on it. You can actually monitor everything that person is doing, all the communications, and you can do this on a large scale because the information is readily available and the direct exposures that are actually on the website.

And one other thing I want to show you, and this is a sanitized version of this, which is, there was an exposure that we identified at TrustedSEC, and I am not going to say which website is in-

volved in it, but basically allows us to extract personal information of over 100,000 individuals including first name, last name, email addresses, their user account information as well as a lot of other additional information that we can fully extract from the website itself. I just want to show you an example, and this information has been sanitized as to not actually show individual people that have been exposed to this, but you notice here, you can see it up here. What we are going to do is we are going to track one record for someone that has actually registered for the site. Notice here, the first record that we pull back is actually an administrator for the website itself, so notice here, permission or administrator. Now I am going to extract the next 10 records in there. Now we have three admins, and then sanitized information of individuals that have registered for the website. So we can see here that we can extract over 100,000 individuals' information from the website itself.

And one last thing—I know I am running low on time here—is the talk that this attack has only happened 16 times and that the website has only been attacked 16 times is not possible. The attacks that happen on the internet are so frequently used and so frequently done that that means that there is not much detection capabilities on HealthCare.gov. And just as an example, this was recently posted yesterday. If I throw a semicolon into the search field, you can actually see the top results for the websites for semicolons, and those are all what we call SQL injection attacks, which means that hackers are continuously trying to find vulnerabilities in this, and the training program results on the website are actual attacks happening on the website itself. So the attacks that are happening are much larger scale right now. They are trying to infiltrate the website. They are trying to break into it, and there is definitely data on the website itself that is indicative of that.

I appreciate your time. Thank you very much.

[The prepared statement of Mr. Kennedy follows:]



Healthcare.gov Security Analysis –
Congressional Hearing November 19, 2013

Version 1.1 FINAL

TrustedSec, LLC
E: info@trustedsec.com
11565 Pearl Road
Suite 301
Strongsville, Ohio 44136
1.877.550.4728

Disclosure statement: Information contained in this report was obtained through passive analysis of readily available information. Under no circumstance did TrustedSec conduct any type of "hacking" efforts or attempt to exploit any weaknesses in the healthcare.gov website.

To Whom It May Concern,

November 18, 2013

TrustedSec performed an open-source analysis of the security around the healthcare.gov website. This report contains information regarding the concerns for the security around the website and the ability to keep United States citizen information protected to an adequate level. TrustedSec did not perform analysis through "hacking" techniques, as our organization was not authorized to perform offensive activities against the site.

Instead, TrustedSec utilized information readily available on the Internet as well as analysis of information presented back from the website to perform the assessment. What this analysis shows us is that as an attacker, there are known exposures in the healthcare.gov website today that could lead to significant compromise of the website and information. Additionally, the website is integrated into multiple agencies including some of the largest collections of United States citizen data – this includes the Internal Revenue Service (IRS) and other federal agencies.

Based on our evaluation of the website, we have serious concerns over the security of the website and the ability to protect information. This document will explain our approach, what was identified, and the future roadmap to ensuring that the website and its integration into multiple agencies can be successful and secure.

We appreciate the opportunity to present this information to government officials and look forward to our testimony on November 19, 2013.

Sincerely,



David Kennedy
CEO, Founder - **TrustedSec**
11565 Pearl Rd, Suite 301
Strongsville, OH 44136
E: INFO@TrustedSec.com



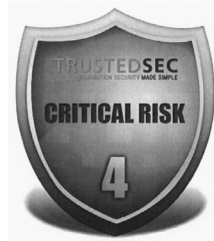
Table of Contents

1.0 EXECUTIVE SUMMARY	3
2.0 PUBLIC INFORMATION ANALYSIS	6
2.1 HEALTHCARE.GOV TARGETED ABOUT 16 TIMES	6
2.2 SECURITY WARNINGS IGNORED	7
2.3 PERSONAL INFORMATION DISCLOSURE	7
2.4 EMAIL ENUMERATION EXPOSURES	8
2.5 MULTIPLE EXPOSURES IDENTIFIED	8
2.6 OTHER USER INFORMATION EXPOSED	8
2.7 ADDITIONAL REFERENCE	8
3.0 ACTUAL ANALYSIS	9
3.1 UNDISCLOSED EXPOSURES	9
3.2 OPEN URL REDIRECTION	9
3.3 VULNERABILITY QUERY STRING XML OUTPUT (XML INJECTION)	9
3.4 TEST DOMAINS EXPOSED ON THE INTERNET	9
3.5 EXPOSED PROFILES	11
3.6 USERNAME ENUMERATION	13
3.7 PRIVACY SIGN OFF	14
3.8 EXPERIAN THIRD PARTY VERIFICATION	14
3.9 JQUERY FILE UPLOAD EXPOSED	14
3.10 HTML5 CROSS-ORIGIN SHARING	15
3.11 CKEDITOR (HAS BEEN REPORTED AND REMOVED)	15
3.12 ATTACKS HAPPENING FREQUENTLY	15
4.0 WEBSITE RECOMMENDATIONS	17
OPTION 1: VERSION 2.0 (HIGHLY RECOMMENDED)	17
OPTION 2: SHUT DOWN AND FIX	17
OPTION 3: FIX IN PRODUCTION	17
5.0 SECURITY RESEARCHERS	18
6.0 RISK CALCULATION METHODOLOGIES	19



1.0 Executive Summary

The Affordable Health Care Act was a sweeping change to the availability and affordability of health insurance for much of the United States population. The act provided a conduit for integration into multiple state-exchanges, as well as navigates citizens of the United States to different and competitive pricing. In order to support the integration process, the healthcare.gov website was created to provide a centralized approach and easy navigation to the general public. In order to meet the deadlines of the website, contractors were brought in to build and develop a customized solution to the website interface. Based on our research and the exposures identified, the healthcare.gov website is at critical risk for unauthorized access.



In traditional development lifecycles, websites are created formally with two major components (depending on methodologies i.e. waterfall, agile, etc.). A formal development process takes into consideration multiple teams and groups and merges them into one cohesive development process that integrates several areas. When a group of developers or several hundred developers work on something new, typically a framework is utilized (often referred to as a content-management system or CMS). This framework is used to ensure consistency while the logic on the background is developed in order to make the website work. In the case of the healthcare.gov website, two frameworks are utilized for content generation and the underlying framework. These are called Jekyll (<https://github.com/mojombo/jekyll>) and Bootstrap (<https://github.com/twbs/bootstrap>).

Frameworks provide a continuous way to have consistency and make the "look and feel" the same, however it does not actually create the functionality behind the website. This requires a formal development team to produce code in order to integrate into multiple federal and state departments as well as provide results to the end user based on the information provided. The website cost an estimated \$624 million and consists of over 500 million lines of code. With the number of lines of code, this is one of the most complex applications ever written in the history of applications. To put this in comparison, the Microsoft Windows 8 operating system, which is the latest, has an estimated 50 to 80 million lines of code and has over 25 years of development and maturity. It should be noted that with 80 million lines of code, the Windows operating system has had a significant amount of "exploits" that have hit their product line since its early existence. Additionally, the Linux Kernel which runs the most popular open-source distributions such as Ubuntu, Debian, Fedora, Redhat, etc. has roughly 15 million lines of code.

Microsoft has one of the largest and most sophisticated security development, protection, and remediation processes today. This process has taken years to mature and places security at the forefront. With a website that is over 6 times more complex than the Microsoft operating system and developed in an extremely short period of time, there is and was no foreseeable way to build security into the website. This is apparent based on our research and what exposures we as well

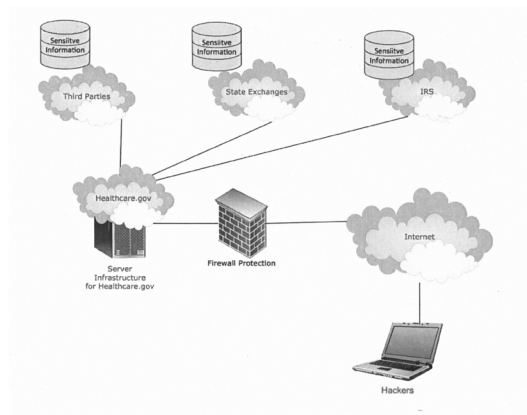


as other security researchers have uncovered since the website's initial release. Based on our findings, we are confident that the security around the application was not appropriately tested prior to release, that the safeguards to protect sensitive information are not in place, and that there are and will continue to be for a significant amount of time serious security concerns with the website unless direct action is taken to address these concerns.

Again, TrustedSec has not performed direct "hacking" on the website, however based on the information contained within this document and issues that you will see walking through the report, there are clear indicators that even basic security was not built into the healthcare.gov website. TrustedSec is confident based on the exposures identified that the website has critical risks associated with it and security concerns should be remediated immediately.

While TrustedSec may not have the full picture of the underlying technologies, based on the research identified and public information available about how the system integrates into other federal and state departments, there is serious cause for concern with the website.

In it's simplest form a website is the programming and the "logic" behind how a user interfaces with a website and how it behaves. Behind the scenes are databases, supporting infrastructure such as routers, switches, and other technology devices to make things work. The claim thus far on the healthcare.gov website is that there is no actual sensitive information stored on the actual webserver itself. This may be accurate however in order for the website to pull the information needed, it requires tight integration into multiple state and federal sites as well as third parties. In order for this to work, integration through other databases or web services is required. Following is an example of how this may work within the healthcare.gov infrastructure.



In the previous depiction, an attacker would circumvent the website and gain control of trusted connections between the healthcare.gov website, its databases, and ultimately the integration into all of the other areas. This is one of the most likely scenarios and major concerns for the current healthcare.gov website. If a vulnerability or exposure is identified on the website, it can directly impact the federal and state governments.

Also note that TrustedSec identified multiple severely critical exposures that it is not publishing publicly until they have been addressed.



2.0 Public Information Analysis

This section covers areas of public information that were disclosed through other researchers, or through information that has been made public since the launch of healthcare.gov.

2.1 Healthcare.gov Targeted About 16 times

Reference link: http://investigations.nbcnews.com/_news/2013/11/13/21440068-healthcaregov-targeted-about-16-times-by-cyberattacks-dhs-official-says

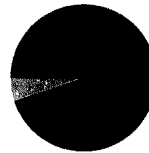
This is one the most alarming statistics released publicly. It's highly inaccurate and not probable for a publicly facing website with such high profile to only experience "about 16" attacks. What this statement shows is the lack of a formal detection and prevention capability within the website and it's infrastructure. This should be one of the most alarming pieces of information released to date as it shows that there is little to no visibility into what actual attacks are occurring on the website. This means that in the event that the website is hacked (or already has been), the attacks would go largely un-noticed and the website would remain compromised for a long period of time. On average, while working for an international Fortune 1000 company, our main website was attacked over 230 (averaged 232 attacks a day for the year of 2012) times a day with a much smaller footprint and profile, and less publicity than the healthcare.gov website.

Additionally, basic reconnaissance was performed on the healthcare.gov website, and it appears that there are little to no preventative measures in place to stop attackers from hitting the website continuously, nor detect attackers. The only precaution that appears to have been taken is the website does not allow browsing from The Onion Router (TOR) which masks traffic and locations over the Internet (privacy related).

Analysis on Attacks: TrustedSec has an open-source project called Artillery (<https://github.com/trustedsec/artillery> and <https://www.trustedsec.com/downloads/artillery/>), which actively monitors attack vectors geographically from all over the world. Even including websites that are not well known, the breakdown shows that websites are attacked roughly 32 times per day on average.

As an example, <https://www.trustedsec.com> received 46,689 known attacks in a one month timeframe:

Attack Count For All Sites		
Site Name	Attack Count	Percentage
www.trustedsec.com:443	44350	94.99 %
www.trustedsec.com	2335	5.00 %
trustedsec.com	4	0.01 %
Total count	46689	



Additionally, you can see the direct attacks as they occur and the heavy attack volume for a website that is purely dedicated to a specific industry:

Next event up	
Event details	
Server	15/11/2013
Date	
Server	01:41:40 GMT-5
Time	
Rule	Compromised/Hacked Servers \ Hackers use compromised servers for a variety of attacks, thus presenting a high risk to the application.
Category	
Matched Pattern	^1(28\,13 31\,157 32\,220 32\,232 34\,33 38\,121 38\,252 39\,81 41\,196 42\,105 43\,49 46\,100 46\,20 47\,11 48\,3 50\,112 52\,147 58\,73 59\,2 60\,122 68\,245 70\,67 92\,150\,240 92\,153\,43 92\,189\,206 92\,67\,16 92\,83\,107 96\,4\,167 98\,133\,130\,
Applied Policy	Redirect
IP Address	142.105.166.11
Port Number	443
Destination URL	https://www.trustedsec.com/
Request Method	GET
Site profile	Default Security Profile
Reference ID	a3c2-1942-0e02-0f68
Severity	0

Based on Internet statistics, it is evident that the website would be attacked significantly more based on pure Internet volume and not including targeted attacks.

2.2 Security Warnings Ignored

Reference Link: <http://www.pcworld.com/article/2063220/lawmakers-healthcaregov-security-warnings-came-before-launch.html>

One of the more alarming trends is that the actual security testing of the website was deferred due to project delays. The website was launched without formal testing and with known risks around the security of the applications. Even further, there was little to no security built into the website or through the development. With the complexity of the website, this would indicate that the website will suffer from significant security concerns for a long period of time unless significant action is taken to address the issues and flaws within it.

2.3 Personal Information Disclosure

Reference Link: <http://arstechnica.com/information-technology/2013/10/healthcare-gov-deferred-final-security-check-could-leak-personal-data/>

Recently, an exposure identified shared personal information with third party groups such as rum-collector.pingdom.net and doubleclick.net (statistical information).



2.4 Email Enumeration Exposures

Reference Link: <http://swampland.time.com/2013/10/28/exclusive-password-reset-security-glitch-fixed-on-healthcare-gov/>

In the referenced link, an email disclosure vulnerability was identified that would allow an attacker to enumerate email accounts for individuals. While this may seem minor, the ability to identify who has registered on the healthcare.gov website makes it significantly easier to target individual accounts and utilize social-engineering techniques to compromise the system. As an example, TrustedSec's CEO was on the Katie Couric show recently and showed how easy it was in under ten minutes to compromise someone online once the email address was exposed: <https://vimeo.com/77102165>.

2.5 Multiple Exposures Identified

Reference Link: <http://blog.isthereaproblemhere.com/2013/10/appalled.html>

The mentioned link shows multiple exposures identified including the ability to brute force user accounts through the error messages, reveal password reset codes without access to the actual account or email address, reveal email addresses, and reveal the security questions. These issues are prone to multiple areas of attack and show a lack of formal security practices around the website.

2.6 Other User Information Exposed

Reference Link: <http://blog.heritage.org/2013/11/02/exclusive-healthcare-gov-users-warn-of-security-risk-breach-of-privacy/>

User logged into the healthcare.gov website and saw information from a completely different person's profile (PDF document).

2.7 Additional Reference

<http://www.popularmechanics.com/technology/how-to/computer-security/can-healthcare-gov-keep-your-data-safe-16119563>
<http://apnews.myway.com/article/20131022/DA9JEPK81.htm>
<http://www.forbes.com/sites/theapothecary/2013/10/01/healthcare-gov-crashes-during-first-day-why-massachusetts-never-had-this-problem/>
<http://dailycaller.com/2013/11/13/hacking-tool-destroy-obamacare-poses-new-threat-to-health-care-website/>
<http://fedscoop.com/decoding-healthcare-gov-security/>
<http://blogs.wsj.com/digits/2013/11/11/chart-a-car-has-more-lines-of-code-than-vista/>



3.0 Actual Analysis

TrustedSec conducted analysis of the website and identified a number of exposures that could expose United States citizen's sensitive information or direct exposures that could actually lead to the compromise of the website. Note that several exposures were not posted publicly because they expose extremely sensitive information.

3.1 Undisclosed Exposures

Reference Link: Not disclosed.

TrustedSec has identified critical exposures for the healthcare.gov website as well as sub-sites which it cannot demonstrate at this time due to responsible disclosure principles and the possible impact of sensitive information disclosure.

3.2 Open URL Redirection

Reference Link (provided by independent security researcher [Gillis Jones](#)):
<http://finder.healthcare.gov/cms/sites/all/modules/ckeditor/link/proxy.php?url=http://example.com>

When clicking on the above link, users could visit the website thinking they were going to the legitimate healthcare.gov website but instead be redirected to a malicious website that would completely hack their computer.

3.3 Vulnerability Query String XML Output (XML Injection)

Reference Link: <https://spa.healthcare.gov/search-server/search?test='test'>

Within spa.healthcare.gov you have the ability to manipulate the response data to whatever you want by changing the query string parameter "test" to whatever you want. This means that an attacker has the ability to perform XML injection and have it directly reflect back onto the webpage and possibly execute.

3.4 Test Domains Exposed on the Internet

Reference Link: <https://test.healthcare.gov>

Test domains are exposed to the Internet, which is often an area for focus of attack. Additionally, there is a significant amount of test data already indexed all over the Internet.



site:healthcare.gov intext:"test"



Web Images Maps Shopping Blogs More Search tools

About 401 results (0.26 seconds)

Test Form | Data.HealthCare.gov

<https://data.healthcare.gov/dataset/Test-Form/ryf7-afr>

Nov 7, 2013 - Test Form. Based on. Based on Test Form. Expand. Subscribe to Changes; Share Alert. Yes; No. Based on Local Help (TEST). More Views1.

Local Help (TEST) | Data.HealthCare.gov

<https://data.healthcare.gov/dataset/Local-Help-TEST-/s2ws-5e6w>

Nov 7, 2013 - Permalink: [https://data.healthcare.gov/dataset/Local-Help-TEST-/s2ws- ... ?category=dataset&view_name=Local-Help-TEST-\(new window\)](https://data.healthcare.gov/dataset/Local-Help-TEST-/s2ws-...?category=dataset&view_name=Local-Help-TEST-(new%20window)).

Local Help Test | Data.HealthCare.gov

<https://data.healthcare.gov/dataset/Local-Help-Test/mt8-cmsa>

Nov 7, 2013 - HealthCare.gov Local Help Data. Organizations that can help you apply for health insurance.

Test Form | Data.HealthCare.gov

https://data.healthcare.gov/dataset/Test-Form/.../widget_preview?...

Test Form · Go to an accessible version of this page · Data.HealthCare.gov · Search · About this Dataset · Test Form · Full screen · Close. Author: Hiko Naito ...

Local Help (TEST) | Data.HealthCare.gov

https://data.healthcare.gov/dataset/...TEST-/.../widget_preview?...

Local Help (TEST) · Go to an accessible version of this page · Data.HealthCare.gov · Search · About this Dataset · Local Help (TEST) · Full screen · Close.

Addition screenshot here:



site:test.healthcare.gov



Web Images Maps Shopping More Search tools

2 results (0.16 seconds)

Google promotion

Try Google Webmaster Tools

www.google.com/webmasters/

Do you own **test.healthcare.gov**? Get indexing and ranking data from Google.

<https://search.test.healthcare.gov/>

A description for this result is not available because of this site's robots.txt – [learn more](#).

Individual Market-Dental Only - HealthCare.gov

<https://test.healthcare.gov/.../dental-plan-information-download.xlsx>

A, B, C, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, Instructions and Notes: 11, 12, 1) Overview of QHP Landscape files. 13, This website contains plan information for states in ...

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.

If you like, you can repeat the search with the omitted results included.

3.5 Exposed Profiles

Reference Link: Google -> site:healthcare.gov inurl:profile

It appears that individual user accounts and names are indexed via Google and can expose profile information of individuals that sign up on data.healthcare.gov.



[\[Redacted\] | Data.HealthCare.gov](#)
[https://data.healthcare.gov/profile/\[Redacted\]](https://data.healthcare.gov/profile/[Redacted]) ✓
 [Redacted] Joined on June 17, 2013 Last logged in November 11, 2013.
 Datasets. 1. Forms. 1. [Redacted]

[\[Redacted\] | Data.HealthCare.gov](#)
[https://data.healthcare.gov/profile/\[Redacted\]](https://data.healthcare.gov/profile/[Redacted])
 smith_ca. Joined on October 01, 2013 Last logged in October 01, 2013
 Followers (0). Following (1). [Redacted] Datasets ...

[\[Redacted\] | Data.HealthCare.gov](#)
[https://data.healthcare.gov/profile/\[Redacted\]](https://data.healthcare.gov/profile/[Redacted]) ▼
 Nov 7, 2013 - [Redacted] DataSlate Developer Intern, Socrata Washington, District of Columbia, United States. Joined on June 03, 2013 Last logged in ...

[\[Redacted\] | Data.HealthCare.gov](#)
[https://data.healthcare.gov/profile/\[Redacted\]](https://data.healthcare.gov/profile/[Redacted])
 10+ items - Skip to main content Skip to footer links. Hello, Unknown User ...
 2 RY2011 MLR Dataset 20121206 134,882 views.
 3 RR Submission Version Policy 116,306 views.

[\[Redacted\] | Data.HealthCare.gov](#)
[https://data.healthcare.gov/profile/\[Redacted\]](https://data.healthcare.gov/profile/[Redacted]) ▼
 New Mexico QHP Individual Market Dental Landscape 10-7-13. For instructions on how to read and use this data, please view the documentation available ...



3.6 Username Enumeration

Reference Link: <https://www.healthcare.gov>

When logging into the website, the website will let you know when an invalid username is specified and when an invalid password is specified. This will allow an attacker to enumerate userID's used in the website.

Invalid user:

What is your Marketplace username?

! Important: This is not a valid Username

Valid user:

Check your email!

We sent an email to the email address associated with your account with instructions on how to reset your password.

