

HEALTHCARE.GOV: CONSEQUENCES OF STOLEN IDENTITY

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

SECOND SESSION

JANUARY 16, 2014

Serial No. 113-62

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

86-900PDF

WASHINGTON : 2014

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 COLLINS, New York	
VACANCY	

CONTENTS

January 16, 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	7
Written Statement	8
Statement by Representative Eddie Bernice Johnson, Ranking Member, Com- mittee on Science, Space, and Technology, U.S. House of Representatives	9
Written Statement	10

Witnesses:

Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC	
Oral Statement	13
Written Statement	16
Mr. Waylon Krush, Co-Founder and CEO, Lunarline, Inc.	
Oral Statement	30
Written Statement	32
Mr. Michael Gregg, Chief Executive Officer, Superior Solutions, Inc.	
Oral Statement	40
Written Statement	42
Dr. Lawrence Ponemon, Chairman and Founder, Ponemon Institute	
Oral Statement	49
Written Statement	52
Discussion	57

Appendix I: Answers to Post-Hearing Questions

Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC	88
Mr. Waylon Krush, Co-Founder and CEO, Lunarline, Inc.	102
Mr. Michael Gregg, Chief Executive Officer, Superior Solutions, Inc.	108
Dr. Lawrence Ponemon, Chairman and Founder, Ponemon Institute	113

HEALTHCARE.GOV: CONSEQUENCES OF STOLEN IDENTITY

THURSDAY, JANUARY 16, 2014

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

The Committee met, pursuant to call, at 9:13 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

Healthcare.gov: Consequences of Stolen Identity

Thursday, January 16, 2014

9:00 a.m. to 11:00 a.m.

2318 Rayburn House Office Building

Witnesses

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

Mr. Waylon Krush, Co-Founder and CEO, Lunarline, Inc.

Mr. Michael Gregg, Chief Executive Officer, Superior Solutions, Inc.

Dr. Lawrence Ponemon, Chairman and Founder, Ponemon Institute

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

HEARING CHARTER

Healthcare.gov: Consequences of Stolen Identity

Thursday, January 16, 2014
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

Purpose

On Thursday, January 16, 2014, the Committee on Science, Space, and Technology will hold a hearing titled, *Healthcare.gov: Consequences of Stolen Identity*. This hearing will be a follow-up from the Committee's November 19, 2013 hearing on the security concerns of the Healthcare.gov website.¹ At that hearing, expert witnesses raised concerns about the vulnerabilities and risks to the privacy and security of Americans' personal information. Today's hearing will provide the Committee with an updated security assessment to determine the likelihood of personal information being accessed or compromised because of an attack on Healthcare.gov. It will also examine the consequences of identity theft to Americans if hackers with malicious intent gained personal information through the Healthcare.gov website, which is one of the largest collections of personal information ever assembled, linking social security numbers, birth dates, and tax and other financial information of its users.

Witnesses

- **Mr. David Kennedy**, Chief Executive Officer, TrustedSEC, LLC
- **Mr. Waylon Krush**, Co-Founder and CEO, Lunarline, Inc.
- **Mr. Michael Gregg**, Chief Executive Officer, Superior Solutions, Inc.
- **Dr. Lawrence Ponemon**, Chairman and Founder, Ponemon Institute

Overview

On November 19, 2013, the Committee held a hearing to assess the security of data on Healthcare.gov where witnesses raised numerous concerns about the lack of security and privacy standards for personal information passing through the website. When asked whether Healthcare.gov had been compromised by hackers, one witness testified that he believed the website already has been hacked or soon will be. In addition, all of the witnesses agreed that Healthcare.gov is not secure. When the witnesses were asked if they would have launched the website, the unanimous answer was "No." Further, when the witnesses were asked if they would require front-end personal data disclosure on the site, again, all four responded "No." Lastly, each of the experts said taking down Healthcare.gov should be seriously considered to address the security concerns raised.

¹ House Committee on Science, Space and Technology hearing, "Is My Data on Healthcare.gov Secure," November 19, 2013, available at: <http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure>.

Congressional investigations into the flawed website have identified varying degrees of concern among those involved in developing the website prior to its launch last October. A Centers for Medicare and Medicaid Services (CMS) memo on the Federally Facilitated Marketplaces (FFM) System from September 3, 2013 noted that “[t]here is the possibility that the FFM security controls are ineffective,”² and that “[i]neffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise.”³ Later that month, a memo addressed to CMS Administrator Marilyn Tavenner stated, “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.”⁴ Further, a former senior security expert at CMS stated last month that she recommended against launching the Healthcare.gov website on October 1, 2013 because of “high risk security concerns.”⁵

Despite an improved ability for Americans to log on and create accounts in their search for healthcare plans since the flawed October 1st launch, it is unclear how much has been done to address the types of privacy and security concerns raised over the past few months. Since the data on Healthcare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies⁶ along with state agencies and government contractors, a security breach would be devastating to the millions of Americans forced by Administration regulations to enroll in health insurance plans through the website. Without proper security measures in place, participants are vulnerable to hackers who might be able to access such personal information, leaving them to deal with the consequences that come along with identity theft.

Issues

Target... and others

To understand what a potential data breach of the Healthcare.gov website could mean to the American public, it is useful to review the recent hacking of Target department stores’ online billing information. Initially, Target reported that “payment data was stolen from about 40 million customers”⁷ who shopped in its U.S. stores over the holiday season. But upon further review of the exposure, last week Target “revised the number of customers whose personal information was stolen...now reporting a range of 70 million to 110 million people.”⁸

² CMS Memo, “Authorization Decision for the Federal Facilitated Marketplaces (FFM) System,” available at: <http://oversight.house.gov/wp-content/uploads/2013/11/9.3.13-Trenkle.pdf>.

³ Ibid.

⁴ Memo to Marilyn Tavenner from James Kerr and Henry Chao, “Federally Facilitated Marketplace – DECISION,” September 27, 2013, available at: <http://www.scribd.com/doc/180332001/CMS-Memo-on-Marketplace-Security>.

⁵ House Oversight and Government Reform Committee press release, “CMS Officials Launched Healthcare.gov Against Warning Agency’s Top Cybersecurity Official,” December 20, 2013, available at: <http://oversight.house.gov/release/cms-officials-launched-healthcare-gov-warning-agencys-top-cybersecurity-official>.

⁶ 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>.

⁷ Elizabeth Harris and Nicole Perlroth, “For Target, the Breach Numbers Grow,” The New York Times, January 10, 2014, available at: http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0.

⁸ Ibid.

While original reports noted the theft of credit and debit cards as well as PIN data from bank ATM cards, the recent disclosure includes more personal information such as “mailing and email addresses, phone numbers or names, the kind of data routinely collected from customers during interactions like shopping online or volunteering a phone number when using a call center.”⁹

In a December 22nd letter to the Federal Trade Commission calling for an investigation of the Target breach, Senator Richard Blumenthal (D-Conn.) stated, “Those Target customers who have their data misused by hackers or thieves could lose their good credit and in turn their ability to purchase the goods and services they need for their wellbeing and the wellbeing of their families. Even customers whose stolen data will never ultimately be misused must live with the fear and uncertainty of knowing that it could be.”¹⁰

It is important to note that besides the Target data breach, media reports from this past weekend identified retailer Neiman Marcus as also experiencing network breaches over the holiday season.¹¹ Additionally, smaller “breaches on at least three other well-known U.S. retailers took place and were conducted using similar techniques as the one on Target.”¹²

Experian

The credit bureau and consumer data tracking service Experian provides “the identity verification component of the Health Insurance Marketplace enrollment process.”¹³

Experian also offers data breach services to companies through its Experian Data Breach Resolution arm. According to a recent Experian report, data breach incidents in the healthcare industry will rise in 2014 with the addition of the insurance exchange:

“With the addition of the Healthcare Insurance Exchanges, millions of individuals will be introduced into the healthcare system and in return increase the vulnerability of the already susceptible healthcare industry. When combined with new HIPAA data breach compliance rules taking shape, the healthcare industry is likely to make the most breach headlines in 2014.”¹⁴

⁹ Ibid.

¹⁰ Senator Richard Blumenthal press release, “In Response To Massive Data Breach, Blumenthal Calls For FTC Investigation Into Target Security Practices,” December 22, 2013, available at: <http://www.blumenthal.senate.gov/newsroom/press/release/in-response-to-massive-data-breach-blumenthal-calls-for-ftc-investigation-into-target-security-practices->

¹¹ Jim Finkle and Mark Hosenball, “Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks – Sources,” Reuters, January 12, 2014, available at: <http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112>.

¹² Ibid.

¹³ Experian website, “Information about Experian’s role in the Health Insurance Marketplace,” available at: http://www.experian.com/help/health-insurance-marketplace-verification.html?intcmp=hcinfo_hp.

¹⁴ Experian Data Breach Resolution, “2014 Data Breach Industry Forecast”, available at: <http://www.experian.com/assets/p/data-breach/experian-2014-data-breach-industry-forecast.pdf>.

GAO Report

Last month, the U.S. Government Accountability Office (GAO) released a report in which it reviewed issues related to personally identifiable information (PII) data breaches in the government.¹⁵ GAO reviewed the policies and procedures of eight federal agencies, including CMS, and determined that the agencies “inconsistently implemented”¹⁶ policies for “responding to a data breach involving PII that addressed key practices specified by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.”¹⁷

Further, according to the report, a “data breach can leave individuals vulnerable to identity theft or other fraudulent activity. Although federal agencies have taken steps to protect PII, breaches continue to occur on a regular basis. In fiscal year 2012, agencies reported 22,156 data breaches - an increase of 111 percent from incidents reported in 2009,”¹⁸ with 4,172 incidents reported at CMS.

Consequences of Stolen Identity

When a data breach occurs and an individual’s identity is stolen, then that information can be used to make purchases, obtain medical care, or for some other nefarious purpose. In 2013, 1.84 million Americans became victims of medical identity theft, with the total out-of-pocket cost incurred at \$12.3 billion.¹⁹ This cost included identity protection, legal counsel, and reimbursements to healthcare providers for fraudulent medical services. There is also a significant amount of time and effort spent on remedying the situation. In addition to the financial and time burden, in cases of medical identity theft, there is the risk that medical record inaccuracies created by an imposter may be unknown or may become permanent, potentially putting victims’ lives at risk.