[RETURN TO LOG IN PAGE](#)

3.7 Privacy Sign off

Reference Link: <https://www.healthcare.gov/individual-privacy-act-statement/>

Information is shared with multiple third parties and other government agencies:

In order to verify and process applications, determine eligibility, and operate the Marketplace, we will need to share selected information that we receive outside of CMS, including to:

1. Other federal agencies, (such as the Internal Revenue Service, Social Security Administration and Department of Homeland Security), state agencies (such as Medicaid or CHIP) or local government agencies. We may use the information you provide in computer matching programs with any of these groups to make eligibility determinations, to verify continued eligibility for enrollment in a qualified health plan or Federal benefit programs, or to process appeals of eligibility determinations. Information provided by applicants won't be used for immigration enforcement purposes;
2. Other verification sources including consumer reporting agencies;
3. Employers identified on applications for eligibility determinations;
4. Applicants/enrollees, and authorized representatives of applicants/enrollees;
5. Agents, Brokers, and issuers of Qualified Health Plans, as applicable, who are certified by CMS who assist applicants/enrollees;
6. CMS contractors engaged to perform a function for the Marketplace; and
7. Anyone else as required by law or allowed under the Privacy Act System of Records Notice associated with this collection (CMS Health Insurance Exchanges System (HIX), CMS System No. 09-70-0560, as amended, 78 Federal Register, 8538, March 6, 2013, and 78 Federal Register, 32256, May 29, 2013).

3.8 Experian Third Party Verification

Reference Link: <http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/>

Verification information shared with Experian recently was identified in selling consumer information to ID theft services.

3.9 jQuery File Upload exposed

Reference Link: https://www.healthcare.gov/marketplace/global/en_US/js/jquery.fileupload.js

Upload forms are often an area for an attacker to upload malicious content and attempt to execute it or use it in social-engineering campaigns.



3.10 HTML5 Cross-Origin Sharing

Reference Link: <https://www.healthcare.gov>

For a detailed list of cross-origin sharing, refer to this link:
<https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity>

3.11 CKEDITOR (HAS BEEN REPORTED AND REMOVED)

Reference Link: Google -- site:healthcare.gov filetype:php (SINCE REMOVED)

CKEDITOR was installed on the ~~finder~~ healthcare.gov website which contains multiple vulnerabilities. This has since been removed.

<http://www.exploit-db.com/exploits/24530/>
<http://www.exploit-db.com/exploits/25493/>

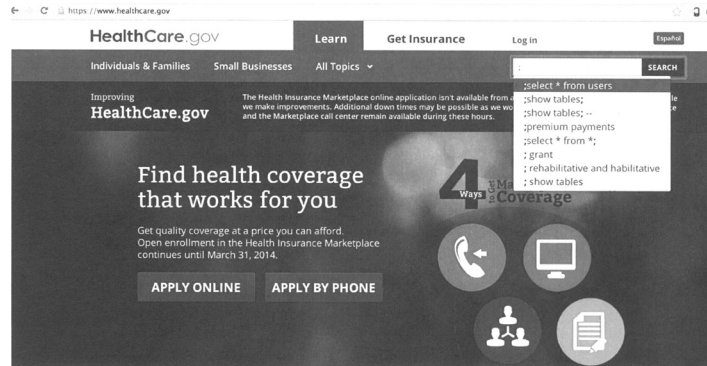


3.12 Attacks Happening Frequently

Reference Link: healthcare.gov

When throwing a ";" inside the search field for the healthcare.gov website, the search terms populate the most used terms for that specific match. In the field below, you can see multiple attempts for what is called "SQL Injection". This technique attempts to utilize a trusted database connection in order to execute malicious queries or code on the backend database. In this example in the screenshot below, the website is pulling related hits to SQL injection attempts on the website. This is indicative that attackers are going after the website and frequently.





4.0 Website Recommendations

Complex websites such as this are bound to have exposures and "glitches," however it appears based on the sheer number of exposures and the lack of formal testing around security that there are systemic and serious concerns with the healthcare.gov website. Based on our experience, in large web applications such as this, there are a few options available in order to address the security concerns with the website.

Option 1: Version 2.0 (Highly Recommended)

The website that is currently up is functioning in some capacity. The overly complex solution designed for the integration into state exchanges and other areas for real-time display of healthcare programs should be re-written from a code optimization standpoint. In something this complex, if design and code quality weren't created from the start, the fixes that we see now will only be small patches for a much larger problem. The first option would be to write a second healthcare.gov website in conjunction with what's currently up and running. This version "2.0" would be completely redesigned from the ground up with security and proper development processes established.

Option 2: Shut Down and Fix

If the website is shut down for the time being in order to address the situation, this may allow a more rapid response to addressing security concerns with the website. A "penetration test" which is apparently in process on the website is not recommended at this point. A full source code review and dynamic logic testing with use cases on the application should be considered for a more in-depth review. This will alleviate some of the major security issues but based on the complexity and size, the remediation process will span seven to twelve months at a minimum.

Option 3: Fix in Production

The term "production" refers to a site or application that is already up and running with normal user traffic. In this case, significant changes to a production environment need to undergo extensive testing before promotion from a QA/Dev/Test scenario. In a formal process, coding changes would occur, be tested in a formal setting in a non-production instance and then be promoted to production, or the "live site". This process definitely slows down the ability to introduce rapid fixes to the website as it could dramatically impact the end-user experience and functionality of the website.



5.0 Security Researchers

David Kennedy – Founder and CEO of TrustedSec (@HackingDave)

Scott White – Principal Security Consultant at TrustedSec (@s4squatch)

Alex Hamerstone – Practice Lead for Governance Risk and Compliance (@infosecdoc)

Gillis Jones – Independent Security Researcher (@Gillis57)



6.0 Risk Calculation Methodologies

During a technical review of an organization, basic criteria can be identified for the calculation of a risk that a specific vulnerability or exploit has to a company. TrustedSec utilizes the formula $\text{Risk} = (\text{Vulnerability} + \text{Threat}) * (\text{Impact} - \text{Countermeasures})$. There are several unknowns when calculating risk factors due to the likelihood of occurrence being a large uncertainty. TrustedSec cannot calculate likelihood due to many moving factors including discoverability, adversaries, timing, and opportunity.

TrustedSec can however calculate risk based on the vulnerability and how it could be utilized. Note that TrustedSec cannot calculate true impact due to not understanding the information available on all systems, the loss and damages, and the importance of the data to the company. TrustedSec can however calculate impact as it pertains to the impact it had towards the rest of the assessment and further compromising an organization.



David J. Kennedy
CISSP, OSCP, OSCE, GSEC, MCSE, ISO 27001
 Founder, Principal Security Consultant



David started TrustedSec with the vision in building a world-class information security consulting company. Prior to TrustedSec, David was a Chief Security Officer (CSO) for Diebold Incorporated, a Fortune 1000 company located in over 80 countries with over 16,000 employees. David developed a global security program that tackled all aspects of information security. David is considered a thought leader in the security field and has presented at over three hundred conferences worldwide. David has had guest appearances on FoxNews, CNN, Huffington Post, Bloomberg, BBC, and other high-profile media outlets. David is the founder of DerbyCon, a large-scale

information security conference.

David also authored Metasploit: The Penetration Testers Guide book, which was number one on Amazon in security for over a year. David was also one of the founding members of the "Penetration Testing Execution Standard (PTES)". PTES is the industry leading standard and guidelines around how penetration tests should be performed and methodologies. David has had the privilege to speak at some of the nations largest conferences including Blackhat, Defcon, RSA, ShmooCon, DerbyCon, INFOSEC World, ISACA, ISSA, Infragard, United Security Summit, INFOSEC Summit, Hack3rCon, BSIDES, and a number of other security related conferences.

David is the creator of several widely popular open-source tools including "The Social-Engineer Toolkit" (SET), Artillery, and Fast-Track. David has also released several zero-day exploits and focuses on security research. David has over 13 years of security experience, with over 8 specifically in security consulting. Prior to the private sector, David worked in the United States Marines for cyber warfare and forensics analysis activities. David was instrumental in Operation Iraqi Freedom (OIF) and developed a multi-million dollar classified system aimed at identifying potentially harmful insurgents and worked in a top-secret environment for several years.

Chairman SMITH. Thank you, Mr. Kennedy. I will recognize myself for five minutes to ask questions, and Mr. Wright, let me direct my first couple of questions to you.

Mr. WRIGHT. Yes, sir.

Chairman SMITH. The first is this. Does any other government website collect so much personal information as does HealthCare.gov?

Mr. WRIGHT. When you look at all the interdependencies like David laid out, when we looked around and obviously we are limited to what is in the open source, but there doesn't appear to be anything else that collects information and then uses that information then to check associated records in multiple other databases. So this becomes a central point of attack that if you can compromise one area, you can get into others.

Chairman SMITH. Okay. Next question is this. Is the fact that other websites can be hacked any justification for the lack of security with HealthCare.gov?

Mr. WRIGHT. What we would hope is that by learning from the known vulnerabilities out there and the other attacks that happen is that you would have guarded against this in the initial design to say we know this is going to happen, we know this is going to happen. The password issues and the issues David just showed are things that are so common, they should have been prevented against before the site was even launched.

Chairman SMITH. Okay. And on HealthCare.gov, do you think as a practical measure it can be fixed, or should we start over again?

Mr. WRIGHT. You know one of my examples, my neighbor helped build the Russian Embassy. I told him shame on you, the one that had all the bugs in it. It was easier and much safer to tear down the Embassy and start over again than it was to spend untold number of years and man-hours to remediate the problem, and that is just one issue. I mean, that is—you know, I am not a political person, we are not here to talk politics, but if you are asking from a technology standpoint, it would be easier to start over again, lay a foundation of security and start from the beginning because security has to be the foundation of this site, period.

Chairman SMITH. Thank you, Mr. Wright.

Mr. Kennedy, let me go to your last point, and I know you cannot confess to having hacked HealthCare.gov yourself, that would be illegal, so let me just ask you if you are confident that HealthCare.gov has been hacked and can be hacked?

Mr. KENNEDY. Mr. Chairman, I am very confident on the security ramifications that we can see, basic attacks that you could do at the website, that it is very susceptible to attack and that hackers could break into it. And just as an example, I got an email, a random email from somebody that I have never met before that had about 14 to 30 different exposures on the HealthCare.gov website that they were posting to me personally on my email saying that they had contacted individuals and that they hadn't had any responses back for these security exposures, and some of them are very critical in nature. So these are definitely happening. Hackers are definitely after it. If I had to guess based on what I can see, and again, this is purely from a reconnaissance perspective, I don't

have any understanding of the back-end infrastructure, but I would say that the website is either hacked already or will be soon.

Chairman SMITH. Okay. Thank you, Mr. Kennedy.

Let me address my last question to Mr. Kennedy, Dr. Chang and Mr. Wright, and it is this: what dangers do Americans face if there is a security breach with HealthCare.gov? In other words, if HealthCare.gov is hacked, what are the real-life threats, dangers to the American people who have provided that personal information? Mr. Kennedy?

Mr. KENNEDY. Well, if you look at the type of information that is stored, it is not only, you know, Social Security numbers and data, it is everything that integrates into the state exchanges, the IRS, DHS, multiple other areas. There are some large exposures for personal information being done, fraudulent-type activities being performed, but I think, you know, if you look at what this actually is, it is one of the largest collections of U.S.-based data, Social Security numbers and everything else, that we have ever seen in history. So for attackers, I would go after that personally if I was a bad guy to try to get that information for fraudulent activity, of if you have ever heard the term state-sponsored or other government agencies going after information based on U.S.-based citizens, and while there is no medical records specifically in the website itself, the integration into all the other sites that they have access to, you know, we use that as a trusted connection in term of hacking so getting access to that trusted infrastructure, that the sites trust themselves, allows us to access into that type of information.

Chairman SMITH. Okay. Thank you, Mr. Kennedy.

Dr. Chang?

Dr. CHANG. It is the general risk from identity theft. I don't know if you have talked to people who have had identity theft, it ends up being a major pain in the rear end to kind of get yourself out of that. So, extreme inconvenience and difficulty.

I would also mention that from the perspective of the U.S. government, once identity theft happens, a bunch of other bad things can happen. So if you look—I mention in my testimony about the loss from fraudulent tax returns so as people end up stealing identities, they start—they end up, you know, kind of doing fraudulent tax returns. In 2012, I think the number was something like in excess of \$3 billion loss in fraudulent tax returns, so it is just sort of an implication if identity theft.

Chairman SMITH. Okay. Thank you, Dr. Chang.

And Mr. Wright.

Mr. WRIGHT. This becomes the largest collection of personally identifiable information, and as a taxpayer and a consumer, I don't want my government becoming the unwitting accomplice in the largest disclosure of personally identifiable information. David's point is right, and Ranking Member Johnson, you expressed concerns about some of the medical records. It is not so much the medical records, it is the fact that once I can obtain your identity and I can now—medical insurance fraud is actually a very large growing area. I can actually go in and receive services. My issue as a consumer is that if my medical records get conflated with somebody else's and that I am now given a diagnosis or information that says I have something I don't have or I don't have something I do have,

that is one of my biggest concerns, and I think the threat—it is the threat of the unknown.

Chairman SMITH. Thank you, Mr. Wright, and thank you all, and the gentlewoman from Texas is recognized for her questions.

Ms. JOHNSON. Thank you very much, Mr. Chairman, and thank all of you for being here.

Mr. Kennedy, you mentioned that you were able to get 100,000 user names from a website but you did not mention which site that was. Was this the HealthCare.gov?

Mr. KENNEDY. It is part of the same infrastructure. Without disclosing—

Ms. JOHNSON. Excuse me. Was it a part of the HealthCare.gov?

Mr. KENNEDY. Yes.

Ms. JOHNSON. So you were able to get that information from HealthCare.gov?

Mr. KENNEDY. It is from the infrastructure from HealthCare.gov. It is from—if you look at what makes up HealthCare.gov, if you go to www.HealthCare.gov, that is one site and server. But what makes up HealthCare.gov is chat.HealthCare.gov, finder.HealthCare.gov, data.HealthCare.gov. There are multiple things that feed information into the main website. So you have all of these different working parts that feed into what makes up HealthCare.gov and that entire infrastructure, and that is what we found the exposure on.

Ms. JOHNSON. HealthCare.gov?

Mr. KENNEDY. On the infrastructure, on one of the sub-sites for HealthCare.gov.

Ms. JOHNSON. But not the site of HealthCare.gov?

Mr. KENNEDY. That is correct.

Ms. JOHNSON. Thank you.

Dr. Rubin, before—I mentioned earlier before I came to Congress I was a nurse, and in fact, I graduated from St. Mary's at the University of Notre Dame over 50 years ago, and my master's from SMU over 30 years ago. I went there because there was no school of first class in Texas that I could attend in nursing at that time. So that tells you how old I am, which I am very proud of.

But Dr. Rubin, what is your impression of the security in the health care industry? I have worked in the health care industry, and I have not found anybody seeking health care information to make a profit. Most of the time it is some scheme for people seeking information that they want to do that. In the Affordable Care Act, the preexisting conditions is no longer a factor, and so while I am not trying to make a judgment on the information, I am trying to understand why is there such an outcry at this point when medical records have been so available in any institution that I have worked in. Anyone who has any kind of hospital identification, whether it is a janitor or the nutritionist, a physician, a nurse can access a patient's chart that has everything on there that is going to happen or is happening to that patient while they are in the hospital, and that is something I know from personal experience. So I am trying to understand, is the health care industry lagging in these security measures or why—what is it about this non-security in the past is going to impact where we are now?

Dr. RUBIN. So to answer your question about where the health care industry stands with respect to security, I have done consulting in many different vertical industries—financial, all commercial—and in the last few years I have been working in the health care industry doing tours of hospitals and doctors' offices to assess their security, and I have found it is actually perhaps the most far behind in terms of the security at hospitals, even things in the emergency room that surprised me and the operating room. And so to your question, I think that the health care IT industry needs to learn a lot from some of the other industries in order to bring its security up to par.

Ms. JOHNSON. Thank you. Thank you, Mr. Chairman.

Chairman SMITH. Thank you, Ms. Johnson.

I would like to ask unanimous consent to put into the record a letter from the Identify Theft Resource Center, and they make the point, medical identity theft is one of the worst forms of identity theft for many reasons. For one, it is extremely attractive for identity thieves and hackers because the sale of medical identities is so lucrative. Second, medical identity theft is extremely difficult to mitigate, and lastly, medical identity theft is extremely dangerous. Without objection.

[The information appears in Appendix II]

Chairman SMITH. And then the gentleman from California, Mr. Rohrabacher, is recognized for his—

Ms. JOHNSON. Mr. Chairman, before you go to the gentleman—

Chairman SMITH. Before the gentleman from California is recognized, the gentleman from Texas, Ms. Johnson.

Ms. JOHNSON. Woman. I just wanted some clarification. Do they talk about the profitability sources in that letter?

Chairman SMITH. If you are asking about the letter that we just put in the record, I will give you a copy right there.

Ms. JOHNSON. Okay, because I am trying to figure out the value to anyone to access medical records, and I think this—did you say it spoke to it?

Chairman SMITH. Yes. The gentleman from California.

Mr. ROHRABACHER. Thank you very much, Mr. Chairman.

This has been a little bit overwhelming. Are you gentlemen saying that basically the American people are being put at risk by this incredible effort that our government is making in order to set up a health care system that will serve the people, that instead we are ending up putting them at risk?

Mr. WRIGHT. Let me take the first pass at that, sir. Back in February 7th of 2000, I was leading the computer emergency response team for SCIC, and we had financial services client, government clients. That date is significant because that was the first distributed denial-of-service attack ever launched nationwide. It took down Amazon, Yahoo, CNN. And one of the things we saw is, things don't happen on the first day. You have to build up the critical mass. The issue with HealthCare.gov is, you will not see the attacks in the first day as a detective. Nobody ever robbed a bank while it was being built. They wait until it was built, it had the money in there. What I am saying here is that yes, I mean, you are looking at the first 30, 45 days. That is not the issue. I am more concerned six months out at this information comes—

Mr. ROHRABACHER. We are predicting that the American people, unless there is a dramatic change in the way things are being put together, that families throughout this country will face huge problems, their bank accounts will be hacked into or maybe there will be false information put into their health care so if they go to the hospital, they won't get the right kind of medicine. Is this what we are talking about?

Mr. KENNEDY. I can kind of speak to that. From a security perspective, there are things that we can see that are patterns of inconsistencies around security, and if you could see those patterns and you look at those patterns, you can see that there is not a lot of security built into this site, at least from what we can see from a 10,000-foot view, again, without actually attacking the site itself. And there are things that we can do to prevent those, and if you look at how a website is supposed to be developed, it is supposed to be developed from the ground up with security integrated and being an integral part of that portion so you can protect sensitive data, U.S. citizen-based data, and it does not appear to be done, from what we can see and what we are finding as far as independent researchers and the information that is ready available out there.

Mr. ROHRABACHER. So when we are talking about hackers and you say you are a hacker, and we are talking about the American people being vulnerable, are we making the American people vulnerable to people, hackers from Russia or China or overseas?

Mr. KENNEDY. Absolutely. There is, you know, really different types if criteria of hackers. You have your hacker that you picture, you know, probably me 20 years ago in my basement, right, you know, hacking away or whatever. Then you have the criteria of more of organized crime, which is more on the monetary fraud perspective of just purely financial-type gain. And then you have obviously the state-sponsored element, which is more of like the folks that you see from governments of other areas, and they are looking for things like high-impact vulnerabilities so they can actually exploit a system, get access to the data behind it and use that information against us.

Mr. ROHRABACHER. But we are facilitating some of the worst scum in the world, not even in our own country, which we have enough problems of criminals in our own country, but the worst type of elements throughout the world to actually now get at our citizens?

Mr. KENNEDY. Objectively, we should have had a lot of defensive capabilities put into this site well ahead of it being released. There is technologies, there is detection capabilities, there is coding that we can do to make the site secure.

Mr. ROHRABACHER. And it should have happened before we—

Mr. WRIGHT. It should have happened well before it was ever released, and that is what you see in commercial areas.

Mr. ROHRABACHER. Let me—I only have one minute left. Someone said, one of you testified, it would be better right now, considering there is so much vulnerability that we now are putting our people in that it would be better to start all over again and just restructure the system from zero rather than trying to correct the problems that are in the system now because it was done wrong.

Do you all agree with that? Is that something that we have come to agreement here? Is there someone who disagrees with that?

Dr. RUBIN. Well, I can personally say that I haven't looked at the system carefully enough to make that judgment. I do think that we know as a computer industry how to build websites like this that can be more secure and meet the best practices, and I think that what would be necessary would be a security review of the system to establish whether there is a deep infrastructural problem with it or whether it is just—

Mr. ROHRABACHER. Okay. So you are not sure about that. The other witnesses would suggest that it would be better for us to start over with security in mind rather than trying to correct the problems in the current system. Is that correct?

Mr. KENNEDY. If you build a house, a foundation off of something that is flawed from the beginning, the foundation doesn't work, you know, the foundation sinks, it is crumbling, you can put a metal door on, you can bolt different things to make the house better but the foundation is still bad.

Mr. ROHRABACHER. So if we don't, Mr. Chairman, we are putting average American citizens, we are making them vulnerable to the worst godawful people in the whole world who are malevolent human beings who now don't have that access to our people. This is mind-boggling. Thank you very much, Mr. Chairman, for holding this hearing.

Chairman SMITH. Thank you, Mr. Rohrabacher.

The gentlewoman from Oregon, Ms. Bonamici.

Ms. BONAMICI. Thank you very much, Mr. Chairman and Ranking Member, for holding this hearing, and thank you so much to our witnesses for participating in the hearing.

Certainly since HealthCare.gov came on line, many of us have spoken with constituents who have had trouble navigating the site and some have expressed concerns of course about privacy on the site and further, I don't think there is a single Member who isn't somewhat frustrated about the problems that have plagued the rollout of the website and also the websites in some of our states. But frankly, the Affordable Care Act isn't about a website. I know I am not the only one who has spoken with just as many constituents whose biggest concern isn't the functioning of the website, it is the fact that they haven't been able to get health insurance or access health insurance or access health care, and in fact, right now they can go to get health insurance by calling or applying in person or by mail. The Affordable Care Act is designed to help these people who haven't had access to health care, and we should make that process as simple as possible, especially with regard to the website and make sure their personal information is protected.

I want to point out that right now in the United States, about 83-1/2 percent of Americans e-file their taxes. Do you all e-file your taxes? Yes, do you e-file your taxes? So you all e-file your taxes? You are among the 83-1/2 percent?

Mr. WRIGHT. I am sorry. That is—no offense, but what we do and how we do it only gives information to let people—we can neither confirm nor deny, and there is a reason the intelligence community says that because they don't want to tell people—

Ms. BONAMICI. Understood.

Mr. WRIGHT. —the threat vector that you can attack me on.

Ms. BONAMICI. Well, I understand, but I just want to clarify that a lot of people e-file their taxes.

So I want to also talk about the sort of conflation of electronic health records, which has been discussed here this morning, and certain detractors are suggesting that HealthCare.gov is sort of a clearinghouse that includes access to electronic medical records. So I want to get this from—let us start with Dr. Rubin. Does HealthCare.gov collect or store electronic medical records?

Dr. RUBIN. It is my understanding that it does not.

Ms. BONAMICI. Okay. And so let us talk a little bit about the Data Hub, because we have been talking about how through HealthCare.gov there is certain enrollment information that gets verified through Data Hub, so it is my understanding, and I would like, Dr. Rubin, confirmation of this, the Data Hub is not a database, it does not store information. Is that your understanding?

Dr. RUBIN. My understanding of what the Data Hub is, is that it is a queue of requests that are supposed to go out to different entities for information and so once a request gets processed, it is taken off of the queue and it is not stored.

Ms. BONAMICI. So the data is not stored. I just want to clarify that. It is used to verify information but not stored, it is not a database. It is also my understanding that it is not necessary to actually—consumers can still shop on the website without creating an account. It is my understanding that that was originally the case but now consumers can shop and look for plans and compare plans without creating an account first. Can somebody clarify that for me? Is that—has that been changed so that you do not have to—consumers do not have to set up an account?

Mr. WRIGHT. In my written testimony, one of the security issues was, is that they required you to give you personally identifiable information upfront and go through the registration process before you were given access to that information. However, a website called healthsherpa.com created by three gentlemen in two weeks did exactly what you were talking about, which should have been done is just puts in your age, your zip code and your sex and then you would be able to shop for plans based upon a range of options. But when I went through and started going through the process, it required you to, and to this day it requires you to give your information upfront.

Ms. BONAMICI. Okay. Well, we will clarify that.

I wanted to ask Dr. Chang a question and also because I want to give you an opportunity to say “Go ducks” like your colleague said. In the lead-up to this hearing, we have heard the reports about the attacks on the website, the distributed denial-of-service attacks. So how would you describe those attacks, and how might they compromise the functionality of HealthCare.gov?

Dr. CHANG. Go Ducks.

Ms. BONAMICI. Thank you.

Dr. CHANG. In the case of denial-of-service attacks, what that would amount to is that it would essentially be an attack on availability; people couldn’t access the site, they couldn’t gain access to it and do the business they want to perform. I guess I would mention sort of more generally as we talk about the fact that the web

is sort of this extremely powerful place, it is also sort of a dangerous place. I got some statistics out of 2012, and it basically talks about how 86 percent of websites have at least one serious vulnerability. The average website had 56 serious flaws. The organization only fixed 61 percent of these, and it took an average of 193 days. I mean, so basically we have this powerful capability in which we can launch all these sort of wonderful things but the downside is that this power results in some danger.

Ms. BONAMICI. And my time is expired, but I want to thank you for your expertise, all of you for being here today. It seems like there is a lot of places where people put in their Social Security number and it doesn't—yes, we need to fix things but that happens in a lot of places now. I yield back. Thank you, Mr. Chairman.

Chairman SMITH. Thank you, and the former Chairman of the Committee, the gentleman from Texas, Mr. Hall, is recognized.

Mr. HALL. I thank you, Mr. Chairman. I thank you for having such a capable Committee here, a group here, and I am really amazed as I read your backgrounds here, and I might ask Mr. Wright, when you were doing security work in Kansas, were you working under Governor Sebelius at that time?

Mr. WRIGHT. No, I was working under Governor John Carlin and then Governor Mike Hayden, who became, I think, a secretary of one of the agencies out here.

Mr. HALL. And Dr. Chang, I am going to have some questions to ask you in just a minute because I am a little closer to you. I am in Rockwall there, not too far from—come and get more information from you if you don't tell me what I want to hear from you. I graduated from there in law school years ago. Both my sons graduated from law school there, and I am amazed at SMU now, and I can't believe that Dave Kennedy being the CEO of all those places is a hacker light, I would call him something pretty capable. And might as well touch on Dr. Rubin too. When you say Johns Hopkins University, you are going to expect some class testimony. So Mr. Chairman, you and Eddie Bernice got together a good group for us here, and I think there is a lot of information there that we can look to. You have already talked pretty much about the house with no foundation, and I think you doubt that it can be patched up, and I thank you all for your testimony.

As we examine the security of the website, HealthCare.gov, or as we are finding out, the lack of security of this website is in its current form, would you agree that if a system is not only functioning—and that is my understanding from you. I think that was your testimony, was it not, that you have a bad basic for it. You have to go out and come in again, and that it is not functioning, and that is another thing wrong with the thrust of the health care that has been offered to the people.

So Dr. Chang, would you agree that if a system is not only not functioning properly, that it is also not secure from possible breaches and other cyber attacks, does that give you some anxiety?

Dr. CHANG. Yeah, it would. You know, in medical ethics, they use this term "do no harm."

Mr. HALL. Right.

Dr. CHANG. The exploit that David talked about is quite literally the website attacking the user. I mean, that is sort of the way to

think about it. And you know, as others have mentioned, it is really critical that security get built in from the very beginning. If you are trying to add lines of code to a software program on a sort of fundamentally unsound base, that is not good. So I think you are hearing some agreement among the folks around the table that security needs to be built in from the very beginning, and to the extent it is not, then that is—

Mr. HALL. Okay. How long do you think it would take to fix these problems and assure public confidence in the website?

Dr. CHANG. Pretty difficult to speculate. Maybe some of the other panelists—I would say it is maybe sort of a matter of months. I would be happy to—

Mr. WRIGHT. I think Donald Rumsfeld said it best when he talked about the levels of knowns. This is an unknown unknown. I mean, we don't know because there is no transparency. We have no information on the extent of the flaws. The information that is documented on the FISMA requirements in the authorization to operate have redacted information, so as practitioners, we actually are hamstrung to be able to give you our best advice because we don't have enough information to tell you we can give you a best guess but a best guess can't translate into a project plan in exact dollars.

Mr. HALL. And when you can't believe the information a President of the United States gives you, you don't want to say which time was he lying. I would rather say which time was he not telling the truth, and I think that is where we are going to come up with all these things that are breaking down now, and I regret that we are trying to give them opportunities to correct a bad bill, a bad health bill, with additional information. Ought to kill it and start all over again and fix the foundation.

Administrative officials have indicated that testing was performed on pieces of the website, just on pieces of it, but the entire website was not tested, and then how important, Dr. Chang, is testing prior to launching a website of this magnitude?

Dr. CHANG. Extremely important. As you heard from the others, this is what, you know, a professional website would do. They would do testing before, during and after. In fact, I am aware of one company in the private sector that conducts quarterly unscheduled penetration tests after the site has gone operational.

Mr. HALL. Do you think three years provides sufficient time? Just yes or no.

Dr. CHANG. What, for testing?

Mr. HALL. Yes.

Dr. CHANG. It seems reasonable.

Mr. KENNEDY. Sir, on the actual testing piece, you know, it is not a matter of testing it, you know, stopping the code, testing it, stopping the code, testing it. It should be built into the process. So the process itself continuously tests the security throughout the entire what we call the software development lifecycle, and then through there you have the security issues that are remediated prior to it. It doesn't hinder or stop any type of production, and a three year time period definitely should have been adequate enough to do the security testing to make sure that prior to any type of release, all those issues were vetted, and then from there you do what is called

penetration testing or hacking into the site to make sure that you didn't miss anything important.

Mr. HALL. I thank you. My time is up. I may want to inquire by mail to the four of you on some of these things. Thank you, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Hall. The gentleman from Massachusetts, Mr. Kennedy, is recognized for his questions.

Mr. KENNEDY OF MASSACHUSETTS. Thank you, Mr. Chairman. I want to thank the Ranking Member as well for holding the hearing, and thank each of our witnesses for your testimony.

Just want to echo my colleague's comments and say from somebody from Massachusetts, obviously where we—coming from a state that has gone through some of these challenges but a state that now has nearly 100 percent of all adults covered—or excuse me, 100 percent of all children covered, 98 percent of all adults covered, where our rate of cost increase for the overall health care system is right in line with our gross state product, that for the risk pools for individuals and for small businesses is about 1.8 percent, at least current data for the year upcoming. Contrast that to about ten percent what it was a decade ago. I think that Massachusetts has proudly evidenced that if there is a collective will to get health care, meaningful health care reform bill passed and to continue to work on it, to continue to tweak it to make sure it works together, it can be successful. And to the extent that I am hearing from my colleagues today a new refrain of rather than just repeal but actually repeal and replace, I think we are finally actually getting somewhere. So thank you.

With regards to the actual website itself, and unquestionably needs for improvement, and I want to thank the witnesses for highlighting some of them, I did have a couple of basic questions. First off, is it—Mr. Wright, is it clear that you can actually get estimates about how much you are going to pay for health insurance without having to put in any sort of personal identifying information?

Mr. WRIGHT. On the healthsherpa.com site, which has taken it directly from the government site, yes, but when I went through and tried it myself to get to the point to see how much information it would require, I couldn't get to that point without disclosing all of my information first.

Mr. KENNEDY OF MASSACHUSETTS. So would it surprise you to know that in the past 5 minutes, I could log on to the HealthCare.gov website, put in an exchange, put in a county, put in no other identifying information other than age bracket for me and whether I wanted coverage for myself or my spouse and click through and get an estimate of various costs?

Mr. WRIGHT. No, it wouldn't surprise me. In fact, I am glad that they did it because it means that they learned from the gentleman who created healthsherpa.com.

Mr. KENNEDY OF MASSACHUSETTS. Do you actually know who they learned from?

Mr. WRIGHT. No. That is the ones who originally did it, that showed that model how it should be done.

Mr. KENNEDY OF MASSACHUSETTS. Okay. So—

Mr. WRIGHT. But I am glad that they did it.

Mr. KENNEDY OF MASSACHUSETTS. Well, me too. Now, sir, your testimony—and I take it from the chairman that the focus of the testimony today in the hearing was, can Americans trust government with the information on the HealthCare.gov website, and Mr. Wright, the testimony that you offered basically broke it down into four categories: the end-to-end security testing, the user account creation and registration, the cyber squatting domain name confusion, and insider threat. Is that right, those four broad categories?

Mr. WRIGHT. Yes.

Mr. KENNEDY OF MASSACHUSETTS. And so the end-to-end security testing, those were the overall basic security issues that we have—that many of the people on the panel and you yourself talked about today, that every major website or most major websites come under attack for cybersecurity threats. Is that right?

Mr. WRIGHT. Well, the need for end-to-end testing, yes, and every site is—you must assume every site is under attack.

Mr. KENNEDY OF MASSACHUSETTS. Yes. Fair enough. That user account creation and registration, if my understanding of your testimony is correct is that your concern there is that it creates a new norm that could be exploited by other websites not pertaining to HealthCare.gov.

Mr. WRIGHT. When it was originally done and they required you to give you personally identifiable information upfront, that created a new norm that people would use then to exploit to say you must—this is the way we do it.

Mr. KENNEDY OF MASSACHUSETTS. Because so many people are accessing health care and have signed up for HealthCare.gov that that many people has now created a new norm?

Mr. WRIGHT. I am not sure exactly your point.

Mr. KENNEDY OF MASSACHUSETTS. Well, how do you create the new norm by—

Mr. WRIGHT. You establish the new normal by saying this is the way we do it. I mean, it could be one people that have registered or 50 but at some point if the government says the speed limit is now 65, that doesn't mean everybody starts traveling 65, but that starts becoming the new norm that you start enforcing against.

Mr. KENNEDY OF MASSACHUSETTS. Okay. And we have see that proliferate across—you have seen that now proliferate across other websites and other domains, other user forums? If it is a new norm, that norm is something that now spreads, right?

Mr. WRIGHT. Well, if it is a new norm, what you do is, people who create deceptive websites, or what David was showing, is because you are used to doing that because it has been said that you do that on HealthCare.gov—

Mr. KENNEDY OF MASSACHUSETTS. Have you seen that yet, sir?

Mr. WRIGHT. Yeah, actually what David just showed.

Mr. KENNEDY OF MASSACHUSETTS. Now, have you seen that spread across—if it is a norm, that becomes the norm, right? Have we seen that?

Mr. WRIGHT. I think we are probably getting into semantics, and I apologize, sir. I didn't mean to do that. When I said it starts becoming the new norm is, you start setting a standard and people start doing it. Everything starts out with a low level of adoption, then you get critical mass, and if they change it and they do that,

you can actually prevent the fraud, which is a good thing, because you reestablish what the norm should be, not that you should give personally identifiable information upfront.

Mr. KENNEDY OF MASSACHUSETTS. And I am just going to — I know I am running close over time. Thank you for clarifying, sir.

The last piece that I just want to touch on, I don't know if any of you—and I don't want to put anybody on the spot here but applications for a passport where you have to submit—or it asks for information including identifying information, proof of citizenship, proof of identity off a website. We haven't had any hearings based on the confidentiality or security of those issues. Is that—have any of you investigated other government website about the use of and the safety of classified—or of confidential material?

Mr. KENNEDY. And I can talk to that. One of the examples earlier was around the e-filing system. I have actually done security testing around the e-filing application part, and they have had security embedded into that at a very different type of level. There is actually state laws around the protection around what you have to do around Social Security numbers, and in the private sector there is what is called HIPAA around protecting against, you know, patient health care information. So there are laws and regulations around the protections of those, and I have done actual security testing on those in the past and they have done pretty well.

Mr. KENNEDY OF MASSACHUSETTS. And you think HIPAA—but we heard a lot of concerns about confidential patient information and the mix-up of electronic medical records—or electronic medical records, HIPAA.

Mr. KENNEDY. So there is a difference between compliance and what we call proactive security. Compliance doesn't mean security in any way shape or form but what HIPAA was designed to do was to put protections in place around patient health care information, or PHI, and while that is not necessarily successful across 100 percent of the board, I have run into some outstanding medical institutions that have very good security to protect patient health care information and take it very seriously, just a matter of negligence versus folks that go on the proactive side to actually fix the issues that they identify.

Chairman SMITH. Thank you, Mr. Kennedy.

Mr. KENNEDY. Mr. Chairman, thank you for the extra time.

Chairman SMITH. The gentleman from Texas, Mr. Neugebauer.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

I think we need to make sure we are clear here because even when people call in to HealthCare.gov, they are talking to individuals, but they are putting that data into the very same system that the web page is putting that and so basically all of that data is going into a central repository, and a number of these people that are helping put this data into the system are referred to as, I believe, navigators, and I think Ms. Sebelius stated in a recent hearing that these people do not undergo a federal background check, and Dr. Chang, as someone that was once the Director of Research at NSA, what are some of the risks of allowing people that have not had background checks run on them to have access to this kind of data?

Dr. CHANG. Yeah, so you would basically be worried about the issues of identity theft. I once went to a restaurant and gave the server my credit card. They wrote down my credit card and racked up some charges. So the worry would be to the extent that these folks that haven't had background checks—and honestly, I don't know how severe the backgrounds might be but if they haven't had background checks, who knows what they could do with the information. It is valuable information, there is a lot of it, and, you know, maybe they could do malevolent things.

Mr. NEUGEBAUER. Mr. Wright, do you want to comment on that?

Mr. WRIGHT. Yes, sir. I actually conducted behavior analysis training at the National Security Agency. We had the damage assessments agents in from significant espionage cases like Earl Edwin Pitts from the FBI, Aldridge Ames and Nicholson from the CIA, and one thing over and over again was, you can do a background check, you can give a high level of trust, and it still doesn't mean, as we know from Robert Hanson, for example, people still don't turn bad, but from my experience and training and when we have gone and looked at the fact that you don't do at least a cursory background check and eliminate the obvious threats from the beginning means that convicted felons, people with other—you would no more want a convicted felon than somebody with a conviction for child pornography having access to certain government systems. There is the SF-85-P from OMB establishes at least a baseline of information you can use to weed out candidates who should be disqualified from holding a position of public trust. The question is, would you define a navigator from a policy standpoint as a position of public trust, and if you do, the procedures are already in place to assess those backgrounds.

Mr. NEUGEBAUER. Mr. Wright, when I was reading your testimony, and I think you alluded to in your oral testimony, about the fact that the HealthCare.gov has over five million lines of code—

Mr. WRIGHT. Five hundred million.

Mr. NEUGEBAUER. Five hundred million? Yeah, it's even worse than stated. And that the Windows has 50 or 80 million lines of code, I think one of the questions that I have is also about security, but the American taxpayers, I think are going to pay like \$680 million for the system, or that is what is reported. So the question is, you know, we have got a lot of e-commerce sites out there that have been in place for a very long period of time, why would the government choose to try to build something from scratch that already is pretty readily available out there? Is there something about the way that HealthCare.gov operates that is different from the rest of the world operates or should be different from the rest of the world?

Mr. WRIGHT. Yes, there is, and it is the issue of accountability. If you are in the private sector and you have shareholders and you screw up, you are gone. I mean, there is accountability. There is also exposure to civil litigation. I can tell you, I worked at Cisco for six years, great company. We worked with a lot of countries and places. But the legal ramifications of doing something wrong went up and down the chain of command. Here you don't have the same. The government has a lot of immunity from liability. It should have gone out to the private sector to do this because what you

have done — my example was, can you imagine if the government put out a request for proposal to build Facebook, what that would look like. Facebook was built with 20 million lines of code and serves 1.2 billion people. This has 500 million lines of code and it has been challenged to provide the security and the functionality that you need. So yes, looking from the private sector, this actually would require a reinvention in terms of how you go out for proposals as opposed to an IDIQ contract, which this was done under. It is actually to go out and say, give us your best shot, we have a statement of objectives, here is what we would like to achieve, now innovate and build towards that. Your costs would have gone down. The complexity of the code would have gone down, that Dr. Chang talked about.

Mr. NEUGEBAUER. Thank you.

Mr. Kennedy, so the complexity of this program means that some of the proven techniques that have been used out there in the private sector that have run through these security checks might not have been incorporated into this code and so basically when you have this much new code, does that increase the vulnerability of the system?

Mr. KENNEDY. It does significantly and if you look at Microsoft, everybody here has heard of Microsoft before, Windows, Microsoft Windows. You know, you hit the 50- to 80-million mark for lines of code. Microsoft still continues to this day to have security flaws and exposures, albeit significantly less because they have done formal testing. They have a great security program that actually looks at a lot of these. But in its very early stages, it was definitely one of the most hacked operating systems that there was out there with hackers basically breaching with what call zero days or exploits every single day. And so when you have 500 million lines of code, which is six times greater than the code of Microsoft, you have significant problems with manageability of code, the complexity of the code and the introduction of exposures that are out there as far as exploits and attackers. So it is very difficult to manage something like that. It is very difficult to fix something like that as well as even be able to address some of the security concerns you have in a short period of time.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

Chairman SMITH. Thank you, Mr. Neugebauer. The gentleman from California, Dr. Bera, is recognized.

Mr. BERA. Thank you, Mr. Chairman. Thank you, witnesses, for being here.

We never let politics get in the way of addressing health care, addressing getting access to care. This body never would let that happen. So since we are going to work together as Democrats and Republicans to make sure we are able to get a system up and running, my goal is not to defend the HealthCare.gov website. Obviously this was a botched rollout. It is to take advantage of the fact that we have some security experts here, to take advantage of the fact that we have got to fix and make this better. My colleague from Massachusetts, Mr. Kennedy, already identified one way that we have made this fix and made it better in terms of the sequencing, right? So when I have gone to my home state exchange, Covered California, it doesn't ask for any personal information. It al-

lows me to just put basic information in, zip code, basic income level and then it gives me an estimate. It sounds like HealthCare.gov fixed that. That is a good thing. It makes it more secure, right? Everyone would agree with that?

Dr. Chang, you mentioned that 86 percent of all websites have at least one vulnerability. We are not here suggesting that we shut down 86 percent of the internet. What we are suggesting is we should be vigilant and address those vulnerabilities and we should do everything we can to the extent possible to make things secure. Again, I think we all agree on that.

Mr. Wright has mentioned four things. We just talked about sequencing. So this change in sequencing makes us better. Cyber squatting, domain name threats. I know in my state last week, the Attorney General shut down, I believe, 10 websites that were posing as Covered California look-alikes. We should be able to address that as well if we are vigilant about that. I would say we should just have someone looking at websites every day saying hey, these are fake website, let us go after them, let us shut them down. That is something we should be able to address, wouldn't you agree?

Mr. KENNEDY. I think you can definitely address a lot of those issues from identifying what sites are trying to impersonate as the website itself. There is definitely proactive steps you can take to minimize the risk to the website itself, absolutely.

Mr. BERA. So all of you would recommend that that is something worth doing?

Mr. KENNEDY. Absolutely.

Mr. BERA. So we should make that recommendation and get on that right away and make sure that no one is going to a fake website that looks like HealthCare.gov and putting information in. So that is a recommendation I think we can make as a Committee to immediately get on and it is something that should be done today, if in fact it is not being done.