One example of medical identity theft in the U.S. involves a woman named Anndorie Sachs. After receiving a phone call one day stating that her newborn baby had tested positive for drugs, authorities arrived at her house the next day threatening to take her other children away from her for being an unfit mother. In reality, Ms. Sachs had not given birth in years, but someone stole her information and had a baby under her name. Ms. Sachs had to take a DNA test to prove that it was not she who gave birth at the hospital, deal with the \$10,000 hospital bill, and live in fear over “the long-term damage that may have been done to her medical records.”²⁰

¹⁵ GAO report, “Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,” December 9, 2013, available at: <http://www.gao.gov/products/GAO-14-34>.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ Ponemon Institute, “2013 Survey on Medical Identity Theft,” available at: <http://medidfraud.org/2013-survey-on-medical-identity-theft>.

²⁰ Caitlin Johnson, “Protect Against Medical ID Theft,” CBSNews.com, October 9, 2006, available at: <http://www.cbsnews.com/news/protect-against-medical-id-theft>.

Chairman SMITH. The Committee on Science, Space, and Technology will come to order.

Welcome to today's hearing titled "HealthCare.gov: Consequences of Stolen Identity." I will recognize myself for an opening statement and then the Ranking Member.

When the Obama Administration launched HealthCare.gov, Americans were led to believe that the website was safe and secure. As the Science, Space, and Technology Committee learned at our hearing last November, this was simply not the case. We heard troubling testimony from online security experts who highlighted the many vulnerabilities of the Obama website. These flaws pose significant risks to Americans' privacy and the security of their personal information.

One witness, Mr. David Kennedy, who has been re-invited for today's hearing, testified that there are "clear indicators that even basic security was not built into the HealthCare.gov website." In addition, all four experts testified that the website is not secure and should not have been launched. Mr. Kennedy will update the Committee on the security of the website since November 30, 2013, which was the Administration's self-imposed deadline for when it would be fixed.

Since the November hearing, other events have emerged that prompted the need for today's hearing. In December, a former senior security expert at the Centers for Medicare and Medicaid Services stated that she recommended against launching the HealthCare.gov website on October 1st because of "high-risk security concerns."

A letter addressed to the Committee from Mr. Kennedy and independently signed by seven other security researchers who reviewed his analysis of vulnerabilities presents some very troubling information. To paraphrase one of the experts, Mr. Kevin Mitnick, who was once the world's most wanted hacker, breaking into HealthCare.gov and potentially gaining access to the information stored in these databases would be a hacker's dream. According to Mr. Mitnick, a breach may result in massive identity theft never seen before. Without objection, Mr. Kennedy's letter will be made a part of the record.

Chairman SMITH. Further, a recent report by the credit bureau and consumer data tracking service Experian forecasts an increase in data breaches in 2014, particularly in the healthcare industry. Specifically, the report states: "The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014. Add to that the Health Care Insurance Exchanges, which are slated to add seven million people into the healthcare system, and it becomes clear that the industry, from local physicians to large hospital networks, provide an expanded attack surface for breaches." Experian provides the identity verification component of the Health Insurance Marketplace enrollment process.

Because of increased accessibility to HealthCare.gov, concerns continue to grow about the security of personal information. The work of this Committee will help Congress make decisions about what actions may be necessary to further inform and safeguard the American people.

We are here today to discuss whether the Americans who signed up for healthcare plans have put their personal information at risk. If Americans' information is not secure, then the theft of their identities is inevitable and dangerous.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF CHAIRMAN LAMAR S. SMITH

When the Obama Administration launched Healthcare.gov, Americans were led to believe that the website was safe and secure. As the Science, Space, and Technology Committee learned at our hearing in November, this was not the case.

We heard troubling testimony from online security experts who highlighted the many vulnerabilities of the Obamacare website. These flaws pose significant risks to Americans' privacy and the security of their personal information.

One witness, Mr. David Kennedy, who has been re-invited for today's hearing, testified that there are "clear indicators that even basic security was not built into the Healthcare.gov website."

In addition, all four experts testified that the website is not secure and should not have been launched. Mr. Kennedy will update the Committee on the security of the website since November 30, 2013, which was the Administration's self-imposed deadline for when it would be fixed.

Since the November hearing, other events have emerged that prompted the need for today's hearing. In December, a former senior security expert at the Centers for Medicare and Medicaid Services stated that she recommended against launching the Healthcare.gov website on October 1st because of "high risk security concerns."

A letter addressed to the Committee from Mr. Kennedy and independently signed by seven other security researchers who reviewed his analysis of vulnerabilities presents some very troubling information.

To paraphrase one of the experts, Mr. Kevin Mitnick, who was once the world's most wanted hacker, breaking into Healthcare.gov and potentially gaining access to the information stored in these databases would be a hacker's dream. According to Mr. Mitnick, "A breach may result in massive identity theft never seen before."

Further, a recent report by the credit bureau and consumer data tracking service Experian forecasts an increase in data breaches in 2014, particularly in the healthcare industry. Specifically, the report states: "The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014. Add to that the Healthcare Insurance Exchanges, which are slated to add seven million people into the healthcare system, and it becomes clear that the industry, from local physicians to large hospital networks, provide an expanded attack surface for breaches."

Experian provides the identity verification component of the Health Insurance Marketplace enrollment process.

Despite increased accessibility to Healthcare.gov, concerns continue to grow about the security of personal information.

The work of this Committee will help Congress make decisions about what actions may be necessary to further inform and safeguard the American people.

We are here today to discuss whether the Americans who have signed up for health plans have put their personal information at risk. If Americans' information is not secure, then the theft of their identities is inevitable and dangerous.

Chairman SMITH. That concludes my opening statement, and the gentlewoman from Texas, Ms. Johnson, is recognized for hers.

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

Since we held our November 19th hearing highlighting security issues at HealthCare.gov, up to 110 million people have had their debit card or credit card information compromised by a hack of Target store records. But Target was not alone in being successfully hacked: The Washington Post, Facebook, Gmail, LinkedIn, Twitter, YouTube, Yahoo, JP MorganChase, SnapChat, and my friends at the Dallas-based Neiman Marcus stores have all announced security breaches.

However, do you know one system that has not been successfully hacked since the last hearing? HealthCare.gov. Also since the last hearing the Center for Medicare and Medicaid Services (CMS) staff and contractors have been working around the clock to improve the performance and security of HealthCare.gov. There have been numerous fixes to the website that have improved the site's responsiveness compared to its first 60 days. Millions of Americans have been able to access the site and obtain medical coverage.

During that entire time top security contractors, including Blue Canopy, Frontier Security and the Mitre Corporation have been working to test the system and identify weaknesses that need to be addressed. The Chief Information Security Officer has also been running weekly penetration tests to support security mitigation steps for CMS. Further, CMS says that none of the Majority's witnesses' concerns voiced in that November hearing have turned into any actual breach of security.

The last hearing did not feature a single witness who had any actual information about the security architecture of HealthCare.gov, nor what is being done to maintain the integrity of the website. Today, we have the same kind of hearing. As smart and experienced as these witnesses are, not one of them has actual knowledge of the security structure at HealthCare.gov. The best that they can do is speculate about vulnerabilities. I think it would be good for Members to remember that.

I am concerned that the intentions in this hearing appears to be to scare Americans away from the HealthCare.gov site. This appears to present a continuation of a cynical campaign to make the Affordable Care Act fail through lack of participation. While we are holding this hearing, both the House Oversight and Government Reform Committee and the Energy and Commerce Committee are holding similar events, all with the apparent goal to create a sense of fear, thereby manufacturing an artificial security crisis.

It is my hope that all of our witnesses can agree that it is important to make HealthCare.gov work for the American people to help give all our citizens access to affordable healthcare. I do not want to believe that any of the witnesses testifying today want the site to be hacked or shut down, or even see the program fail, or see Americans go without healthcare insurance.

This country faces a lot of real issues and real policy challenges. If we are truly interested in hacking and identity theft, we should have representatives of the largest retail institutions in the country here to discuss the challenges they face in protecting people's information. Instead, it appears that the Majority has allowed the Com-

mittee to become a tool of political messaging to a degree that I have never witnessed any time in my time in Congress, and I am in my 22nd year.

Thank you. I hope that the Committee hearing will be the last of this topic, absent some actual allegations of wrongdoing, so that we can focus on legitimate oversight issues facing the country and this Committee.

Mr. Chairman, before I yield, I would also like to comment on the letter you want to put in the record. I was hoping after reading it that you would have some testimony or give the people opportunity other than a 24-hour showing of this letter, but you don't have to take my word on this. Mr. Kennedy's own document reads, this report is for public use. The report is not appended to his testimony, and I imagine it was not added because it would violate our 48-hour rule. He did not give us testimony in time but late yesterday afternoon presented this report out of the blue, and I am guessing your counsel told him to make it a letter because we routinely accept outside letters from groups and experts all the time with minimal notice.

So the report now pretends to be a letter addressed to you and to me. However, I cannot remember another time that a witness for the Committee also felt they had to write us a letter. I think it is an elaborate way to try to get testimony before the Committee in violation of the 48-hour rule.

As the substance of the report, it includes what amounts to testimony from experts who are not appearing before this Committee and is against the practice of the Committee to accept testimony from people who are not personally available to answer our questions.

The one thing I do know is that none of the individuals who signed these statements in the packet have worked on HealthCare.gov or the security protocols behind the website. In other words, they know no more about the actual security of the site than does Mr. Kennedy. In deference to the Chairman, I will withdraw my objection but I would point out that this report includes language that I consider vulgar and beneath the dignity of the Committee. That alone should be reason to keep it out.

Even if the Chairman is comfortable with the way our rules are being stretched, if you insist, I will withdraw, but I want the record to reflect that we have gone beyond professional behavior of this Committee. Thank you.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF RANKING MEMBER EDDIE BERNICE JOHNSON

Since we held our November 19th hearing highlighting security issues at healthcare.gov, up to 110 million people have had their debit card or credit card information compromised by a hack of Target store records. But Target was not alone in being successfully hacked: The Washington Post, Facebook, Gmail, LinkedIn, Twitter, Youtube, Yahoo, JP MorganChase, SnapChat, and my friends at the Dallas-based Neiman Marcus stores have all announced security breaches.