Mr. WRIGHT. Dr. Bera, in fact, on the front page of the site, one of the things I suggest is exactly that. It would be nice for people to know what is an authentic account. Like when you get your banks, they say we will not ask for your password, we will not do this, just getting information like that from the government itself saying these are things we do and these are things we do not do and these are not authorized site, or here is the only sites that count would actually go a long way to preventing that fraud.

Mr. BERA. So we could certainly make that recommendation.

In my State of California, it is my understanding that all the navigators have to go through a background check, so I would ask the Committee to verify which states are making navigators go through background checks and which ones aren't. It is my understanding that because of the government shutdown, part of our challenge in California is that there is a backlog of navigators at the Justice Department going through the background checks. So that is an easy recommendation that we could make broadly as well, that at a minimum, the navigators should go through at least a basic background check. I would ask the Committee to verify which states are not doing navigator background checks versus which ones are. I don't think we can make a blanket statement that says navigators aren't going through background checks be-

cause, again, my understanding is that my home State of California, they are going through background checks. So again, easy recommendation, easy fix, an easy way for us to make sure that we are not compromising security.

And then the more complicated one—I am not a computer programmer, I did hear Dr. Rubin suggest that writing more lines of code doesn't always make a system more secure, in fact, it may make a system less secure. So, what I would encourage all of you, as well as all of the folks in the security industry, is to get out there as patriotic Americans, we want to make sure our country is secure. I would start making those recommendations to the federal government and I would ask the Administration to be open to inviting folks in to come in and make those suggestions because there is a lot of knowledge out there. You know, again, Dr. Chang suggested there are lots of vulnerabilities out there, so my message to the Administration would be, instead of being insular, let us actually invite folks in, Democrats and Republicans, to look at this website and make sure it is secure, and with that, I will yield back.

Chairman SMITH. Okay. Thank you, Dr. Bera. The gentleman from Alabama, Mr. Brooks, is recognized.

Mr. BROOKS. Thank you, Mr. Chairman.

I am not a computer security expert but I can read the words of those who are. The Science, Space, and Technology Committee staff prepared for Members' use a document called Hearing Charter, and according to our hearing charter, in order to use HealthCare.gov, American citizens will be asked to input or verify this type of information: birth and Social Security numbers for all family members, household salary, debt information, home mortgage information, credit card information, place of employment, previous addresses and the like. So when I see that, that causes me to pause. It causes me to have concern because that is a lot of personal information. I am sure that some criminal identity theft type of individual would consider that a dream, a wealth of information to get their hands on. Which brings me to the benefit of some of your written testimony, which of course is more extensive than your oral testimony, and if the Committee will bear with me, I am going to read from some of the written testimony that we received before we heard the oral testimony. "The vast amount of code also means applying industry standard security practices is a task that can have no real chance of success at present." No real chance of success at present. "The first major issue is the lack of an inability to conduct an end-to-end security test on the production system." Obamacare "also creates massive opportunity for fraud, scams, deceptive trade practices, identity theft and more." Another one: "The lack of effective security controls has created the conditions for massive fraud and hacking." Yet another one: "The most troubling insider threat aspect would be the lack of a personnel policy that requires background checks for individuals with access to PII"—personal information—"or sensitive information systems."

During testimony November 6, 2013, Secretary Sebelius admitted that convicted felons could be hired as navigators and that no federal policy existed to require background checks. So we have got the insider threat. Another one: "There are clear indicators that even basic security was not built into the HealthCare.gov website."

Another one: "There are systemic and serious concerns with the HealthCare.gov website. Based on our experience in large web applications such as this, there are a few options available in order to address the security concerns with the website," and the list just goes on and on and on.

It seems to me that the Obamacare website is the mother lode for identity theft, internet fraud and other criminal activity. It is quite frankly frightening and outrageous that the White House so callously and cavalierly exposes so many Americans to risk of debilitating financial damage, and all of this brings me to my questions. If HealthCare.gov identity theft occurs, an American citizen is financially damaged. What recourse does that citizen have under Obamacare against the federal government for compensation for financial losses occurred because we American citizens use the website we were told to use under Obamacare? Can any of you all describe to me what remedies, what recourse, what compensation can a citizen receive from the federal government for use of the website we are mandated to use that results in identity theft or other adverse effects?

Mr. WRIGHT. My very quick answer is, what form do I fill out to get my identity back because there is no way to do that. You can give me a credit card, you can fix my card, but once my identity is taken how do I get that back. That is probably one of the key things that has concerned me just from a technology standpoint is the protection from an identity theft standpoint. We can fix a lot of other stuff but your identity is what makes you who you are.

Mr. BROOKS. Dr. Chang, do you have any compensation that a citizen who has been wronged can get from the government for use of Obamacare's website?

Dr. CHANG. I think I would just maybe respond sort of generally. There is this notion kind of in credit card fraud that you basically hold the consumers harmless. This is very complex. They talk about 500 million lines of code, all this kind of scripting and stuff. It is very complex, and to expect users to have any sort of deep understanding of it, you might say gee, it is sort of like a credit card. You kind of hold them harmless.

Mr. BROOKS. I have only got 30 seconds left, so I am going to conclude with one quick question. Given HealthCare.gov's security issues and assuming for the moment that you would be personally responsible for all damages incurred, if any, from your advice, would any of you advise an American citizen to use this website as the security issues now exist? Yes or no.

Mr. KENNEDY. No, sir, not at this time.

Mr. WRIGHT. Same answer.

Dr. CHANG. Same answer.

Dr. RUBIN. Yeah, I wouldn't yet.

Dr. BROOKS. So it is a unanimous no, don't use the web site because of the security risks?

Dr. RUBIN. I would say that the security would have to be studied a lot more carefully before I would agree to that.

Mr. KENNEDY. And disclosed.

Mr. BROOKS. Thank you for your insight. I hope the American people are listening. With that, Mr. Chairman, thank you for the time.

Chairman SMITH. Thank you, Mr. Brooks. You elicited a unanimous response on that question.

The gentleman from California, Mr. Takano, is recognized.

Mr. TAKANO. Thank you, Mr. Chairman. I am disappointed that the Committee is spending its time this morning adding to the political drama around the Affordable Care Act. There have already been over 40 hearings this year on the Affordable Care Act by House committees, 15 of those since open enrollment began on October 1. And now we can add the Science Committee to that list.

While there certainly have been issues with the rollout of the website, the stories of how the Affordable Care Act is already helping millions of people are drowned out by the scare tactics used by my colleagues on the other side of the aisle. I have here the Republican playbook for undermining the ACA. It is filled with examples of how to scare constituents away from Obamacare. It is in the American people's best interest to encourage participation in the exchanges to help bring down premiums for everyone. But for my colleagues, it seems it is not about the American people winning, it is about them winning.

This hearing is just another attempt to undermine the President's signature law and follow their playbook.

Mr. ROHRABACHER. Mr. Speaker, Mr. Chairman——

Mr. TAKANO. Well, I would like to——

Mr. ROHRABACHER. Mr. Chairman, I——

Mr. TAKANO. While I would like to balance the record and share——

Mr. ROHRABACHER. Mr. Chairman, might I ask——

Mr. TAKANO. Mr. Chairman, I do not yield. I reclaim my time.

Mr. ROHRABACHER. I am not asking you to yield. I am asking the Chairman to make a decision as to whether or not what you just did was impugning the integrity of those who are disagreeing with you on this side of the aisle which is——

Chairman SMITH. Yeah, I would say the gentleman from California——

Mr. ROHRABACHER. —inconsistent with the rules of this Committee.

Chairman SMITH. I appreciate the gentleman from California bringing that issue up, but in the Chair's judgment, the accusation was general enough and not specifically addressed towards any individual. So I am sure the gentleman will not repeat it. But I would not say at this point it was out of order.

Mr. ROHRABACHER. Thank you very much.

Mr. TAKANO. Thank you, Mr. Chairman. I would like to balance the record and share a bit about how the ACA is helping my constituents. Twenty-four percent of my constituents are uninsured. That is 175,000 people in my district alone. The Affordable Care Act will get them covered so they don't have to worry about going bankrupt or being unable to get care if they become sick. Just yesterday I heard from a constituent who lost her insurance when her husband became sick with Parkinson's disease at the age of 50. Now through Covered California, she and her sons are able to get robust coverage, and they are saving more than \$600 a year.

Yes, the federal rollout has been complicated, and yes, we should be sure the website is protected from attack and Americans' per-

sonal information is secure. The law is about more than the website. It is about peace of mind for millions of Americans who need and deserve affordable coverage.

Now, I have seen a lot of—I am an English teacher, and I have seen a lot of rhetorical, a lot of red herring, rhetorical confusion sort of statements and testimony being made, and I just want to clarify something with you, Mr. Kennedy. I have—you were asking, responding to—excuse me. Before the hearing, you met with staff to discuss the vulnerability you found on the Data.HealthCare.gov site. In that meeting you said that you could not know what the architecture of Data.HealthCare.gov, what it was or how it was connected at the systemic level with HealthCare.gov. These are two separate websites.

Now you are saying that they share an infrastructure. I am not sure what you mean by that, but it implies that they are one in the same site. Now, let me ask you a simple question. You could see the account information for Data.HealthCare.gov, a site that is not designed for consumers but for researchers who look at national aggregations of data on health plans. Is an account at Data.HealthCare.gov also an account at HealthCare.gov? Are they the same?

Mr. KENNEDY. There are two questions there. The first is, is the account the same.

Mr. TAKANO. Are they the same? That is my question.

Mr. KENNEDY. They are not the same.

Mr. TAKANO. Okay. Thank you. Dr. Rubin, based on what you were able to learn preparing for this hearing, what are the vulnerabilities at HealthCare.gov implicit in Mr. Kennedy's discovery about the data website managed by CMS?

Dr. RUBIN. It is really not clear to me. The Data.HealthCare.gov, I went to it and looked at it, and it is a different kind of a site. And I am not sure. I would need to study the linkage between, if there is any, the accounts on HealthCare.gov and the accounts on Data.HealthCare.gov.

Mr. TAKANO. Okay. So Mr. Kennedy, do you believe there is any connection?

Mr. KENNEDY. I do. I do believe that there is significant connection. If you think HealthCare.gov, it is not just www.HealthCare.gov. Think of a house where you have a door which may be the entryway into it. There are things that support that website that pull data feeds in, and there are direct data feeds that get pulled in from Data.HealthCare.gov that are directly represented on HealthCare.gov. Information consists—

Mr. TAKANO. But are consumers going to be going to that site?

Mr. KENNEDY. Not necessarily. I don't know enough about the infrastructure to say whether or not consumers—

Mr. TAKANO. So you don't know anything about the infrastructure?

Mr. KENNEDY. I don't know enough about the infrastructure—

Mr. TAKANO. Yet, in your testimony there is an implication that people could draw that there is one.

Mr. KENNEDY. Well, there are over 100,000 individuals registered for that website. It would be indicative that it is.

Mr. TAKANO. Well, I think this is kind of an example of the confusionous sort of testimony, a red herring to make the American people—to scare the American people.

Mr. KENNEDY. I would say that extracting 100,000 individuals' email addresses—

Mr. TAKANO. Again, you don't know the infrastructure.

Chairman SMITH. Mr. Takano, would you mind letting the witness answer one of those questions?

Mr. TAKANO. Thank you. My time is up, Mr. Chairman.

Chairman SMITH. Okay.

Mr. WRIGHT. Mr. Chairman, could I actually add something? I wanted to clarify something. I just talked with your staff.

I just went through to create an account because the implication was made is that they have changed it. I am actually here right now with an account asking me to verify my home mortgage, Social Security number and stuff. So in terms of my testimony, I just wanted to make sure to be factual is that it still requires me to verify and provide personally identifiable information, Social Security number, credit information before I can create an account.

Chairman SMITH. Thank you for that clarification. The gentleman from Utah, Mr. Stewart, is recognized for his questions.

Mr. STEWART. Mr. Chairman, could I beg to defer my question for several and come back?

Chairman SMITH. Absolutely. We will return to you in just a minute. We will go to the gentleman from New York, Mr. Collins.

Mr. COLLINS. Thank you, Mr. Chairman. I think it is probably appropriate after that give and take, I am just going to ask six yes/no questions. How is that? We will start with Mr. Wright, go down the line, and there are six of them.

Number one, would any of you have launched HealthCare.gov, recommended the launch, given the factual, known status of the website on October 1?

Mr. WRIGHT. No.

Dr. CHANG. No.

Dr. RUBIN. No.

Mr. KENNEDY. No.

Mr. COLLINS. Number two, would any of you have signed off as experts on the front-end requirement to enter personal data to be able to go get pricing and other information?

Mr. WRIGHT. No.

Dr. CHANG. No.

Dr. RUBIN. No.

Mr. KENNEDY. No.

Mr. COLLINS. Do any of you today think today that the site is secure?

Mr. WRIGHT. No.

Dr. CHANG. No.

Dr. RUBIN. No.

Mr. KENNEDY. No.

Mr. COLLINS. While this is a hypothetical, in your opinion do any of you think the site will be secure on November 30?

Mr. WRIGHT. No.

Dr. CHANG. No.

Dr. RUBIN. No.

Mr. KENNEDY. No.

Mr. COLLINS. In your opinion, how long do you think it will be before the site could be secure? Just give me an estimate of months.

Mr. WRIGHT. Unknown.

Dr. CHANG. Hard to estimate.

Dr. RUBIN. I don't have enough information.

Mr. KENNEDY. A long time.

Mr. COLLINS. And finally, last question. This will be a record, Mr. Chairman, in a five minute questioning session. Would you recommend today that this site be shut down until it is verified to be secure?

Mr. WRIGHT. Yes.

Dr. CHANG. Yes.

Dr. RUBIN. I would need more information.

Mr. KENNEDY. Yes.

Mr. COLLINS. Thank you, gentlemen.

Chairman SMITH. Thank you, Mr. Collins. You would be a dangerous lawyer. The gentleman from Texas, Mr. Veasey, is recognized for his questions.

Mr. VEASEY. Thank you, Mr. Chairman. I wanted to specifically ask you about a couple of events that have been in the press here lately. One was a large bank, financial institution that had their information compromised. CitiGroup had an attack of about 146,000 people that had their Social Security numbers, their date of births and other information that was compromised, and there was also a large defense contractor that also had over 70,000 individuals that had their names, Social Security numbers, date of birth, blood type, other contact info. Can you explain how individuals are at greater risk of identity theft under HealthCare.gov than any of these other sites that I have just named?

Mr. KENNEDY. I can take that, and I appreciate your question there. There is no doubt that the hacking community and what is going on right now with technology is a great threat. I mean, it is happening all the time. There are attacks happening all over the world from different locations on different companies as well as government agencies.

And so what we need to do and what we need to bring awareness to, and this is why we are here as experts on the security side, is bring awareness to what you can do to prevent these type of attacks from happening because they are preventable. You can do secure coding. You can do things that prevent hackers from breaking in. You can stop them in the very early stages of an actual attack. And these companies that experience these type of breaches fundamentally had flaws in their security program that allowed these type of exposures to happen. There is a lot of success stories that have happened, a lot of companies that haven't experienced breaches. And those are the companies that I think hold true to proper secure coding practices, proper testing and ensuring that they have security injected into their software development lifecycle to prevent these type of exposures in the meantime.

Mr. VEASEY. Dr. Rubin, I would be interested to hear what you have to say.

Dr. RUBIN. I mean, he was echoing my thoughts exactly—

Mr. VEASEY. Okay.

Dr. RUBIN. —that there are known practices that if they are followed with proper personnel and proper training and proper security practices and encryption and the right software and the right software life cycle. You can't ever make a system that any security professional would claim is entirely secure, but you can make something that should stand up to the attacks that we are seeing today.

And so the sites that have been compromised, if you dig deep, and I have had experience and opportunity to dig deep in some of the sites that have been compromised, you often find that they either weren't vigilant enough, were running the wrong software or weren't following some well-known best practice that would have prevented the problem.

Mr. VEASEY. Have any of you, particularly because of the question that you just answered from the previous Congressperson on the dais on the Republican side, have any of you done a security assessment of HealthCare.gov? Because I mean, for you to be able to say that, no, you think that it should be shut down, I am assuming that you have done a security assessment.

Mr. KENNEDY. To answer that question, what we can see is indicators of security flaws, things that would be basic for an attacker to go after that should be addressed, even by the most simplistic scans or ways of detecting exposures. So to answer your question, I have not performed a security assessment on HealthCare.gov because I am not authorized to. However, based on using public information and information that is readily available, there are clear indicators that there are major security concerns on the website based off of what we can identify without actually attacking the site itself.

Mr. VEASEY. I would like for everybody to answer that one.

Mr. WRIGHT. Yeah, and what he is getting at, too, it is just the example I was talking about when the original denial of service attacks happened. They didn't happen right away. They built up until they got critical mass over a period of six months. The Chinese People's Liberation Army, the Mandiant report, advance persistent threat one did this for years. You will not see the massive attack in the first 30 to 60 days, but what you have are the precursors and the indicators and in a sense warnings is that all the conditions are there, the vulnerabilities are there, the lack of an end-to-end security test is there which will create the condition in the future, just like a forest fire. It is a recipe for disaster at some point in the future if it is not remediated.

Dr. CHANG. Yeah, I guess I would echo what some of the others have based on information that seems to be publically available, based on the testimony of David, and just this general idea that I mentioned before that the web is basically a pretty dangerous place, and some of these precautions haven't been inserted is cause for concern.

Dr. RUBIN. I think that the attacks that have been published so far and that I have seen have all been ones that are easily fixable, and the ones that have been around for a little while have been fixed. And before I would recommend shutting something down, I would have to know that there was some inherent security problem

or architectural flaw that necessitated that as opposed to some small superficial type risks that can be easily fixed. I don't want to minimize them, but if they can be fixed, that is better than shutting it down.

Mr. VEASEY. And to clarify the exchange that you had with Mr. Kennedy a little bit earlier, you talked about the HIPPA protocols, I just want to clarify something for everybody that may be watching this. HIPPA applies to medical records which are not stored in HealthCare.gov, is that correct?

Dr. RUBIN. That is my understanding.

Mr. VEASEY. Okay. All right. Mr. Chairman, thank you.

Chairman SMITH. Thank you, Mr. Veasey. The gentleman from Arizona, Mr. Schweikert is recognized for his questions.

Mr. SCHWEIKERT. And thank you, Mr. Chairman, and to a couple of my fellow Members, thank you for letting me skip ahead. I have another appointment in a moment. I need to disclose, I am sort of a junior-level SQL programmer which makes me just dangerous enough to think I know what is going on. Not that I wouldn't know about any of these blogs, but while sitting here I went on a couple of the hacker blogs that I have some familiarity with. Some of them, you all know, because I am sure when you are hunting for public information—that is why I have been a little surprised at some of the dialogue back and forth here saying let's have sort of a technical discussion instead of a political one that seems to be coming from the other side.

Outside of the, what is it, a DDoS type attacks, which are easy conceptually, mechanically, I found one whole discussion group talking about SQL injections. I would think that would have been just a junior-level thing to have avoided and tested for. So Mr. Wright, should I have a level of concern that just in sitting here in 40 minutes I was able to find a number of blogs talking about here is a script you might try?

Mr. WRIGHT. I am shocked it took you that long because it is out there. You look at the common vulnerability expressions, basically a common vulnerability database. One of the things you can do that is a very easy check is to check your site against the top 20 things that are out there and see how you rank against that. That is public information. The FBI does that. I think it is the San Francisco Field Office in concert with the security administrator networks. It is called SANS, I think, and then MITRE has that. There is stuff out there you can already test it again.

Mr. SCHWEIKERT. It is an automated script. You can just load it in and test your—

Mr. WRIGHT. And you can do—there is a lot of automated testing. But again, to David's point, there is no authorization from our side to conduct that and nobody wants to run afoul of the law. So you can only do things that are passively or recognizance. You can't do anything active against the site.

Mr. SCHWEIKERT. Dr. Chang?

Dr. CHANG. So I guess I would relate back to this idea that hackers will be patient. So David talked about, you know, kind of probes and scans. They are basically going to sort of check things out, try to understand if they will recognizance. They will, you know, press and probe. They will be patient.

Mr. SCHWEIKERT. Dr. Rubin?

Dr. RUBIN. Yeah. I mean, I think that the sequel injection attacks are one of the better-known types of attacks, and they can easily be prevented up front. From the demonstration that Mr. Kennedy did, it shows that people are actively trying out to see if there are sequel injection vulnerabilities.

Mr. SCHWEIKERT. Mr. Kennedy, I was going to actually go to something else because it is come up now I think two or three times in the discussion. HealthCare.gov, we should think of it as a portal that is reaching out and touching a number of different databases, and those different databases all, you know, most likely have also entries into those. So it is a connected web. And there has been some of the absurdity of some of the argument coming here is, well, you know, is it HealthCare.gov? If there is lots of ways to get into the hub, you will have lots of different paths of vulnerability. And I mean, I am trying to describe it as simply as possible. Am I doing okay?

Mr. KENNEDY. You are perfect. It is entirely accurate. If you look at what was mentioned, the data hub and the different sites that make up HealthCare.gov, HealthCare.gov is what we call the end-user experience, the user interface, the UI. That is when people browse and kind of view and things like that. But data that comes in from there comes from different areas. It comes from state exchanges, it comes from Data.HealthCare.gov. If you want to click on the live chat button on the bottom right, it takes you to Chat.HealthCare.gov. So there are different sites that make up what you see in your browser.

Mr. SCHWEIKERT. And that is often the vulnerability. It could be over here just a discussion group that actually has access in and that is my path in the line of code.

Mr. KENNEDY. In fact, right before this all started, I got an email from an individual that had sent me basically about 14 different exposures that they identified, and one of them was basically how to manipulate data that could be directly portrayed on the HealthCare.gov website because it pulls in from these different areas.