However, do you know one system that has not been successfully hacked since that last hearing? Healthcare.gov.

Also since the last hearing the Center for Medicare and Medicaid Services (CMS) staff and contractors have been working around the clock to improve the performance and security of healthcare.gov. There have been numerous fixes to the website

that have improved the site's responsiveness compared to its first 60 days. Millions of Americans have been able to access the site and obtain medical coverage.

During that entire time top security contractors, including Blue Canopy, Frontier Security and the Mitre Corporation, have been working to test the system and identify weaknesses that need to be addressed. The Chief Information Security officer has also been running weekly penetration tests to support security mitigation steps for CMS.

Furthermore, CMS says that none of the Majority's witnesses concerns voiced in that November hearing have turned into any actual breach of security.

The last hearing did not feature a single witness who had any actual information about the security architecture of healthcare.gov, nor what is being done to maintain the integrity of the website. Today, we have the same kind of hearing. As smart and experienced as these witnesses are, not one of them has actual knowledge of the security structure at healthcare.gov. The best that they can do is speculate about vulnerabilities. I think it would be good for Members to remember that.

I am concerned that the intention of this hearing appears to be to scare Americans away from the healthcare.gov site. This represents a continuation of a cynical campaign to make the Affordable Care Act fail through lack of participation. While we are holding this hearing, both the House Oversight and Government Reform Committee and the Energy and Commerce Committee are holding similar events. All with the apparent goal to create a sense of fear, thereby manufacturing an artificial security crisis.

It is my hope that all of our witnesses can agree that it is important to make healthcare.gov work for the American people to help give all our citizens access to affordable health care. I do not want to believe that any of the witnesses testifying today want the site to be hacked or shut down, or see the program fail, or see Americans go without medical insurance.

The country faces a lot of real issues and real policy challenges. If we are truly interested in hacking and identity theft, we should have representatives of the largest retail institutions in the country here to discuss the challenges they face in protecting people's information. Instead, it appears that the Majority has allowed the Committee to become a tool of political messaging to a degree I have never witnessed in my time in Congress.

Thank you, I hope that today's hearing will be the last on this topic, absent some actual allegations of wrongdoing, so that we can focus on all the legitimate oversight issues facing the country and this Committee.

Chairman SMITH. I will recognize myself to respond to the Ranking Member's comments.

All Committees, including this one, have a longstanding practice of affording Members the courtesy of entering items that they believe are relevant to the topic at hand into the record. I am sure the Ranking Member knows this. Members on both sides have generally approached the development of the record in the spirit of bipartisanship and comity. I am disappointed if the gentlewoman from Texas would now seek to question a letter I have asked to place in the record. We frequently place items in the record that express the opinion of various groups or make statements regarding an issue at the request of Members on both sides of the aisle. Often, those who have written those letters are not testifying before the Committee and have not been asked to do so, yet their opinions are still made part of the record.

One such example is a 54-page submission that Mr. Maffei requested be placed in the record at a hearing last August. This document, which was not even addressed to the Committee, but instead to the Administrator of the EPA, was entered into the record without comments. It includes a letter from six different tribes signed by eight different people, none of whom testified before this Committee. It includes a letter from a lawyer who represented the tribes. He also did not testify before the Committee, yet we made his letter a part of the record. Finally, it includes another letter to the Administrator of the EPA that purports to be from 15 different national organizations, 17 international organizations, 75 Alaskan organizations, and numerous other organizations from other states. None of these organizations testified before this Committee.

I placed Mr. Kennedy's letter in the record here today. He is testifying before us shortly—

Ms. EDWARDS. Mr. Chairman.

Chairman SMITH. —and Members will have the opportunity to question him on its contents.

Ms. EDWARDS. Mr. Chairman.

Chairman SMITH. I am still in the middle of my statement.

I regret the Ranking Member has questioned the longstanding prerogative of a Member to enter a relevant document into the record, especially when Members on her side of the aisle have done so many times without objection from the Majority.

I hope this is not indicative of her desire to make this Committee's business more partisan.

That concludes my statement, and I will now introduce the witnesses.

Ms. EDWARDS. Mr. Chairman.

Chairman SMITH. I am going to introduce the witnesses, and—

Ms. EDWARDS. Mr. Chairman, I object to the entry of the letter into the record.

Chairman SMITH. The letter has already been entered into the record and the objection is not timely.

Ms. EDWARDS. Mr. Chairman, I would ask for a vote on whether we enter the letter into the record.

Chairman SMITH. That is no longer a proper motion because it is not timely.

Ms. EDWARDS. Well, Mr. Chairman, I think you have deeply politicized this hearing.

Chairman SMITH. Well, I am sorry for the Ranking Member's comments that caused it, and now I will recognize and introduce our first witness.

Mr. David Kennedy is the President and CEO of TrustedSEC LLC. Mr. Kennedy is considered a leader in the security field. He has spoken at many conferences worldwide including Black Hat, DefCon, Infosec World and Information Security Summit, among others. 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.