So, to put this conceptually and easy, it hooks into IRS, it hooks into DHS, it hooks into Experion which is a third party. You have all these trusted connections. You have all these things that make up the site itself. But the pieces that actually make up www.HealthCare.gov are multiple areas.

Mr. SCHWEIKERT. Yeah, I just need everyone to sort of understand that because there seems to be a misunderstanding of thinking it was a siloed website, and it is just the opposite. You know, think of it sort of as the spider web.

In my 20 remaining seconds, we have half-a-billion lines of code. Market value or market pricing right now for really beautiful, high-end code is what, 45 bucks a line? 50?

Mr. KENNEDY. It averages and depends based on what type of programming language and infrastructure, but sure.

Mr. SCHWEIKERT. And so that is where I have been trying to get my head around saying if just half-a-billion lines of code, particularly when you are reaching out and pulling in out of other data-

bases and then standardizing it, does something seem almost absurd?

Mr. WRIGHT. Well, there is also another paradigm, to, that if it costs you \$1 to fix it before you launch, it will cost you up to \$100 to fix it after you launch.

Mr. SCHWEIKERT. You beat me to the punch line.

Mr. WRIGHT. Oh, sorry about that.

Mr. SCHWEIKERT. No, it is okay. Mr. Chairman, thank you for tolerance, and thank you everybody.

Chairman SMITH. Thank you, Mr. Schweikert. The gentleman from Illinois, Mr. Lipinski, is recognized for his questions.

Mr. LIPINSKI. Thank you, Mr. Chairman. As Mr. Veasey had said and others have said, I think it is important enough to make the point again for those watching as I have been in my office up until now, HealthCare.gov does not store any personal, medical information or other information. So a hacker could get access to sensitive information, the hacker could not simply access all a person's life and medical history. I think it is important that we make clear that to the American people.

You know, it should be said that also cyber security threats are not unique to HealthCare.gov, and I have some concerns that we are just focusing on the security of HealthCare.gov but not other potentially vulnerable systems. Just yesterday, for example, the Treasury Inspector General for Tax Administration issued a report which found the security configuration settings on IRS servers were not set in accordance with IRS policy. The report stressed that if these servers were accessed by unauthorized persons, they might be able to access large amounts of sensitive information.

So I think that there are other things we should be looking at. It is easy right now to beat up on HealthCare.gov, but I think we should make sure we are doing our job in looking at all of the potential vulnerabilities in cyberspace, with cyber security, with government systems. But everyone would have to admit that the HealthCare.gov website rollout has been an unmitigated disaster. My personal experience with DC Health Link so far has not been very good, either, but I don't think—we are not talking about that right now.

Apart from the obvious issues of the lack of usability of the website, there have been security flaws present at the time of the launch which would have compromised the data that people entered into the site as has been mentioned. The fact the information is not stored on the website would be cold comfort to anyone who had their Social Security number and other sensitive info stolen as it was submitted to the website. I never want to downplay that importance.

In a memo on September 27, the CMS Administrator, Marilyn Tavenner, revealed that a contractor had not had access to all the security controls to test the system. The memo went on to say that, "From a security perspective, the aspects of the systems that were not tested expose a level of uncertainty that can be deemed a high risk."

So we certainly have examples of problems with HealthCare.gov. We have talked about those. I have long been concerned about cyber security issues in general, which is why in the last three

Congresses I have cosponsored the Cyber Security Enhancement Act with Congressman McCaul. This legislation would improve federal research and workforce development in the field of cyber security. I am glad that we have moved that here in this Congress.

I have also sponsored several bills which would make necessary changes to the Affordable Care Act including one to delay the individual mandate unless HHS's IG was able to certify that the website was working by November 30. I did not vote for the Affordable Care Act, but I think that we owe it to the American people to put partisanship aside and make necessary changes to the Affordable Care Act when they are required. I have certainly stepped forward to try to do that.

So with that long introduction, my question for the panel—hope you had some time to rest there—is whether a similar approach in some ways is needed for HealthCare.gov. So I want to ask, would it be helpful to have the—and this is for everybody. Would it be helpful to have HHS's IG certify that all known security issues have been dealt with and that a process was in place to proactively identify and address major security issues as they arise? Do you feel that an adequate process is currently in place. That is we talked a lot about issues here. Do we need to have a system maybe, like I said, HHS's IG or someone else who is looking at this and making sure that the processes are in place as these things are found? We never know for certain every single possible weakness. But would you think that would be helpful to help moving security along on this system?

Dr. CHANG. I wrote down some questions that are kind of along those lines. Maybe I will read them now. They might be useful. I think I would ask questions like how resilient is HealthCare.gov to a hacking attempt? What is your evidence? When there is a breach, how will we respond? What is our process for monitoring the security of HealthCare.gov? When a vulnerability is found, how quickly is it remediated? Are we taking all reasonable steps to protect the sensitive data on HealthCare.gov? What is the evidence?

Mr. WRIGHT. And to your point, it would be helpful because then we are dealing with a known. Now we have a report, and it may be is that the report would ameliorate a lot of the uncertainty that is out there. But on the other hand, you have to be prepared for the fact is that the report would identify the structural deficiencies that cannot go on and still allow the site to operate. But at any point, a knowledge base as Dr. Rubin was talking about would be helpful to make the proper assessment by experts and trusted people in the field to give you an idea, they, yeah, this can be fixed or no, it can't be fixed.

Dr. RUBIN. I think it is important to do what you are suggesting and to have reviews both at the high level because the questions that Dr. Chang was asking were high-level questions but as well as the low-level questions, a technical checklist of particularly known problems and making sure that all of those are addressed.

Mr. KENNEDY. I think the fundamental differences that we have here is there's no question that there is no security vulnerabilities with the website or that there are security issues that we know about right now with the website itself. So we know that there are vulnerabilities. We know that there are security concerns.

So having a process in place to actually address those in a very quick manner is a very good process to have and ensuring that they get remediated in a very timely, effective manner. Now, the question I would pose back is it is so complex that introducing changes to what we call a production site or something that is live and running becomes extremely critical and very hard to do because of the working code that is behind it.

So meeting those timeframes and meeting the ability to actually fix those issues may become more difficult to do in the current working environment that you have right now.

Mr. LIPINSKI. Thank you.

Chairman SMITH. Thank you, Mr. Lipinski. The gentleman from Utah, Mr. Stewart, is recognized.

Mr. STEWART. Thank you, Mr. Chairman. Thanks for holding the hearing, and to the witnesses, thanks for your service. Thanks for being here today.

You know, I am just a guy. I am not a genius, but I got to tell you, you don't have to be a genius to listen to your testimony today and to be scared to death. If I were in my living room or home doing dishes, listening to you as you have testified today, I would be scared to death. Americans should be scared to death.

I would like to come back to my friend, Mr. Collins, and his series of questions. I am not going to ask you to repeat or answer these questions again but just to review them for you and your response. Would any of you have launched HealthCare.gov? Unanimously, the answer was no. Would any of you have signed off on the front-end personal data requirement? Again, unanimously the answer was no. Is the site secure now? Once again, no. Will the site be secure on December 1? Once again, the answer is no, that you provided.

I would add one more, and I would ask your response on that. Is it possible to know how many attacks have occurred against HealthCare.gov and its associated sites? Are you aware of any? And let me kind of frame it in this question. If you were a Chinese cyber terrorist, wouldn't you consider this just a target-rich environment?

Mr. WRIGHT. So sir, to that point, you can only manage what you can measure, and if you are incapable of measuring the attacks and you don't have the capacity, you won't even be aware that those attacks have occurred.

So the point where they say they have only had so many attacks, that is based on what they know. Again, I go back to what Donald Rumsfeld said, you know what you know, you know what you don't know. What we are dealing with—

Mr. STEWART. Sure.

Mr. WRIGHT. —here is we don't know what we don't know, and until you have a comprehensive review of the site and you really understand your security posture and then put the defense in-depth strategies in place you have absolutely no idea about how many attacks.

Mr. STEWART. But there is no reason for us to be optimistic about the number of attacks or the vulnerabilities of this site, wouldn't you agree?

Mr. WRIGHT. I would say the number of attacks vastly understate the actual threat.

Mr. STEWART. Yeah, absolutely.

Dr. CHANG. Yes, I would happen to agree. We are very early on in the start-up of this website. My concern would be that they are spending now time basically kind of, you know, investigating, analyzing, kind of preparing. So this is the prep phase.

Mr. STEWART. Okay. Anyone else, if you have something to add? Okay. Let me kind of make this point then. If you were a federal official who had the authority and this was a private company and you were examining this company and saw the issues that you do with HealthCare.gov, and again, if you had the authority, would you shut that site down?

Mr. WRIGHT. Yes, and I will tell you what we suffered from. If you think of the Challenger disaster and the Apollo missions, people had go fever. This was going to happen on October 1 no matter what. No matter what risk finding you had and regardless of how serious it was, go fever said that we were going to launch on October 1. That is not the way to run a business.

Mr. STEWART. Okay. Anyone else want to—

Dr. RUBIN. Sure. I agree that it is pretty bad to have a particular date in mind that you are going to go no matter what. I think that the shutting down again will require a review to ascertain whether there are fundamental security problems or kind of scratching the surface security problems that can be easily fixed.

Mr. STEWART. Yeah. You know, I just think the irony isn't lost on people when they say the government, one of the responsibilities they have is to help set up processes to protect my personal information. And yet we have exactly the opposite here where not only are they not protecting them but they are requiring them and allowing the government to move forward with the program that is going to do exactly the opposite which then, if I could make my final point and question to you, what would you say to your constituents if you were me? What should I tell the people that I represent, the American people? I mean, how could I in good conscience go back and encourage them to participate in this program when we know that they are exposing themselves if they do? Can you help me with that? I mean, I would appreciate any advice you got on that.

Mr. WRIGHT. That is the advantage on being on this side of the table is I don't have to.

Mr. STEWART. Okay.

Mr. WRIGHT. No, you are in a very tough—and it is very tough. But at some point, people intuitively know. You have to tell them the truth. They have to make their own decisions. Still, the consumer needs to be aware. Educate them, tell them what the risks are, and if they choose to do it, it is still a consumer issue. But what we are dealing with here is a lack of awareness, education and people really understanding what the risk is. If they choose to take the risk, that is their issue at that point. But without knowing it, it is very hard to make that decision.

Mr. STEWART. Anyone else want to counsel us on that? Thank you. Mr. Wright, I think you hit on the key to that is all we can do is tell the truth, and I think that is the purpose of this hearing

here is to help people understand what is the truth, what is actually happening here. And that is why I think this has been valuable.

So Mr. Chairman, with that I yield back my remaining two seconds.

Chairman SMITH. Thank you, Mr. Stewart. Dr. Chang, I know you have to leave at noon. We are now a couple minutes past that in order to catch your flight. So thank you for being here today and thank you for your testimony.

Dr. CHANG. Okay. Thank you.

Chairman SMITH. Thank you. And we'll go to the gentleman from Oklahoma, Mr. Bridenstine, for his questions.

Mr. BRIDENSTINE. Thank you, Mr. Chairman. I just wanted to ask the panel—first of all, thank you so much for being here, and thank you for your service. There has been a lot of accusations from the other side of the room. I just wanted to ask the panel, did any of you guys come here because you wanted to scare the American people in an effort to bring down this law? Was that the intention of anybody on the panel?

Mr. KENNEDY. The purpose for us coming here is to explain what issues we identify. We are agnostic when it comes to the politics side. We are security researchers. We are folks that understand security, and our whole purpose here is to educate around what security concerns that we can see. I mean, I don't understand how you do your day-to-day jobs and how you work the government in every single side of the House. But I understand security. I understand how security works, and these things can definitely be fixed ahead of time. And it is not to instill fear at all. It is just to get the awareness out there, to get the information out there to help better educate and fix the issues that are apparent with the site.

Mr. BRIDENSTINE. Thank you.

Mr. WRIGHT. I think it was Harry Truman who said it best. We don't give them hell, we just tell the truth. They think it is hell. No, there is no R or D or I in computer codes. It is ones and zeros. The computer is agnostic about what it does. We had discussions—everybody here, we are not here to talk about the political issue, should it be up or down. We are saying if you are asking us, based on our background and experience and put our reputation on the line to say should we do this, it is about the technology. That is why, Congressman Stewart, I am glad we are on this side because you deal with the politics, we deal with the technology which sometimes is far easier than what you deal with. But no, the purpose coming here today is educate, awareness, give you our opinions. But we don't control those levers of power. What we do, as David said and Dr. Rubin says, we are here to give you our unbiased opinion what we think.

Mr. BRIDENSTINE. Dr. Rubin?

Dr. RUBIN. Yes, I agree with both of them.

Mr. BRIDENSTINE. Okay. Speaking of it, you mentioned the code, the code is non-partisan, there are 500 million lines of code. What is the risk? When you talk about 500 million lines, can you give me some comparisons and share with me what does that mean as far as risk?

Mr. KENNEDY. Whenever you introduce this amount of complexity, you introduce a significant amount of risk, especially from what we are understanding around the security testing, which was rushed out the door and not all components actually tested. So it is very much a critical risk from the lines of code that were developed, and to be honest with you, I have not seen—and I have worked for Fortune 10, Fortune 50, Fortune 100, Fortune 1000 companies as well as on the government side, I have not seen an application that pales in comparison to 500 million lines of code, including some of the largest applications you would ever see in the history of man.

Mr. WRIGHT. Just to put it in perspective, the website should be similar to a game of checkers. It should be that easy to understand. Instead, we are trying to find a chess master who can play 20 games of 3-D chess at the same time. That is the difference in the complexity of code because when you have two pieces of data, there's just not one possibility. There are actually four possibilities. There is no data, one piece, the other piece and then both pieces together. So when you add 500 million lines, then you are talking do the old checkerboard thing, put a penny and keep doubling it until you get to the 64 square, that is the complexity we are talking about.

Mr. BRIDENSTINE. So when you talk about this complexity, Mr. Wright, I think you are hitting on a critical component that it is hard for people who aren't computer programmers to wrap our brains around which is if you fix one piece of that 500 million lines of code, what are the—I mean, there's got to be some side-effects that result from that, is that correct? And how does that work?

Mr. WRIGHT. Side-effects is a good term. Yeah, you create an unintended series of cascading events that you have no control over because you don't have a grasp of what the code is actually doing. And to David's point, and he can actually show you these vulnerabilities, you think you have changed one thing, by doing that you have opened up a Pandora's box of vulnerabilities on the other side because you could not account for the path, the 72 places it had to go to before it finally got there. It is so complex, you can't manage that.

Mr. KENNEDY. And just taking it from the functionality side, when you introduce a piece of code that fixes a flaw, you could break the functionality piece that users see on a regular basis, too, because again it is so complex. So you fix one, you break another. It doesn't necessarily mean you fixed the security issue. You may not be able to actually browse a site or visit what you intended to actually use.

Mr. BRIDENSTINE. Just out of curiosity, if you had to assess the length of time it would take even to assess the security risk, how long of a period of time are we talking?

Mr. KENNEDY. To look at 500 million lines of code, there is a process we call source code analysis where you actually look at the code itself. And that is going to be your most comprehensive way of looking at the actual exposures.

And then you have what is called dynamic testing which is on top of it to look at the live running sites. So you marry those two together to perform kind of a holistic approach to looking at the

overall security around the site itself. Five hundred million lines of code? I would say to do it properly would probably take about six months or so just to do the review cycle of it.

Mr. BRIDENSTINE. And then after that you would have to do the fixes to secure it. How much longer would that take?

Mr. KENNEDY. And that is the problem. So in my written testimony, I gave three different options for recommendations on how to actually address the concerns with this because if you look at it then, let's just say that 20 percent of the code needs to be rewritten based on the exposures that are identified. If you introduce 20 percent new code into a running website that is up there right now, you are absolutely going to have some major systemic issues with the stability of the site as well as introducing new exposures to it.

So the first recommendation was to rebuild it in a sense of kind of like a version 2.0 which incorporates all of these changes or is rewritten from scratch to really kind of address it.

The second option was shutting down the site itself, making the changes and putting it back up after you've addressed those.

The third option was basically letting the website run and introducing new code into that environment which would obviously create stability concerns.

Each one of those has different links and times. If you do a version 2.0, based on the knowledge you already have with how to integrate into the already-running state exchanges, that would probably take six months to develop a new site that would be operational. The three folks that built it in two weeks are definitely a testament, but to do a fully production instance I think would take about six months. To shut it down, to actually shut it down and recode would probably take four to six months to get the critical concerns out of the way to at least get it back up and running again.

The portion around keeping it stable or keeping it up and running while introducing it could take years.

Mr. BRIDENSTINE. Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. Bridenstine. The gentleman from Texas, Mr. Weber, is recognized.

Mr. WEBER. Thank you, Mr. Chairman. Have any of you all assessed on a scale of one to ten the cost of this website with the volume of stores, the interaction, the cost per participant? In other words, you are going to have—I forget. I think they have said 100-something thousand had been on there, whatever it is, but versus private industry. From your knowledge about those websites and how they have been created and produced, on a scale of one to ten, ten being the most efficient bang for the buck, what would you give this? We will start with Mr. Wright.

Mr. WRIGHT. Back-of-a-napkin calculation, I mean, it is got to be somewhere around a two. Your average cost per user is significantly high because you have got few users and you have got a lot of money in it.

Mr. WEBER. Right. Got you.

Dr. RUBIN. I haven't had that data to perform a cost analysis.

Mr. WEBER. Okay.

Mr. KENNEDY. When you look at the website the infrastructure supported, I believe there was a statistic that came out that they

could handle 600 users per second on the site during registration process. So if you look at that infrastructure, you look at the amount of money that was spent on this, and it was in excess of I believe \$600 million? Is that correct?

Mr. WEBER. That is huge. Yes.

Mr. KENNEDY. I would give this a one as far as operational efficiency and the type of money that was spent on it.

Mr. WEBER. All right. Thank you. And my second—we are going to talk projected costs going forward because if it so expensive to maintain this thing and they can't hire the right people, then Americans' security is going to be at risk.

So going forward, if there was going to be a maintenance contract on maintaining this thing, which I am assuming there is, you are going to have to have personnel that are doing that. Now, my colleague from Utah said this would be a great vulnerability for Chinese cyber terrorists was the word he used. But I would submit that there might be some Edward Snowdens. They don't have to be in China.

From what you know, is that system available to disallow something like that happening where somebody inside could walk out with just tons of information? Yes or no.

Mr. WRIGHT. Based on what we know, no. Or at least what I know.

Mr. WEBER. Right.

Dr. RUBIN. I don't have enough information again about how the system is architected to answer that.

Mr. WEBER. Okay.

Mr. KENNEDY. And I don't have enough information on the back-end process for that, but it is my understanding no.

Mr. WEBER. I got you. What I wanted to is guarantee a platform, but that couldn't happen. So let's go back now. We ranked the efficiency on the dollar, but how about on a security scale? I think I am going to know this answer, one to ten, ten being the most secure, you have got to give this abysmal ratings, right?

Mr. WRIGHT. Based on what we previously said that we would not allow it to go. It would have to be a zero.

Mr. WEBER. Absolutely, has to be—okay. Go ahead.

Dr. RUBIN. So I think we have seen a bunch of security problems that were easily fixed, and a deeper dive is necessary in order to determine where we are on that scale of one to ten.

Mr. WEBER. But versus what you know about the private industry—

Dr. RUBIN. There is no doubt that compared to a private system that goes live, this system has more problems than you would expect to see.

Mr. WEBER. Well, I don't know that that is accurate because this is the federal government. We expect a lot of problems.

And then finally, Mr. Henry Chao I guess is how you say that, the Chief Information Officer for the CMS, said that the site was no problem. He would recommend it to his sister. I don't know, you all probably didn't read that. It is in our notes. So I guess this question is for Mr. Kennedy. You are the hacker. How long do you think it would take you to get his sister's information or do you already have it?

Mr. KENNEDY. I am not going to confirm that second one, but no.

Mr. WEBER. Okay.

Mr. KENNEDY. No, I do not have any type of public information. But you know, confidently I would say, and this is being very generous, I would say within a day to two days.

Mr. WEBER. One to two days you could go in and hack the site based on the platform that is there now, which is not guaranteeing zero or one level of security, if that is even—

Mr. KENNEDY. Yes, sir, and that is just understanding the amount of time it takes to understand an application is where the bulk of the one to two days comes in. It is just understanding how the infrastructure works, being able to start to kind of probe it a bit. It would take about a day or so. I could probably, you know—to be honest with you, it would probably take a few hours, but I am giving myself two days.

Mr. WEBER. All right. That is great. I mean, that is good news and bad news. It is bad news what you are saying it could be done, but it is good news is the American public is going to know this. So once you learn that system and get into it, then you can hack anybody's information really quickly.

Mr. KENNEDY. That is correct. Yes, sir.

Mr. WEBER. Makes me feel more secure.

Mr. WRIGHT. And sir, I think the biggest danger, too, is everybody keeps talking about the data hub. But what concerns me about the data hub is it operates as a trusted broker. In other words, all these other systems trust the data hub to say the transaction is authenticated, it is trustworthy. If that is not the case, you have just unintentionally done it similar to a Donnie Brasco, introduce somebody in that everybody trusts because of the introduction, not because it is actually trustworthy.

Mr. WEBER. So not only do we have politicians saying trust me, I am from the federal government, now we have computers saying it.

Mr. WRIGHT. Essentially yes. I mean, there's a certain level of trust that comes from the data hub.

Mr. WEBER. Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. Weber. The gentleman from Indiana, Mr. Bucshon, is recognized.

Mr. BUCSHON. Thank you, Mr. Chairman. First of all, I am a medical doctor, I was, before coming to Congress, and I want to briefly comment on some of the comments that were made about personal health information and whether that is profitable or not profitable, and I would ask the question would anyone in this room want to let everyone in this room know all their personal medical information? And I would say that the answer to that is no because it is personal. This is about people. This is not about profit on medical information.

Let me give you an example. When you ask people to direct donate blood, for example. Say someone is having surgery and their family members want to donate blood. Actually statistically, the blood from the regular pool is safer than having your family donate blood for you. Why is that? The reason is is because you don't know what all kinds of health problems that your family members have had because they haven't told you. And so I would argue this is a

personal privacy issue, and if there's any chance that people's medical information can get out there based on a government website, it is not correct.

The other thing I would like to say is quickly, and then I will have a question, is just because other websites of the federal government or in the private sector have problems doesn't justify this website having problems. I have heard that here today, too. Well, this website has been breached and this private sector has given up information. That doesn't matter. We are not talking about that. We are talking about this website, and it doesn't justify failures of this website.

So with that said, on September 3, 2013, a memo signed by the Chief Information Officer, there were at least two open high findings for the federally facilitated marketplace, the Federal exchanges. The first high finding, although substantially redacted, indicates that the threat and risk potential is limitless. It indicates corrective action must be taken by May 31, 2014. And information on the second high finding is completely redacted. It indicates that due date for corrective action is February 26, 2015. I think we have mentioned that before.

As cyber security experts, based on these findings, would anyone recommend that the federally facilitated marketplace, the Federal exchanges, be made publically available?

Mr. WRIGHT. Yes, sir. That is exactly the same memo I referenced earlier, and when the phrase is said the threat and risk potential is limitless, I don't know how you accept risk based on the fact as you can't quantify the risk.

Mr. KENNEDY. To also address that situation, in the private sector, those type of exposures are what we call showstoppers, things that would not allow the website to be put into production until they actually were remediated, and that would be especially ones that never heard the term limitless before which would mean that basically access to everything and everything that would be part of that infrastructure would be my guess. You would not put that into any type of production environment or go live with it in any way.

Mr. BUCSHON. Mr. Chairman, if this hasn't been introduced in the record—I can't remember if Mr. Wright did that—I would like unanimous consent to introduce the memo from CMS into the record.

Chairman SMITH. Okay. Without objection, it'll be made a part of the record.

[The information appears in Appendix II]

Mr. WRIGHT. And if I could add one more point in clarification, too, the difference in the private sector versus the government is that, gain, it goes back to liability, shareholder lawsuits. If a memo like this came out in litigation, you would find the firm facing financial ruin basically because they knew, they knew they shouldn't have done it and they did it anyway. And that is the basis for company killing litigation.

Mr. BUCSHON. Dr. Rubin, at this point, could you recommend, based on the fact we don't know what the redacted information is but that there was a high finding, would you recommend opening these up to the public at this point? I think it is a similar question

that has been asked before about the website. But this is specifically related to the exchanges.

Dr. RUBIN. Yeah, I mean before I would answer that question, I would want to see the details, the technical details of what the problems really are.

Dr. BUCSHON. It is my point these are redacted and not publically available, and that is an issue because outside people can't assess what the threat is because we have redacted information. And maybe since they have released this, they have made it public, but I don't think that is the case.

Mr. Kennedy, is it common—would anyone out there launch a website with these types of warnings before corrective action is completed? I mean, anybody out there? I mean, would it be prudent to do that?

Mr. KENNEDY. I come from very much a programming background, one that works with organizations on developing software for life cycles and building applications that are large like this.

So what I can say is that it depends on the risk of the organization and what they are able to accept. Based off of what we have seen and the information that is been publically available, I would not know of a company that would release a site like this with the functionality and security concerns that there were ahead of time.

Mr. BUCSHON. So it would be important for the public to know what the concerns were and then you could make a better assessment?

Mr. KENNEDY. Absolutely.

Mr. BUCSHON. That is what you are saying? I think that is what Dr. Rubin has said also.

Dr. RUBIN. Yeah, I agree. I am sorry. I agree. I think that the public should know what the concerns were.

Mr. BUCSHON. Okay.

Mr. WRIGHT. And just to add one point, sir, a final thing. When they establish the advanced encryption standard which became the basis for our encryption, that math, those algorithms were in the public. They were in the public domain. People got to view those, and to this day you can look at all the people who submitted things. Bruce Schneier submitted I think it was called "Two Fish." You have got the AES. The math is public. It was subject to peer review, and if there was any issues, it would have been exposed. And that is really—sunlight is the best thing when you are looking at remediating security problems. Expose it, let it be shown and let the people weigh in on it who've got the expertise. You will find people will crowd source and help you solve the problem.

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

Chairman SMITH. Thank you, Dr. Bucshon. The gentlewoman from Wyoming, Ms. Lummis, is recognized for her questions.

Mrs. LUMMIS. Thank you, Mr. Chairman. Mr. Kennedy, in a recent article by Fox News you were quoted as saying if I was allowed to attack the website by myself and I had approval to go and do it, it would be very simple for me to break into it, steal all the information that is in the database, including all of your personal information that you use to register for those sites, Social Security numbers, everything like that, basically that is what you were saying to one of the previous Members who was talking about Mr.

Chao's sister. You mentioned that you'd like to have two days to get in to access her information.

We have also learned today that these systems are integrated, that they are talking back and forth, that there's integration between HealthCare.gov and the IRS website and Homeland Security and others. Would you be able to get into HealthCare.gov and then use it to get into the IRS website?

Mr. KENNEDY. Without knowing enough about the infrastructure behind it, I can't say yes or no. However, what I can say is that as attackers and as hackers break into infrastructure, they usually use a conduit, a website, to use a trusted connection back to other infrastructure to gain access to that back end.

So without understanding infrastructure, I can't say yes, 100 percent. But based on the information that we know, you can look at the privacy policy on the website itself, it shows who it actually interacts with and the type of information it sends. If you look at that, it is pretty indicative that you could, you know, use that HealthCare.gov as a leaping point and kind of a back door into the other agencies, other Federal portions of government, like the IRS or DHS. And again, I can't say without certainty but it is definitely a common technique that a hacker would use to do it. It is called what we call, you know, pivoting and further attacking into the infrastructure.

Mrs. LUMMIS. And gentlemen, based on that information, would you have recommended that HealthCare.gov be walled off from other federal government databases that have very sensitive information?

Dr. RUBIN. Let me address your first question, and then I'll address the second question. First, just one clarification, that is it is not the IRS website. It is a back-end database of the IRS that is being accessed. And the way the data is being accessed is through this hub where requests are being sent. And so if the site were designed with proper security, with good security practices and principles, there would be a very, very limited interfaced between HealthCare.gov and the IRS where the IRS's database responses would be very limited in their nature. They could only answer certain queries to answer eligibility questions. If the site were designed very poorly and the interface was designed poorly, then I think that could be open. I don't know what kind of design they use, but in my written testimony I talked about focusing on those interfaces, keeping them very simple and very basic and using the hub simply to query those back-end databases at these other sites and get the responses back.

Mrs. LUMMIS. Mr. Wright?

Mr. WRIGHT. I think one of the challenges—and this is why I went back and confirmed after Congressman Kennedy said that—is that you still have to provide this information up front. So part of the issue you can get to make the site more secure and make it function better is to not put all this overhead on the initial transaction because the closer you are to the presentation layer to where the user is actually interfacing with it means it is easier to get that information to your point, not necessarily walled off and playing off what Dr. Rubin said, but I would like to push that kind of transaction back farther to where I can maintain better security. My se-

curity perimeter gets smaller. I can defend against things better. As opposed to the Great Wall of China, we are trying to secure the great fence of China, and instead what I want to do is have a smaller, tighter core that I can defend against and have that data hub, and those types of transactions happen in a smaller, confined area. You can't wall it off because it still has to interface, but you can reduce the risk and the threats by reducing the amount of waste and the places that to David's point an attacker can come in because they will do that. They will come in and they will use the same methodologies, the same seven-stage terrorism planning cycle that is in the traditional world is also used in cyber terrorism.

Mrs. LUMMIS. Well, we do know that there are countries that hire hackers, governments that hire hackers that attempt to hack into information in the United States all the time, and we know that some of those government-hired hackers hack for their government by day and they hack for hire by night. And so there are mercenary hackers out there that will hack for money.

Mr. Kennedy, are there vulnerabilities that you've not identified publically out of fear that the consequences are so exploitable that it would be like telling a criminal where you hide the spare key to your house?

Mr. KENNEDY. Yes, there is. There are exposures that I have identified that are not public.

Mrs. LUMMIS. Have you identified them to someone who can use them to plug those holes?

Mr. KENNEDY. Yes, I have. Any time that I discover an exposure or criticality, it is sent to the appropriate people to get addressed and fixed. That is where we come in from the responsible disclosure side of doing the right thing.

Mrs. LUMMIS. Gentlemen, I really thank you for your expertise and your presence here today. Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mrs. Lummis. I would like to thank our witnesses today for being here and helping us better understand the many privacy and security concerns that have been voiced concerning HealthCare.gov. Unfortunately, the personal information that has already been entered into HealthCare.gov is vulnerable to online criminals and identity thieves. This security flaw endangers a large number of Americans who already have used the website. President Obama has a responsibility to ensure that the personal and financial data collected as part of Obamacare is secure. It is clear this is not the case.

There is only one reasonable course of action. Mr. President, take down this website.

That concludes our hearing, and thank you again for testifying and we stand adjourned.

Mr. WRIGHT. Thank you.

[Whereupon, at 12:35 p.m., the Committee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Morgan Wright,
HOUSE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY

"Is My Data on Healthcare.gov Secure?"

QUESTIONS FOR THE RECORD

Mr. Morgan Wright
Chief Executive Officer, Crowd Sourced Investigations, LLC

Questions submitted by Chairman Lamar Smith

1. *According to news reports, Mr. Justin Hadley of North Carolina recently downloaded a letter from the Healthcare.gov website that included personal information belonging to Mr. Thomas Dougall of South Carolina. Mr. Dougall contacted the website to rectify the problem, but soon realized they had "no procedure whatsoever to handle security breaches."¹ In another case involving a Missouri woman, Ms. Lisa Martinson called Healthcare.gov's customer service after forgetting her password. She was informed that three different people were given access to her account, address and social security number and that "it would take up to five days to get her personal information offline."²*

These stories are very disconcerting. If these types of breaches have occurred for two people, how many other potential victims could there be? After hearing these stories, do you think this is just the tip of the iceberg?

The fundamental problem that still exists with providing an accurate answer is that no comprehensive, end-to-end security test has been completed on a stable system. There is no doubt there are other victims yet to be discovered. You can't manage what you can't measure, and there is no current evidence that there has been a baseline security assessment done. Without that information, you can't put limits on the potential risk that still exists.

2. *Can you compare the security of Healthcare.gov to other well-known and widely used federal websites? Are there lessons that can be learned from these other websites?*

¹ Sterling Beard, "Healthcare.gov Users Warn of Compromised Personal Information," *National Review Online*, Nov. 4, 2013, available at <http://www.nationalreview.com/corner/363031/healthcaregov-users-warn-compromised-personal-information-sterling-beard>.

² "Missouri woman's personal information stolen from Obamacare website," *Examiner.com*, Nov. 9, 2013, available at: <http://www.examiner.com/article/missouri-woman-s-personal-information-stolen-from-obamacare-website>.

I would think that the way the IRS handles the safety and security of information would be a better model for similar types of data that Healthcare.gov should model itself around.³

3. *What is your assessment on whether or not Healthcare.gov reflects best practices in website security technology?*
 - a. *Can you provide examples of a failure to use best practices?*
 - b. *What threats exist for website users due to these failures?*

I would refer to the analysis and report delivered by David Kennedy to the Committee. His testimony accurately and fairly reflected the security issues with the site, including examples of well-known security vulnerabilities that should have been patched on Day 1.

4. *In your testimony, you discuss cybersquatting. Can you explain what cybersquatting is and what dangers it poses? Are there some examples of this related to Healthcare.gov?*

Cybersquatting, also known as domain squatting, is generally defined to be the intent to profit from the trademark or goodwill of others by using a similar sounding domain name.⁴ The primary danger is that consumer will be deceived into believing that another site – not the authentic site – is legitimate and enter personally identifiable information, including credit card data to pay for any premiums. Since this is such a complex issue, bad actors exploit this confusion with similar sounding domain names.

A recent Washington Examiner article detailed an analysis by a cyber security expert that revealed that over “700 websites have been created playing off of Obamacare or Healthcare.gov, making it likely that some Americans will mistakenly hand over private information to unknown third-parties.”⁵ An early example cited was the use of “Obama-care.us” which led originally to a very well designed site that fooled the expert. The use of these tactics is not new. In fact, as early as 1997, the domain ‘whitehouse.com’ was registered and was originally an adult site.⁶

5. *The Authorization to Operate (ATO) that was signed on September 27, 2013, indicates that “Due to system readiness issues, the Security Control Assessment was only partly completed.” It further states that “From a security perspective,*

³ http://www.treasury.gov/tigta/auditreports/2013reports/201320126_oa_highlights.html

⁴ <http://en.wikipedia.org/wiki/Cybersquatting>

⁵ <http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare.gov-state-exchanges/article/2537691>

⁶ <http://news.cnet.com/2100-1023-202985.html>

the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM (Federally Facilitated Marketplace)."

What concerns would you have as a security expert based on these statements? Knowing the scope of this system and the type of information collected, would you advise a client to go forward with the launch of a site in this type of situation?

A site with a high-risk finding never should have been granted an ATO. The fact that the chief information security officer (CISO) for CMS, Teresa Fryer, refused to sign off on the ATO because of the risk should have been the final word on the subject. Both Teresa and Troy Trenkle, the chief information officer (CIO) at CMS (who also refused to sign), would have been in the best position to know the risks and understand the magnitude of this decision. Marilyn Tavenner, the Administrator for CMS and a political appointee, eventually signed the ATO. Knowing that both the CISO and CIO refused to sign off on the ATO, my guidance to any client would be to heed their advice and address the issues preventing the issuance of the ATO.

6. *Does the difference in size and scale of Healthcare.gov as opposed to a state-based exchange affect security strategy?*
 - a. *Should the federal government be responsible for providing states with guidance on website security to ensure conformity?*

The size and scale of the federal site presents a range of complexities that are not shared by state sites. Every state site must connect to the federal site, but not to other state sites. They have one connection essentially to worry about. However, Healthcare.gov must concern itself with every state exchange connecting to it. The federal government should provide guidance and formulate a collaborative security strategy to standardize the approach to securing sensitive information. There is already a model with DHS for cybersecurity, and with DOJ for securing some of the most sensitive information being shared – criminal history information.

The FBI CJIS Division has a security policy that is obligatory upon all law enforcement agencies (nearly 18,000) in order to access the system of services provided. It has been developed in collaboration with a Federal Advisory Committee called the Advisory Policy Board (APB). All 50 states participate and have input. The result is a

comprehensive set of standards and guidelines that govern the sharing of sensitive law enforcement data.⁷

7. *Numerous questions have been raised by security experts regarding the security of the website and whether it received the proper review envisioned by the Federal Information Security Management Act (FISMA) before it was launched. Georgetown Law professor, Lawrence Gostin, a strong supporter of the Affordable Care Act, told CBS News:*

“They should’ve really had this fully tested from top to bottom before the rollout. It would’ve made so much more sense politically, policy-wise and from a security and privacy perspective.”

CMS officials have indicated that testing was performed on pieces of the site but the entire system was not tested end-to-end. How important is end-to-end testing prior to launching a website of this magnitude? What potential flaws and vulnerabilities can exist if such testing is not done?

Testing the entire site, and not just pieces, is as important as testing the entire airplane before putting passengers on it. As detailed in the findings of the ATO, by not doing an end-to-end test you have a threat potential that is limitless. Since there is no way to quantify the risk, there is no way to create an effective remediation plan. This approach leads inevitably to greater vulnerability and risk.

8. *A report issued by the HHS OIG in August states, “CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub.”⁸*

Given your respective experiences, should this language have raised red flags at the highest levels of the government that problems with the website might not be resolved by the October 1st launch date?

This should not have only raised a red flag; it should have caused an immediate briefing by HHS to the White House to provide accurate information on a project of this technical and political magnitude.

⁷ <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>

⁸ Observations Noted During the OIG Review of CMS’s Implementation of the Health Insurance Exchange—Data Services Hub, A-18-13-30070, August 2013, available at <https://oig.hhs.gov/oas/reports/region1/181330070.asp>.

9. *Given this Administration's repeated and vociferous pledges of transparency, would you consider the construction and management of this website to be in keeping with such pledges? If not, what kind of information would you expect to see?*

It would seem improbable to be able to give a pledge of any kind when the true extent of the threat and risk is unknown and non-quantifiable. The lack of centralized leadership, clear project management and accountability make any attempt to be transparent impracticable.

10. *In a September 3, 2013, memo signed by the Chief Information Officer, there are at least two open "high" findings for the Federally Facilitated Marketplace (FFM). The first "high" finding, although substantially redacted, indicates that "the threat and risk potential is limitless." It indicates corrective action must be taken by May 31, 2014. Information on the second "high" finding is completely redacted, but indicates that the due date for corrective action is Feb. 26, 2015.*

- a. *As a cybersecurity expert, based on these findings, would you have recommended allowing the FFM to be made publically available?*
- b. *Is it common to launch a site with goals of corrective action being completed almost a year and a half into the future?*
- c. *If the threat and risk potential is limitless, how can the website protect the information of the American people attempting to sign up?*

A. The decision to make the findings publically available would require knowledge of the content of the findings. In any event, these findings should have been disclosed to any oversight authority in their entirety in order to determine whether or not a substantial risk to the security of the site would have been created if the information were to be made public.

B. I know of no viable sites in the commercial space that would even consider a timeline of days for a defect of this magnitude.

C. Until the findings are remediated, and the true nature of the risks are publicized and subjected to peer review, there is no way to provide that assurance to the American people.

11. *What kind of harm can be done through identity theft to an individual whose personal information has been stolen or compromised? Would you categorize this kind of harm as a moderate or serious risk to an individual?*

The range of harm could be as simple of a minor amount of fraudulent charges to a credit card, to the wiping out of home equity, personal savings, poor credit scores, loss of a job, law suits and more. This is a serious risk to any individual accessing a site with a threat and risk potential that is limitless.

12. *I understand you are familiar with the National Institute of Standards and Technology (NIST) security levels of low, moderate, and high. In a Centers for Medicare and Medicaid Services (CMS) document from September 3, 2013, Healthcare.gov was labeled as a 'moderate' risk site. Given the amount of personal data available through that site, would you agree with that risk designation?*

I would not agree. The existence of two findings of 'high', with the commentary on one that the "threat and risk potential is limitless" would logically preclude a lower finding.

13. *What are some immediate recommendations you would have if Healthcare.gov was one of your clients? Also, what would be your long term recommendations, and would they be easy to implement and follow through with?*

Create single position with the responsibility, accountability and authority over all agencies and contractors involved in Healthcare.gov. Develop a robust quality assurance testing process for existing features and components. Scale back and turn off or eliminate all unnecessary services and features until a stable operating environment can be maintained at a proscribed set of Key Performance Indicators (KPI's). Once the system can be maintained at these KPI's, then freeze all further development until a complete end-to-end security test can be planned and completed.

Long term all moderate to high risk vulnerabilities must be fixed before continuing further development. Once a baseline has been established, implement a vigorous and robust development plan that tests and measures every component before it is rolled out to a live production system. Security must be in every assessment and feature/function development. Nothing is every easy to implement or follow through with unless there is a plan, accountability for results, and relentless security testing and quality assurance.

14. *As part of the rollout of Healthcare.gov, what types of outreach would you recommend to educate the public regarding steps they can take to protect their personal information from ending up in the hands of identity thieves? To your knowledge, have any of those steps been taken by the federal government?*

I would recommend that public education be conducted on the 'only' official site for the federal government. On the site would be a list of all the official state exchanges. An easy to remember URL, such as MyStateExchange.gov, should be marketed to the public as the only authoritative source for this information. (As of this response, this URL is available for use by the government). It's important that consumers know where to go to get the info. The government should also register MyStateExchange with .com, .net, .org, .info, .us and .biz. This information should be on the landing page for Healthcare.gov and highlighted. As of this written testimony, no information exists on the landing page that educates or warns consumers about deceptive practices and web sites, or legitimate state exchange sites.

15. *The Administration has been working to fix the website and the American public has been assured a much improved site after November 31, 2013. What is your analysis of the website today as compared to when you testified on November 19, 2013? Specifically, is there any indication that the website has addressed the privacy and security concerns raised during the Committee's November 19th hearing?*

Although the site appears to be functioning faster, this does not correlate to better security. It does appear that consumers can view plans now without providing personally identifiable information. However, without a comprehensive end-to-end test, disclosure of the existing vulnerabilities and review by a neutral third party (to include security assessments, penetration and vulnerability testing, policy review, etc.) progress is difficult to measure, much less endorse.

Questions submitted by Rep. Steve Stockman

The administration talks about completing a "punchlist" to get the site working, and otherwise correcting the many problems.

- 1) *Can a collection of code patches create more security vulnerabilities than entirely rewriting the code?*
- 2) *What is the historic record of vulnerabilities from patches vs. rewriting?*
 1. Yes. Patching is a tactic, not a strategy. Patches on top of patches create complexity that is unmanageable. A patch should be used to fix a temporary problem while code is rewritten to eliminate the issue. Once tested, the code is rolled out to the production system, overwriting the patch and leaving new code in its place.
 2. I know of no authoritative source that has measured this. However, best practices in the security domain are analogous to fixing a leak in

a submarine. A temporary patch stops the immediate danger, but is never designed as a long-term fix. Once a remedy has been fashioned, it is applied so that the solution is as close to the original as possible. The longer the temporary patch is left in place, the greater the danger and the higher the chance the original problem will not only present itself again, but that the next episode will be far worse than the first.