Our second witness, Mr. Waylon Krush, is the Co-Founder and CEO of Lunarline. He is also a founding member of the Warrior to Cyber Warrior program, a free six month cyber security boot camp for returning veterans. A veteran of the U.S. Army, Mr. Krush is a recipient of the Knowlton Award, one of the highest honors in the field of intelligence. Mr. Krush holds a Bachelor's degree in computer information science from the University of Maryland University College. He is also a certified information systems security professional, certification and accreditation professional, certified information systems auditor, and has more than 3,000 hours of training with the National Cryptologic School.

Our third witness, Mr. Michael Gregg, is the CEO of Superior Solutions Inc., an IT security consulting firm. Mr. Gregg's organization performs security assessments and penetration testing for Fortune 1000 firms. He has published over a dozen books on IT security and is a well-known security trainer and speaker. Mr. Gregg is frequently cited by print publications as a cyber security expert and as an expert commentator for network broadcast outlets such as Fox, CBS, NBC, ABC and CNBC. Mr. Gregg holds two Associate's degrees, a Bachelor's degree and a Master's degree.

Our final witness, Dr. Larry Ponemon, is the Chairman and Founder of the Ponemon Institute, a research think tank dedicated to advancing privacy, data protection and information security practices. Dr. Ponemon is considered a pioneer in privacy auditing and was named by Security magazine as one of the most influential people for security. Dr. Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy, data protection and cyber security including financial services, healthcare, pharmaceutical, telecom and Internet. Dr. Ponemon earned his Master's degree from Harvard University and his Ph.D. at Union College in Schenectady, New York. He also attended the doctoral program in system sciences at Carnegie Mellon University.

We welcome you all and look forward to your expert testimony, and Mr. Kennedy, will you lead us off?

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

Mr. KENNEDY. Thank you, Mr. Chairman.

Good morning to everybody in the House Science and Technology Committee, to the Honorable Mr. Smith as well as the Ranking Member of the House Science and Technology Committee, the Honorable Ms. Johnson. It is great to see you two folks again as well as all of the other Ranking Members here today. I appreciate your time to hear us discuss the issues with the HealthCare.gov security concerns as well as the consequences around stolen identities.

What I want to first start off with is that to me, this is not a political issue. I take no political-party stance and I have no party affiliate. For me personally, this is a security issue. Working in the security industry for over 14 years including working for the National Security Agency as well as spending a number of years in Iraq and Afghanistan, my testimony here today is to talk about the issues with security, and that is it. So when I talk about the issues that we see here today, it is based on my expertise of working in the security industry, doing these assessments on a regular basis, being a chief security officer for a Fortune 1000 company for a number of years as well as running my own company.

And I am not alone. The mention of the document that was released yesterday had seven independent security researchers that are well known in the security industry including a number of folks that have worked for the United States government, do training for the United States as well as work closely with the United States government. Today is not to talk about the political-party problems with it but also discuss just the security issues alone, and that is what I am here to talk about today.

So I would like to give thanks to Kevin Mitnick, Ed Skoudis, Chris Nickerson, Chris Gates, Eric Smith, John Strand and Kevin Johnson for providing their comments on the issues that we see today. We are pretty unified in our approach. Everybody that I shared with, I put them under non-disclosure agreements and worked with them, and the consistent feedback that we got was that HealthCare.gov is not secure today, and nothing has really changed since the November 19th testimony. In fact, from our November 19th testimony, it is even worse.

Additional security researchers have come into play, providing additional research, additional findings that we can definitely tell that the website is not getting any better. In fact, since the November 19, 2013, testimony, there has only been one-half of a vulnerability that we discovered that has been addressed or even close to being mitigated. When I say but one-half is that basically they did a little bit of work on it and it is still vulnerable today.

I want to throw a disclaimer out there that in no way, shape or form did we perform any type of hacking on the websites. That is a misnomer. The type of techniques that we used is looking at the site from a health perspective, doing what we call passive reconnaissance, not attacking the site in any way, shape or form, not sending data to the site but really looking at the health of it. I would like to put in another analogy. Say my expertise wasn't being in the security industry, it wasn't anywhere near doing anything security related and I was a person that was a mechanic. I had 14 years of being a mechanic. And, a car drove past me that was puffing blue smoke out of the muffler, it was leaking oil, the engine was making clinking sounds, and basically a lot of sympto-

matic problems: the doors are open, the windows are open and everything else. As a mechanic, I can probably say with a reasonable level of assurance that the engine probably has some issues. Same thing with technology and Web applications. Web applications are no different than a car with an engine problem. There are a lot of pieces that make the car work. There are a lot of pieces that make a website work.

From our testimony here today as well as what we have discovered in the past, there is a number of security issues that are still there today with the website. To put it in perspective, I would like to put for the record that there wasn't 70 to 110 million credit cards taken from Target. That is not accurate. The correct statistic is that there were 70 to 110 million personal pieces of information taken about individual people that shopped at Target. There were 40 million credit cards that were taken. The issue with Target isn't specifically around credit cards. Credit cards can be reissued. Your credit that gets taken from the credit cards can be debited back into your account. You are not liable as a consumer. But what you can't fix is your personal identity. If you look at Target, for example, the 70 to 110 million personal pieces of information, that includes address, email addresses, phone numbers, additional information. That is what you can't replace, and we have already seen a number of individuals that are selectively being targeted from a personal information perspective because of that. That doesn't even include Social Security numbers. In fact, I just had another independent security person get targeted yesterday from an email claiming to be Target. As soon as they clicked the link, it hacked their computer and took full control of it.

So this issue here doesn't relate specifically to just credit card data because that is obviously not in the HealthCare.gov website. The personal information around Social Security numbers, first name, last name, email addresses, home of record, those are all a recipe for disaster when it comes to what we see from personal information being stolen and theft. So it is not just that. As an attacker, if I had access to the HealthCare.gov infrastructure, it has direct integration into the IRS, DHS as well as third-party providers as well for credit checks. If I have access to those government agencies, I now can complete an entire online profile of an individual, everything that they do and their entire online presence.

And this isn't just HealthCare.gov alone. I am not trying to single out HealthCare.gov alone. I am really focusing on a much larger issue, which is security in the federal government alone is at a really bad state. We need to really work together to fix it and work on more sweeping changes. Thank you.

[The prepared statement of Mr. Kennedy follows:]



Healthcare.gov Testimony Update
Congressional Hearing January 16, 2014
"Healthcare.gov: Consequences of Stolen Identity"

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 web site.

The Honorable Lamar Smith, Chairman of the House Science, and Technology Committee
The Honorable Eddie Bernice Johnson, Ranking Member of the House Science and Technology Committee

To Mr. Smith and Ms. Johnson,

January 14, 2013

I testified in front of this committee on November 19, 2013 to discuss alarming issues with the healthcare.gov web site. The purpose of the hearing was to discuss possible threats regarding security on the healthcare.gov web site, the amount of integration the web site performs, and to what it has access. I appreciate the time and effort involved in having me back to discuss the implications of what a large breach on the healthcare.gov web site would look like.

Since the last testimony, a number of other security researchers have provided me with additional exposures that are far more expansive than the ones I had originally stated as well as some alarming trends that I would like to discuss with the committee. Additionally, I do not believe healthcare.gov is alone regarding the security threats and vulnerabilities on federally run web sites.

This is a much larger problem than just healthcare.gov and should be looked at in a much broader view than just one web site infrastructure. In stating this, I am not aware of another web site such as healthcare.gov that has the vast amount of access to multiple government agencies and tight integration with several federal systems. It is still my opinion that healthcare.gov poses a significant risk to personal information of U.S. citizens and that the security issues raised have still not been addressed appropriately nor effectively.

Contained in this document is additional information on direct exposures to healthcare.gov as well as opinions on future strategies for working to promote better information security not just with healthcare.gov, but the federal government in general.

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 HEALTHCARE.GOV EVOLUTION	4
3.0 MONITORING AND DETECTION CAPABILITIES	5
3.1 SHORT-TERM OBJECTIVES	6
3.2 MID-TERM OBJECTIVES	6
3.3 LONG-TERM OBJECTIVES	7
4.0 END-TO-END TESTING	7
5.0 RECOMMENDATIONS FOR HEALTHCARE.GOV	10
5.1 QUICK-FIXES ON SECURITY RISK	10
5.2 DEVELOP THE SECSDLC PROCESS	10
5.3 MONITORING AND DETECTION	10
5.4 END-TO-END TESTING	10
6.0 LONG-TERM FEDERAL SECURITY ADOPTION	11



1.0 Executive Summary

On November 19, 2013, David Kennedy testified with a number of other scholars, security researchers, and experts in their retrospective areas. The purpose was to discuss the security threats towards the healthcare.gov web site and its supporting infrastructure. Since the November meeting, there has been a half of one issue fixed (vulnerability still present with fix is easily bypassed) of the 18 issues identified through passive reconnaissance. Some issues still include critical or high-risk findings to personal information or risk of loss of confidentiality or integrity of the infrastructure itself. In addition, a number of other security researchers have contacted me regarding additional security exposures that have been identified and reported which also have not been fixed. These include JSON injection, Un-sanitized URL redirection, mass user information enumeration (name, email, login ID, etc. in bulk), user profile disclosures, cookie theft, exposed sensitive API's, and others. One of the more alarming is the ability to access anyone's eligibility reports on the website without the need for any authentication or authorization.

Please note that TrustedSec is not disclosing these exposures as they are still active and present a risk to the integrity of the web site. TrustedSec will release the exposures that have already been addressed and pose no risk to personal information or risk of loss of integrity of the system. In addition, under no circumstance did TrustedSec perform any form of "hacking." All information was gathered through purely passive reconnaissance and enumeration of information that is already available on the Internet (Google). If these exposures exist without actually attacking the site, there is serious question as to the integrity of the system itself and its back-end infrastructure.

TrustedSec cannot state with one hundred percent certainty that the back-end infrastructure is vulnerable, however based on our extensive experience performing application security assessments for over ten years; the web site has the symptoms that lead to large-scale breaches for large organizations. Also note that all exposures have been reported and TrustedSec would be more than willing to have discussions with HHS to address the security concerns.