Responses by Dr. Fred Chang

Questions submitted by Chairman Lamar Smith

1. *What are some security issues with the website that you have identified? Are they the sort that can be anticipated and prevented, and once identified, easy to mitigate?*

I have not personally performed a security analysis of healthcare.gov. With that said, I would reference the analysis done by David Kennedy of TrustedSec that was submitted as his written testimony to the Committee on November 19, 2013 (1). That document describes some analysis done by TrustedSec and also references other security findings that have been posted on the web. In this document, Mr. Kennedy describes the importance of building security into the application from the very beginning. This is a point that bears repetition and has been made by security professionals for many years. To the extent that an application has allowed security to be a secondary concern (e.g., security is "bolted on" afterwards) then this is an issue that is not easy to mitigate. The healthcare.gov website must be designed with the expectation that it will be the target of a full spectrum of attacks.

2. *In your testimony, you discuss the top 10 web application security risks. Can you give us specific examples of how a failure to address these risks would result in real harm to the individuals logging into the website?*

Here are the 2013 Top 10 Web Application Security Risks that have been issued by the Open Web Application Security Project (OWASP):

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Known Vulnerable Components
- A10 – Unvalidated Redirects and Forwards

The first item on the list, called Injection, refers to how an attacker can "inject" code into, for example, a web input field to tamper with a database. This attack is common and if a website is vulnerable to this attack, in effect it enables an unauthorized user to have access to a database such that the data in that database can potentially be stolen, modified or destroyed. This attack vector has been around for years, and many websites have been compromised by it. The third item on the list, called Cross-Site Scripting (XSS), is another common attack. Rather than an attack on a server database

as described in the example above, XSS attacks are usually against another user's browser. If a website is vulnerable to this sort of attack the result can be hijacked user sessions, website defacement, redirected users, and more. A good description of these Top 10 web application security risks along with remediation techniques can be found here (2).

3. *Can you explain the security of "back-end" software and how it applies to Healthcare.gov as you see it?*

a. *If Healthcare.gov is not sufficiently secure, could it make the additional databases it connects to- such as the IRS, DHS etc. more vulnerable to electronic attacks?*

As I mentioned in my written testimony, as I understand it, the system needs to access very sensitive information contained in "back-end" servers and databases at the Internal Revenue Service, Medicaid/Children's Health Insurance Program, various state agencies, Treasury, the Social Security Administration, the Department of Homeland Security, and Health and Human Services. I have not seen a detailed architectural description as to how these servers and databases are accessed, and thus can't comment on how well they are protected from unauthorized access. But it stands to reason that if you consider the complexity of the system and all the interactions (as depicted in the diagram I referenced in my written testimony) and the increased accesses (both human-to-machine and machine-to-machine), the risk level and chances for mischief have both gone up. From my perspective it is extremely important to have a thorough understanding as to how the increased security risk has been mitigated.

4. *Does the difference in size and scale of Healthcare.gov as opposed to a state-based exchange affect security strategy?*

Systems representing increased size, scale and complexity will certainly create additional security risks and challenges that must be managed compared with their smaller counterparts, but that said, both will represent extremely attractive attack targets and thus should be subject to the highest security standards.

b. *Should the federal government be responsible for providing states with guidance on website security to ensure conformity?*

The goal to insist upon conformance to a consistently high standard of website security across all the exchanges is a laudable one and it is reasonable to expect the federal government to take this on. It is important to realize of course that this must be

an on-going process because the standard will have to change as the attackers adapt to whatever defensive regime is put in place.

5. Numerous questions have been raised by security experts regarding the security of the website and whether it received the proper review envisioned by the Federal Information Security Management Act (FISMA) before it was launched. Georgetown Law professor, Lawrence Gostin, a strong supporter of the Affordable Care Act, told CBS News: "They should've really had this fully tested from top to bottom before the rollout. It would've made so much more sense politically, policy-wise and from a security and privacy perspective." CMS officials have indicated that testing was performed on pieces of the site but the entire system was not tested end-to-end. How important is end-to-end testing prior to launching a website of this magnitude? What potential flaws and vulnerabilities can exist if such testing is not done?

At a high level, the goal of testing is to effectively and efficiently identify and remove software defects -- and specifically as it relates to security, to identify and remove defects that can lead to a security compromise. So questions can be asked: What was the defect removal goal? Was the goal achieved? What is the evidence? To the extent that the testing goal was not completed, then the software will be susceptible, for example, to the sort of flaws discussed in question #2 above.

6. A report issued by the HHS OIG in August states, "CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub." Given your experience, should this language have raised red flags at the highest levels of the government that problems with the website might not be resolved by the October 1st launch date?

Not knowing the entire context of course, in my experience, if security was a top priority, this language would have raised concerns that delays are currently hampering security assessment and testing and minimally would have warranted an inquiry of the CIO to get his/her assessment of the statement and to understand what he/she is planning to do to mitigate the risk.

7. In a September 3, 2013 memo signed by the Chief Information Officer, there are at least two open "high" findings for the Federally Facilitated Marketplace (FFM). The first "high" finding, although substantially redacted, indicates that "the threat and risk potential is limitless." It indicates corrective action must be taken by May 31, 2014. Information on the second "high" finding is completely redacted, but indicates that the due date for corrective action is Feb. 26, 2015.

- a. Is it common to launch a site with goals of corrective action being completed almost a year and a half into the future?
- b. If the threat and risk potential is limitless, how can the website hurt the American people attempting to sign up?

Taken out of context and given the level of redaction involved, it is difficult to interpret these statements, but at the surface the language is concerning, and would certainly warrant further explanation and investigation.

8. Are certain demographics of consumers more susceptible to, or more likely to be targets of, attacks by website scammers? If so who, and why?

Campaigns to raise awareness among consumers regarding cyber defense and cyber "hygiene" have certainly been valuable and beneficial. Despite these campaigns, consumers machines continue to be compromised at a rate higher than any of us would like – there is a gap in the "human firewall". I don't have a study that I can readily reference, but anecdotally, given the sophistication on the part of the scammers, I've heard from a wide range of folks who have been compromised at one time or another.

9. In your written testimony, you reference a report which mentions that "within the first few weeks of the introduction of Healthcare.gov, over 700 fake websites had sprung up. How do website scammers convince individuals to put their personal information into these bogus websites?

The worry here would be that a consumer unwittingly accesses a website that they believe is the authentic healthcare.gov website, but isn't. This unwitting access could be the result of the use of a search engine, or by inadvertently making a typographical error when entering a web address into their browser. Once on the fake website – which happens to look very authentic – they begin to enter sensitive data.

10. The potential security risks from Navigators- who are hired to assist Americans sign up on Healthcare.gov- has received some attention in the media. For a website of this magnitude, what are some other sources of potential risks from the "human factor?"

It is my understanding is that there is no federal requirement for the Navigators to have had a criminal background check, though there may some local (state) rules that impose such a check (3). This is obviously a concern, particularly as it relates to how readily the Navigators can access the sensitive back-end databases. There is a well-known concept in the information security field known as the "insider threat". It is the idea that an employee (a trusted insider) who may have certain system privileges (e.g., greater system access), at some point becomes the hacker. There are stories of disgruntled employees who retaliate against their employer by committing some sort of information security violation. It gets worse if you imagine that an adversary of the organization places a malevolent employee there to do harm (e.g., on the janitorial staff who might have free reign after hours). In the case of the Navigators, a concern would be that without proper vetting, it might be possible to inadvertently hire a particular Navigator who wanted to do harm and could do so because they happened to have a deep software engineering background.

11. From your research, does it appear that sufficient attention was paid to security right from the get-go when Healthcare.gov was created?

a. Can you walk us through the steps of what you think would be appropriate security testing for a website like this from beginning to end?

b. How often should a website of this magnitude be tested for proper functioning of security?

Based on the preparation and research I did prior to the Nov 19, 2013 hearing, and since then, I would tend to agree with the conclusion reached in David Kennedy's written Testimony that sufficient security has not been built into the healthcare.gov application. Based on my reading of the open source material there seems to have been much attention paid to rolling out the application by a particular date (October 1, 2013), and while security was certainly been a consideration, my assessment is that security has not received sufficient up-front attention given how attractive a target healthcare.gov is and will continue to be to attackers.

Best security engineering practices discuss the need to build security into every phase of the software development lifecycle – from requirements, to design, to test plans, to coding, to testing, to feedback from operations (4, 5). Indeed security is an on-going process because as I mentioned previously the attackers will respond to the

system defense, and the application must anticipate this. I am aware of corporate best practices that conduct continuous, unannounced deep, thorough penetration tests to ensure that the targeted application constantly maintains a high security standard at all times.

I would note that the concept of building security into software has gained enough traction in government that there is even a government-based website that promulgates its advancement (6).

12. As part of the rollout of Healthcare.gov, what types of outreach would you recommend to educate the public regarding steps they can take to protect their personal information from ending up in the hands of identity thieves? To your knowledge, have any of those steps been taken by the federal government?

This past October, the U.S. observed the tenth annual National Cyber Security Awareness Month. This event involved a month's worth of activities designed to raise cyber security awareness for large numbers of people and was sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center. I believe that this has been a useful awareness raising tool over this past decade of ever-increasing cyber threat, and that it has made a difference in protecting people from harm in cyberspace. Additionally, the NCSA sponsors a useful website, StaySafeOnline.org, that is devoted to raising public awareness about the cyber threat. I am not aware of any cyber security public awareness raising activities associated with the introduction of healthcare.gov.

13. News articles have identified different potential security flaws within the Obamacare website. Some of the potential problems identified include: encryption failures, Clickjacking, Cookie Theft, Scam and problems with the password reset function among others. Can you explain what these terms mean and the potential problems these security flaws pose for consumers?

I'm not familiar with all of the different news reports that have been released detailing security flaws so my responses will no doubt be somewhat out of context, but encryption failures may refer to an instance where somebody noted that some piece of information should have been encrypted, but wasn't. This would suggest that the information was transmitted "in the clear" which would allow an attacker to read something they shouldn't have been able to read. Clickjacking refers to a technique whereby an attacker uses overlays on a web page to trick a user into clicking on a link

that was not intended thereby initiating an action that was unintended. Cookie theft refers to a security vulnerability that may allow a hacker to steal and read a cookie (small piece of data) that will give the hacker access to user data and/or assist the hacker in hijacking a session. The password reset glitch is probably the same one mentioned in Mr. Kennedy's report (1) that would allow an attacker to enumerate email accounts for individuals, which could be step one toward more serious consequences.

14. The Administration has been working to fix the website and the American public has been assured a much improved site after November 31, 2013. What is your analysis of the website today as compared to when you testified on November 19, 2013? Specifically, is there any indication that the website has addressed the privacy and security concerns raised during the Committee's November 19th hearing?

Based on my reading of some open source materials, it would appear that there has been a considerable amount of effort dedicated to enhancing the user experience -- by improving system availability, system capacity and system response time. I have not read any open source reports that have described any systematic efforts to improve security.

Questions submitted by Rep. Steve Stockman

The administration talks about completing a "punchlist" to get the site working, and otherwise correcting the many problems.

1. Can a collection of code patches create more security vulnerabilities than entirely rewriting the code?

The answer to this question would of course depend on many factors, but in the course of making changes to existing code to improve, for example system capacity, those changes might introduce new security vulnerabilities. As those code changes are being made, it is likely that those changes will add to the size of the software base, and thereby further add to the complexity of the software -- and as I mentioned in my written testimony, complexity is the enemy of security.

2) What is the historic record of vulnerabilities from patches vs. rewriting?

There is some historical information from Microsoft following the release of Windows Vista that is relevant here. Windows Vista was a substantial rewrite of Windows XP, including a total overhaul of security mechanisms. There are two

historical comparisons that can be made. The first compares security vulnerabilities in the first year following each OS release, and it turns out that Vista had 45% fewer vulnerabilities than did XP (7). The second comparison looks at the year 2007 and compares vulnerabilities that both OS's reported that year and Vista had 20% fewer vulnerabilities than did XP (8). With that said, because of the focus placed on security (among other things) the Vista release was delayed.

References

- 1) Kennedy, D. (2013). Healthcare.gov Security Analysis, Written Testimony for the hearing titled: "Is My Data on Healthcare.gov Secure?" convened by the U.S. House of Representatives Science, Space and Technology Committee, November 19, 2013.
- 2) https://www.owasp.org/index.php/Top_10_2013-Top_10
- 3) http://www.weeklystandard.com/blogs/sebelius-obamacare-navigators-dont-need-criminal-background-checks_766342.html
- 4) McGraw, G. (2006). *Software security: Building security in*. Addison Wesley, Upper Saddle River, NJ.
- 5) Allen, J.H. et al (2006). *Software security engineering: A guide for project managers*. Addison Wesley, Upper Saddle River, NJ.
- 6) <https://buildsecurityin.us-cert.gov/>
- 7) Jones, J. (2008). Windows Vista: One year vulnerability report, January 15, 2008. Report can be found here:
<http://blogs.technet.com/b/security/archive/2008/01/23/download-windows-vista-one-year-vulnerability-report.aspx>
- 8) Jones, J. (2008). Microsoft Vista vs. Windows XP SP2 Vulnerability report 2007, May 14, 2008. Report can be found here:
<http://blogs.technet.com/b/security/archive/2008/05/14/microsoft-vista-vs-windows-xp-sp2-vulnerability-report-2007.aspx>

Responses by Dr. Avi Rubin

- 1) In addition to Healthcare.gov, there is plenty of reason to be concerned about the security of states' exchanges as well. According to a Mother Jones article, "Hawaii, for example, does not automatically use SSL [Secure Sockets Layer] across its entire website, potentially leaving user information vulnerable to hackers—particularly if a visitor to the site is using an open wireless network, such as one at a coffee shop. The same is true with the online health exchanges created by Minnesota and Colorado." HHS hasn't been very helpful in this regard as the same article also adds that, "[T]he 15 states currently running their own independent Obamacare websites do not have explicit instructions from the HHS to use SSL."¹

Given your expertise in network security and evaluating the security of systems, including large web deployments, can you explain what impact this state vulnerability could have on the federal site to which they are all ultimately linked?

- 1) You are correct that SSL should be a requirement for any site that involves user authentication or the transfer of sensitive information. Any state that is not requiring SSL should immediately switch to this protocol. The good news is that it is a trivial fix to any modern Web server. SSL can be enabled in under a minute by simply changing a configuration setting.

If a vulnerable state exchange is connected to the federal site, there is a chance that the federal site could be adversely affected. However, if the interface is designed properly the extent of the damage would be that the federal site might receive incorrect information from the state site. The interface should be designed such that a compromised state exchange does not present a vector of attack against the healthcare.gov site, and in fact it would not be that difficult to design the interface in this manner.

- 2) You have stated that you classify Healthcare.gov as a high-maintenance system from a security perspective. A September 3rd CMS memo designates the risk to the site as "moderate." Knowing this, do you believe the government shares your perspective?
- 2) I do not work for the government, so I cannot speculate as to their perspective. I disagree with the assessment that the risk is moderate, given that healthcare.gov represents a significant target for attackers. With proper vigilance and appropriate technologies, I believe that the site can mitigate the risks to an appropriate level. I continue to believe that healthcare.gov will require significant ongoing maintenance for security.

- 3) The Authorization to Operate (ATO) that was signed on September 27, 2013, indicates that "Due to system readiness issues, the Security Control Assessment was only partly completed." It further states that "From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM (Federally Facilitated Marketplace)."

As a security expert, what concerns would you have about these statements?
Knowing the scope of this system and the type of information collected, would you advise a client to go forward with the launch of a site in this type of situation?

- 3) I think it is clear that the site launched before it was ready. I do not believe that hard and fast deadlines make sense for large software installations. When the alternatives are (1) to launch before it is ready or (2) to postpone the launch, I think the solution is to postpone and increase the level of effort until the system reaches a satisfactory state of readiness.

- 4) Numerous questions have been raised by security experts regarding the security of the website and whether it received the proper review envisioned by the Federal Information Security Management Act (FISMA) before it was launched. Georgetown Law professor, Lawrence Gostin, a strong supporter of the Affordable Care Act, told CBS News:

"They should've really had this fully tested from top to bottom before the rollout. It would've made so much more sense politically, policy-wise and from a security and privacy perspective."

CMS officials have indicated that testing was performed on pieces of the site but the entire system was not tested end-to-end. How important is end-to-end testing prior to launching a website of this magnitude? What potential flaws and vulnerabilities can exist if such testing is not done?

- 4) End to end testing is an important component of any system test before deployment. Failure to test end to end can result in a failure to identify potential flaws that relate to the inter-operation between components. In software systems, testing needs to account for a significant percentage of the effort, and unfortunately when systems are rushed out before they are ready, the most likely step that is skipped is testing. It is my understanding from reading the press reports in the last couple of months since the hearing on 11/19/13 that the site has been tested much more thoroughly, and that many of the required security and functional tests are being performed regularly now.

- 5) A report issued by the HHS OIG in August states, "CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub."²

Given your experience, should this language have raised red flags at the highest levels of the government that problems with the website might not be resolved by the October 1st launch date?

- 5) It is clear that CMS did not have the time that they needed to perform proper testing of the site. It sounds as though CMS was concerned that their CIO would not have the information that he might need, given the scramble to finish the system by the deadline. I think the biggest problem was that there was not any flexibility in the deployment date.
- 6) In a September 3, 2013, memo signed by the Chief Information Officer, there are at least two open "high" findings for the Federally Facilitated Marketplace (FFM). The first "high" finding, although substantially redacted, indicates that "the threat and risk potential is limitless." It indicates corrective action must be taken by May 31, 2014. Information on the second "high" finding is completely redacted, but indicates that the due date for corrective action is Feb. 26, 2015.
- a. Is it common to launch a site with goals of corrective action being completed almost a year and a half into the future?
 - b. If the threat and risk potential is limitless, how can the website protect the information of the American people attempting to sign up?
- 6) Yes, in fact, it is not only common, but I believe that in every instance that a major site is launched, there is an expectation that corrective action will be required throughout the lifetime of the system. That is the nature of software and is one of the reasons that I stated that the system will have a high degree of required security maintenance. As to the second part of the question, I believe that in many industries there have been success stories of implementing systems that adequately protect the information of Americans who sign up. Examples of these are the airline systems and the online banking systems. Many industries face similar risks, and there are known solutions for dealing with these problems. The problems of Healthcare.gov were not that the risk is limitless but that the system was deployed too quickly and without enough testing. It is my understanding that many of these issues have been or are being resolved.

- 7) In his opening statement, Chairman Smith provided specific examples of people whose personal information were compromised, including an instance where a gentleman from South Carolina's information from Healthcare.gov was sent to another gentleman from North Carolina without his knowledge or authorization. He had to jump through a great number of hoops to finally get his information deleted from the website. In the other example, a woman from Missouri was told that it would take up to five days for her personal information – which had been divulged to three people – to be taken offline.

Do these examples engender any confidence in you about the existence of high quality system administrators in place to keep up with software patches, respond to incidents, and monitor the systems for suspicious incidents, as you suggest would be needed for this website?

- 7) I think everybody understands that Healthcare.gov had some problems in its early days. However, I understand that they have put new management in place for the site, and that many of the problems that existed when these two incidents took place have been rectified. I do not believe that these incidents could happen again.

Questions submitted by Rep. Steve Stockman

The administration talks about completing a "punchlist" to get the site working, and otherwise correcting the many problems.

- 1) Can a collection of code patches create more security vulnerabilities than entirely rewriting the code?
- 2) What is the historic record of vulnerabilities from patches vs. rewriting?

I will address both of these questions with one answer. Patching is a necessary process that is part of any large software installation. For example, Microsoft issues patches to its operating systems and applications software every Tuesday and occasionally more frequently than that. It is true that patches can themselves introduce vulnerabilities, but more often than not, patches are used to fix problems with software in a benign way. I am not familiar with any study about the security tradeoffs of patching versus rewriting. However, it is safe to say that the most vulnerable system out there would be one that was never patched.

Responses by Mr. David Kennedy

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“Is My Data on Healthcare.gov Secure?”

QUESTIONS FOR THE RECORD

Mr. David Kennedy

Chief Executive Officer, TrustedSEC, LLC

Questions submitted by Chairman Lamar Smith

- 1) *Most websites store data, even if only for a short amount of time, to make the user experience easier should they get kicked off the website or if they have accidentally entered incorrect information. When Americans are entering their personal data on Healthcare.gov, how easy would it be for a hacker to obtain that information even if it is only stored for less than 30 minutes?*

Pretty easy, especially if they have maintained access to the servers. The information traverses through the application and could capture anything that was going through for the checks. As an attacker, I typically look at how the application is programmed and make modifications to intercept that information as it's being sent through.

- 2) *Healthcare.gov links to other agencies' websites, including the Department of Homeland Security, IRS, Social Security Administration, Health and Human Services, as well as Equifax. Is there any way a hacker could have access to these other databases by hacking first through the Healthcare.gov website? If so, how?*

This is my largest concern for the healthcare.gov website. If an attacker compromises the application, they would have the ability to perform lookups and additional access around database connectivity to the other agencies. This is a common attack method called “Pivoting” in the hacking community.

- 3) *News articles have identified different potential security flaws within the Obamacare website. Some of the potential problems identified include: encryption failures, Clickjacking, Cookie Theft, Scam and problems with the password reset function among others. Can you explain what these terms mean and the potential problems these security flaws pose for consumers?*

These are all symptomatic problems of poor coding practices and lack of formal security testing on the site prior to its launch as well as through its uptime. What this means to the average user is that with these flaws, an attacker could have access to their information or even attack them personally and their personal computers just by using the website.

- 4) *According to news reports last month, Mr. Justin Hadley of North Carolina downloaded a letter from the Healthcare.gov website that included personal information belonging to Mr. Thomas Dougall of South Carolina. Mr. Dougall contacted the website to rectify the problem, but soon realized they had “no procedure whatsoever to handle security breaches.”¹ In another case involving a Missouri woman, Ms. Lisa Martinson called Healthcare.gov’s customer service after forgetting her password. She was informed that three different people were given access to her account, address and social security number and that “it would take up to five days to get her personal information offline.”²*
- a. *These stories are very disconcerting. If these types of breaches have occurred for two people, how many other potential victims could there be? After hearing these stories, do you think this is just the tip of the iceberg?*

I believe this is only the tip of the iceberg and only what was reported. What’s happening on the application are errors in programming and logic that restricts access to other peoples information. These are almost always hammered out in “use case” testing to ensure that these types of glitches don’t occur. Another symptom of a much larger problem with the security on the website.

- 5) *The Authorization to Operate (ATO) that was signed on September 27, 2013, indicates that “Due to system readiness issues, the Security Control Assessment was only partly completed.” It further states that “From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM (Federally Facilitated Marketplace).”*
- a. *What concerns would you have as a security expert based on these statements? Knowing the scope of this system and the type of information collected, would you advise a client to go forward with the launch of a site in this type of situation?*

As large as this website is and the amount of information moving through it poses a significant concern around security. This is what would be considered in the private sector as a top tier and high risk application based on the sensitivity of the data and what it provides. If security testing hadn’t been finished or completely tested, there is a significant risk and exposure of compromise as well as misuse of the data on the system. I would highly recommend that until formal testing is fully complete and a level of understanding on the risk it has to personal information, that individuals do not use the website until it can be vetted on the level of risk it provides to other government agencies as well as personal identifiable information (PII).

¹ Sterling Beard, “Healthcare.gov Users Warn of Compromised Personal Information,” *National Review Online*, Nov. 4, 2013, available at <http://www.nationalreview.com/corner/363031/healthcaregov-users-warn-compromised-personal-information-sterling-beard>.

² “Missouri woman’s personal information stolen from Obamacare website,” *Examiner.com*, Nov. 9, 2013, available at: <http://www.examiner.com/article/missouri-woman-s-personal-information-stolen-from-obamacare-website>.

- 6) *Does the difference in size and scale of Healthcare.gov as opposed to a state-based exchange affect security strategy?*
Should the federal government be responsible for providing states with guidance on website security to ensure conformity?

Absolutely. The federal government should be responsible in providing expectations and baselines in security. NIST is a great format for that but there is really no oversight on how implementation around security is performed. The basic gist is we only have FISMA as a basis for security which is overly broad and generic and provides little guidance around appropriate security. Think of security as a pandemic, that if attackers gain access to multiple state and federal websites, especially with information being in an electronic platform, the amount of damage it can cause not only for the United States but its citizens. Information security needs to be looked at as the same as something like the CDC where you have a group that is responsible for a governance strategy and protection for federally and state run sites. Right now there are no breach disclosure laws for breaches that affect consumer data at the federal level, and 49 states that have it for PII on the state level.

- 7) *Numerous questions have been raised by security experts regarding the security of the website and whether it received the proper review envisioned by the Federal Information Security Management Act (FISMA) before it was launched. Georgetown Law professor, Lawrence Gostin, a strong supporter of the Affordable Care Act, told CBS News:*

"They should've really had this fully tested from top to bottom before the rollout. It would've made so much more sense politically, policy-wise and from a security and privacy perspective."

CMS officials have indicated that testing was performed on pieces of the site but the entire system was not tested end-to-end. How important is end-to-end testing prior to launching a website of this magnitude? What potential flaws and vulnerabilities can exist if such testing is not done?

End-to-end testing is paramount and should be mandatory under every circumstance. It would be like releasing a car without doing proper safety checks and it falling apart and the breaks failing while driving. While I am an expert in the security front and have a strong opinion on security, the lack of end-to-end testing is grossly negligent and puts the United States and the individuals that use the website under duress and harm. There are known exposures that were already identified without actually "hacking" the site, I fear that if we were to go deeper and perform end-to-end testing, the results would be highly alarming and frightening.

8) *A software tester in Arizona, Ben Simo, reported to CNNMoney that he had logged on and immediately found disturbing security flaws in the system that would allow someone to:*

- *“guess an existing user name, and the website would have confirmed it exists.*
- *claim you forgot your password, and the site would have reset it.*
- *view the site’s unencrypted source code in any browser to find the password reset code.*
- *plug in the user name and reset code, and the website would have displayed a person’s three security questions (your oldest niece’s first name, name of favorite pet, date of wedding anniversary, etc.).*
- *answer the security questions wrong, and the website would have spit out the account owner’s email address -- again, unencrypted.”*

If these flaws exist, how easy would it be to steal someone’s identity, even with a limited knowledge of computers? What does this indicate to you about the design of the website, and what kind of danger does this impose upon the American people?

The research by Ben shows how a tester without actually attacking can identify flaws and am in agreement with Ben. The flaws can make it extremely easy to gain access to another individuals personal information on a large scale and have access to personal information. I would already consider the findings from Ben a breach based on the level of exposures from the healthcare.gov and the information it provided.

9) *A report issued by the HHS OIG in August states, “CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub.”³*

Given your respective experiences, should this language have raised red flags at the highest levels of the government that problems with the website might not be resolved by the October 1st launch date?

Absolutely – the comments that full testing hadn’t have been completed should have been reviewed and a risk assessment performed to understand the level of exposure that the website would introduce to US citizens. This did not occur and released with known vulnerabilities and exposures – there is cause for major concern and should have been before the October 1.

³ Observations Noted During the OIG Review of CMS’s Implementation of the Health Insurance Exchange—Data Services Hub, A-18-13-30070, August 2013, available at <https://oig.hhs.gov/oas/reports/region1/181330070.asp>.

10) *In a September 3, 2013, memo signed by the Chief Information Officer, there are at least two open “high” findings for the Federally Facilitated Marketplace (FFM). The first “high” finding, although substantially redacted, indicates that “the threat and risk potential is limitless.” It indicates corrective action must be taken by May 31, 2014. Information on the second “high” finding is completely redacted, but indicates that the due date for corrective action is Feb. 26, 2015.*

- a. Is it common to launch a site with goals of corrective action being completed almost a year and a half into the future?*
- b. If the threat and risk potential is limitless, how can the website protect the information of the American people attempting to sign up?*

For point A. It depends on the risk, since these were consider high and “potential is limitless” these would be considered what we call “show stoppers” in almost any website. The website would not be launched based on the level of risk. Especially as high as these are. For point B. If the risk is limitless – this would be one of the highest exposures you could have on a website and the infrastructure. This would indicate that the website cannot protect the information of the American people and should have an expedited timeframe for addressing the risk well before the May and February times allocated. Again, certainty alarming on all fronts.

11) *What are some immediate recommendations you would have if Healthcare.gov was one of your clients? Also, what would be your long term recommendations, and would they be easy to implement and follow through with?*

Immediately, end-to-end testing needs to be performed, this would include a risk assessment, source code analysis, dynamic testing of the application, and a full scope penetration test. This would present a direct picture of what level of exposure the site has at this point in time, and from there a remediation strategy. This would dictate the long term strategy as well as establish process, procedures, and standards for how to move forward and do proactive security measures. This does not address the risk that’s currently on the site, I would be highly concerned at the timeframe between when these assessments were performed which is currently a high risk. Immediate stop-gaps should be considered such as web application firewalls, and heavy monitoring and detection in the meantime.

12) *If you had permission from the federal government to hack the website, what information do you think you could retrieve from it?*

Hypothetically and based on my personal experience seeing the systemic issues as well as the information reported, I am confident I could have access to the entire infrastructure for healthcare.gov and a high probability of gaining access to

sensitive information in other government departments. This would include the largest collections of sensitive data in US history, such as IRS, DHS, etc.

- 13) *If hired by the federal government to test and fix the website, how much would it cost, in terms of time and money?*

To perform a full scope test mentioned before (risk assessment, source code analysis, dynamic testing, and penetration testing) - it would take roughly two months from start to finish to identify what the problems and exposures are (roughly \$250,000 for the initial upfront). This would determine the future roadmap strategy and what would need to be performed to fix it. Without understanding how bad the site is, a prediction on fixing it is difficult or whether it is fixable. If I had to throw a monetary value of fixing the website, it would be around 5 to 10 million to fix the website. This would include developer time on recoding the application, developing an infrastructure that can perform adequate monitoring and detection, as well as implementing technology to help thwart attacks and alert.

- 14) *A recent December 13th memo from Democratic Members of the House Energy & Commerce Committee to Democratic Members of the House Oversight and Government Reform Committee indicates that the website has only experienced 32 Healthcare.gov information security incidents and essentially says that everything is fine with the site. What is your response to these observations?*

I would highly challenge this statistic of only 32 attacks. This would indicate and even more problematic monitoring and detection capability within the healthcare.gov infrastructure. Just based on sheer math, it's not possible to only experience 32 attacks against the site. A normal website experiences significantly more in a week timeframe than the multiple months healthcare.gov has been active as well as its popularity. Additionally, the President of Foreground Security who was contracted to perform the building of the monitoring and detection capabilities testified in front of Congress on November 19, 2013 to the House Energy and Commerce Committee which showed a roadmap to building a security operations center which was not completed (3 phase approach). That directly conflicts with the report that HHS is in any position to detect attacks. (<http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Amsler-OI-ACA-Healthcare-Website-2013-11-19.pdf>)

- 15) *The Administration has been working to fix the website and the American public has been assured a much improved site after November 31, 2013. What is your analysis of the website today as compared to when you testified on November 19, 2013? Specifically, is there any indication that the website has addressed the privacy and security concerns raised during the Committee's November 19th hearing?*

There literally has been little to no change in the security of the website since the testimony or exposures were reported. The website still remains to have a number of security exposures and has a lack of any formal practices in protecting the information.

Questions submitted by Rep. Steve Stockman

The administration talks about completing a "punchlist" to get the site working, and otherwise correcting the many problems.

- 1) *Can a collection of code patches create more security vulnerabilities than entirely rewriting the code?*
 - 2) *What is the historic record of vulnerabilities from patches vs. rewriting?*
1. Since the website is astronomically complex, introducing new coding changes can impact larger portions of the website and introduce more security flaws. If security is not baked into the development of the website, it becomes significantly harder to weed out the older and less security code as well as fix the new code. A rewrite of sections would be highly preferred or rewriting the entire application with security in mind. In stating that, it does not appear that this is an option. In this case, it will be significantly harder to fix the site moving forward.
 2. Historically most applications that are developed without security in mind often experience a breach or some sort of fault in security that causes a kickstart to a new version that is mostly recoded or re-hauled. Healthcare.gov has already experienced multiple breaches of sensitive information and does not appear to be getting any better.

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD



Eva Velasquez
Identity Theft Resource Center
9672 Via Excelencia, Suite 101
San Diego, CA 92126

November 15, 2013

Chairman Lamar Smith
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman,

The Identity Theft Resource Center (ITRC) regrets that we were not able to accept the Committee on Science, Space, and Technology's (Committee) invitation to testify in person; however, we appreciate the opportunity to submit this letter for the Committee's hearing record regarding medical identity theft and related concerns specific to the healthcare.gov website, or any website that collects sensitive medical information, and services.

The ITRC is a non-profit organization established in 1999 to assist victims of identity theft with mitigation of their case at no cost. We have assisted tens of thousands of consumers via our toll free call center, and reached millions of consumers via our website and mainstream media coverage. ITRC also serves as a relevant national resource on current topics related to identity theft such as cybersecurity, privacy issues, scams, and fraud.

The ITRC has been focused on medical identity theft and fraud for years as it continues to be one of the fastest growing and most dangerous forms of identity theft. ITRC and the Medical Identity Fraud Alliance (MIFA) define medical identity theft as the fraudulent use of an individual's Protected Health Information (PHI) or Personally Identifiable Information (PII), such as name, Social Security number, or the use of a fictitious identity, to obtain medical goods and services, or to unlawfully gain financial benefit. According to the *2013 Survey on Medical Identity Theft* conducted by the Ponemon Institute and sponsored by MIFA, an estimated 1.84 million Americans became victims of medical identity theft in 2013. This represents a 19% increase in just one year over the estimated 1.52 million medical identity theft victims in 2012. As a result of this crime, medical identity theft victims paid an estimated \$12.3 billion in out-of-pocket costs.

Medical identity theft is one of the worst forms of identity theft for many reasons. For one, it is extremely attractive for identity thieves and hackers because the sale of medical identities is so lucrative. An identity on the black market is exorbitantly more expensive when complete medical information is included as compared to an identity solely consisting of a Social Security number. This makes health records, particularly electronic health records, a primary target for hackers and thieves looking to sell large quantities of medical identities to make money without even engaging in medical identity fraud.

A national identity theft resource organization since 1999

9672 Via Excelencia, Suite #101, San Diego, CA 92126 | (858) 693-7935 | Toll-free (888) 400-5530 | www.idtheftcenter.org



Second, medical identity theft is extremely difficult to mitigate and often requires more time and money than the victim can devote to the issue without it affecting other aspects of their lives. The lack of a centralized medical database, such as the three major credit reporting agencies in the financial world, makes it very difficult for patients to prevent or detect medical identity theft. One cannot simply order their medical reports from a national organization and determine whether or not any fraud has taken place in their name anywhere throughout the US. The victim will have to track down each medical organization and deal with their billing and medical records departments in order to restore their records. Even while a victim is dealing with mitigating one instance of medical identity theft, a criminal may be using their identity to gain medical services elsewhere. There is no equivalent in the medical world to the financial "fraud alert" or "credit freeze" available to consumers with the major credit reporting agencies, so the crime can continue unabated.

And lastly, medical identity theft is extremely dangerous. When a medical identity thief obtains medical services under a fraudulent identity, they will give the doctor or organization information about their own medical history and status. This means the victim now has medical records with incorrect information that a physician may naturally assume is correct when diagnosing the patient or prescribing medication, leading to adverse outcomes.

In regard to medical identity theft concerns as they relate to the healthcare.gov website and services, ITRC has two main concerns. Our first and foremost concern is the lack of a federal requirement to conduct background checks on the program navigators. Navigators are tasked with educating the uninsured about their healthcare options under the Affordable Care Act and assisting them with enrollment. During this process, navigators may have access to an individual's personal information including Social Security number, tax return information, and medical information. Considering the sensitive nature of the information navigators may receive and the obvious potential for navigators to sell medical identities and engage in medical identity theft, we believe it is prudent to require background checks at a federal level. Even with background checks on navigators, there is still potential for medical identity fraud to occur due to their access to sensitive information, but at the very least we can prevent convicted felons with nefarious agendas from attaining these sensitive positions.

Our other main concern is that the healthcare.gov website requires a visitor to divulge their personal information before they are allowed to peruse the website and shop for health coverage. Typically, when shopping for nearly any product on the Internet the consumer enters any required sensitive information right before a purchase. ITRC believes individuals should be able to "window shop" and view various healthcare coverage options anonymously on healthcare.gov and any health insurance website as this will cut down on the volume of sensitive information trading hands. While we cannot speak as to how exactly this information is protected and transferred once received, generally speaking, less information exchange means less security vulnerabilities. In addition, removing the personal information requirement to shop will make individuals feel more at ease exploring the website knowing their personal information is only required when they decide to actually enroll in a health plan.

A national identity theft resource organization since 1999

9672 Via Excelencia, Suite #101, San Diego, CA 92126 | (858) 693-7935 | Toll-free (888) 400-5530 | www.idtheftcenter.org



Medical identity theft is a serious problem that our nation faces and is why the ITRC is a founding member of the Medical Identity Fraud Alliance, the first cooperative public and private sector effort to develop solutions and best practices regarding medical identity fraud. We want to bridge the knowledge gap between medical organizations and patients regarding data security and medical identity theft so they can better work together to reduce fraud. The ITRC prefers to be "the voice of reason," helping educate the general public about the realities of data protection, medical identity theft and what individuals can do to help protect their personal information.

Sincerely,

Eva Velasquez
President/CEO, Identity Theft Resource Center
Phone: 858-444-3274
Fax: 858-693-4974
Eva@IDTheftCenter.org
www.IDTheftCenter.org

A national identity theft resource organization since 1999

9672 Via Excelencia, Suite #101, San Diego, CA 92126 | (858) 693-7935 | Toll-free (888) 400-5530 | www.idtheftcenter.org

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-25
Baltimore, Maryland 21244-1850

OFFICE OF INFORMATION SERVICES



DATE: SEP 13 2013
TO: Director,
Consortium for Medicare Health Plans Operations (OA/CMHPO) and Acting
Deputy Center Director for Operations, Center for Consumer Information and
Insurance Oversight (CCIO)
FROM: Chief Information Officer and
Director, Office of Information Services (OIS)
SUBJECT: Authorization Decision for the Federal Facilitated Marketplaces (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federal Facilitated Marketplaces (FFM) System is a *Moderate* level system located at the Terremark Datacenter in Culpeper, Virginia. The system maintains records used to support all Health Insurance Exchange Programs established by the Centers for Medicare & Medicaid Services (CMS) under the health care reform provisions of the Affordable Care Act (Public Law 11-148). FFM will help qualified individuals and small business employers shop for, select, and pay for high-quality, affordable health coverage. Exchanges will have the capability to determine eligibility for coverage through the Exchange, for tax credits and cost-sharing reductions, and for Medicaid, Basic Health Plan (BHP) and Children's Health Insurance Program (CHIP) coverage. As part of the eligibility and enrollment process, financial, demographic, and (potentially) health information will flow through the Exchange.

On August 8, 2013, you certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate (ATO) for FFM.

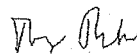
I have determined through a thorough review of the authorization package that the risk to CMS information and information systems resulting from the operation of the FFM information system is acceptable predicated on the completion of the actions described in the attachment. Accordingly, I am issuing an Authorization to Operate (ATO) for the FFM information system to operate in its current environment and configuration until August 31, 2014. The current configuration includes only the Federal Facilitated Marketplaces Qualified Health Plans (QHP) and Dental modules. This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. An impact analysis must be conducted for any system changes implemented after the issuance of this ATO. Any major modifications that affect the security posture of the system will require an appropriately scoped security controls assessment and issuance of a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

- (i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;
- (ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and
- (iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at [REDACTED]. The DISPC team is also available to support staff level questions at [REDACTED]@cms.hhs.gov.



Tony Trenkle

Attachment

cc:
 Mark Oh, Director OIS/CISG/DHIM
 Darrin Lyles, ISSO, OIS/CISG/DSMDS
 Teresa Fryer, CISO, Director OIS/EISG
 Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
 Desmond Young, OIS/EISG/DISPC
 Jessica Hoffman, OIS/EISG/DISPC
 James Mensah, OIS/EISG/DISPC

CMS SENSITIVE INFORMATION -- REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplaces (FFM) System

Authorization Decision

Authorization decision is required for the following reason(s):

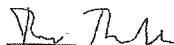
☒	New System
☐	Major system modification
☐	Serious security violation
☐	Changes in the threat environment
☐	Expired authorization to operate

I. Authorization Decision

I have reviewed the information concerning the request for an Authorization to Operate and with consideration of the recommendations provided by my staff, I concur with the assessment of the security risk. This risk has been weighed against the business operational requirements and security measures that have or will be implemented. I have determined the following authorization decision is appropriate.

X	Authorization to Operate The current risk is deemed acceptable. The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II. This authorization will expire: August 31, 2014 . This authorization may be withdrawn at the discretion of the Authorizing Official for lack of progress on the authorization actions in Section II, or any security violations deemed to increase the risk to CMS beyond a tolerable level.
----------	--

☐	Denial of Authorization to Operate The current risk is deemed unacceptable. The applicable system may not operate until the authorization actions listed in Section II are completed, after which, verification of corrective actions and resubmission of the authorization package is required.
--------------------------	--



(Authorizing Official Signature and Date)

Tony Trenkle

CMS Chief Information Officer

CMS SENSITIVE INFORMATION -- REQUIRES SPECIAL HANDLING

Page 1 of 5

II. Authorization Actions

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
FFM has an open high finding: [REDACTED]	[REDACTED] the threat and risk potential is limitless. [REDACTED]	[REDACTED]	The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) without continuous monitoring presents an unacceptable risk. (CA-2).	May 31, 2014

CMS SENSITIVE INFORMATION - REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
FFM has an open high finding:	[REDACTED]	[REDACTED]	The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) without continuous monitoring presents an unacceptable risk. (CA-2).	February 26, 2015

CMS SENSITIVE INFORMATION - REQUIRES SPECIAL HANDLING

Page 3 of 5

Contains Sensitive and Proprietary Business Information --
Maintain as Confidential

CGIHR00002830

CMS SENSITIVE INFORMATION -- REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
[REDACTED]	[REDACTED] Security controls are not documented as being fully implemented.	[REDACTED]	There is the possibility that the FFM security controls are ineffective. Ineffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise. (PL-2).	February 7, 2014
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] exposes the enterprise to additional risk. (RA-2).	February 7, 2014
[REDACTED]	[REDACTED]	Review the FIPS 199 inheritance selections in CFACTS and either select the appropriate inheritance or indicate the controls are solely the responsibility of FFM.	[REDACTED] can lead to controls not being appropriately implemented and a lack of accountability.	February 7, 2014

CMS SENSITIVE INFORMATION -- REQUIRES SPECIAL HANDLING

Page 4 of 5

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
Inconsistent Points of Contact (POCs).	The system developer/maintainer on the CMS Security Certification Form is a different person from [REDACTED]	Identify and update the appropriate system POCs for all of the documents and provide the updated POCs [REDACTED]	Unclear role responsibility can affect the life cycle support of the system. [REDACTED]	February 7, 2014
END OF ACTIONS				

CMS SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING
Page 5 of 5Contains Sensitive and Proprietary Business Information --
Maintain as Confidential

CGIHR00002832