TrustedSec's opinion still holds strong that the web site fails to meet even basic security practices for protecting sensitive information of individuals and does not provide adequate levels of protection for the web site itself. This opinion is not unique, as other security researchers such as Bob Rich did extensive reconnaissance on the web site and notified multiple areas of the federal government without response. Additionally, a second researcher Scott White from TrustedSec also worked on the discovery of what we know today on healthcare.gov. At this time, the risk is still present at healthcare.gov and there has been little effort to address the concerns identified by multiple security researchers. The healthcare.gov security threats demonstrate a much larger problem for the federal government in general. The lack of formal security testing and proactive security measures to which to adhere in the federal government is alarming.

It is accurate that no system can ever remain one hundred percent protected against threats, however it is possible to make compromise of the site extremely difficult, protect the information, and detect the attacks as they happen. Additionally, in the event of a compromise, protecting the



sensitive data through appropriate access control and monitoring can also inhibit lapses in security. Immediate action must be taken in the federal government to protect sensitive information and remain competitive with other nations. TrustedSec has a section dedicated to the recommendations for the federal government for moving forward and hopes that the testimony on the 16th can lead to better proactive practices around information security and sweeping changes in how contractors are selected in the federal space. This opinion is not TrustedSec's alone; the Government Accountability Office released a document in December 2013 documenting Information Security concerns and responses to breach of PII and a lack of consistency (<http://www.gao.gov/assets/660/659572.pdf>).

2.0 Healthcare.gov Evolution

In the testimony on November 19, 2013 and under the written testimony from TrustedSec (http://www.trustedsec.com/files/CONGRESS_Hearing_HealthCareSEC_FINAL_v1.1.pdf), there were three options presented for fixing the current security threats to healthcare.gov. TrustedSec highly recommended option one which was developing a "version 2.0" in conjunction with the running site and releasing a more stable product that incorporated security into the Software Development Lifecycle (SecSDLC). During the actual testimony, it was also mentioned that shutting the website down and starting from scratch is another option. During the November testimony the web site was continuously crashing with intermittent delays and bugs rendering the site ineffective. At the time, this may have been the best option rather than keeping it up and running. Although it appears that the site is still experiencing some issues, the web site seems to be more stable.

TrustedSec still recommends developing a version 2.0 in conjunction with the current site, however there is inherent risk in this approach. The site is currently vulnerable which is evident and highly clear at this point. Immediate action for the time being to patch the existing flaws should be considered while developing a "2.0" future strategy for healthcare.gov with security integration. Additionally, it was recently disclosed that CGI is no longer the contractor performing updates or new rollouts of the website and that Accenture has been selected to perform future updates and rollouts of the website (<http://politicalticker.blogs.cnn.com/2014/01/11/white-house-awards-accenture-healthcare-gov-contract/>). It should be noted that Accenture is an extremely large organization such as CGI and should focus on proactive security measures for protecting the site. Accenture also developed the California state exchange, which has significantly more exposures currently than the healthcare.gov web site (presently).

Two researchers, Matt Ploessel and Kristian Hermansen, disclosed hundreds of exposures on the web site including some of the worst types of application flaws in today's hacking scene. This included the ability extract over 500,000 user's personal information as well discovery of 50 SQL Injection flaws, Cross-Site Scripting, and hundreds of other flaws. A video demonstration was created by the security researchers and can be found here: (<https://docs.google.com/file/d/0B75Y2Pg4wn1RcmtEWnFENFdoaWc/edit>). The researchers have been working on remediation efforts with CERT (cert.org) who has been extremely responsive



and helpful in notifying California of the exposures. With the existing vulnerabilities on the California state exchange, the Federal government should be concerned with future development on the healthcare.gov web sites and ensure appropriate testing.

3.0 Monitoring and Detection Capabilities

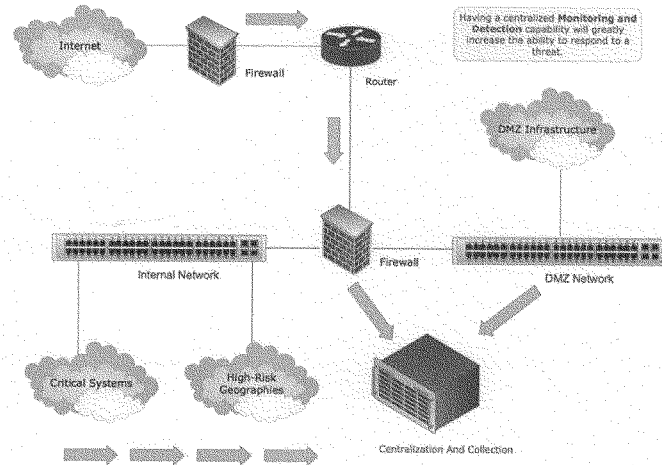
A memo released on December 13, 2013 from the Committee on Energy and Commerce from Reps. Henry A. Waxman, and Diana DeGette detailed that the healthcare.gov web site had only "a total of 32 Healthcare.gov Information Security Incidents" (<http://democrats.energycommerce.house.gov/sites/default/files/documents/Memo-ACA-Security-Briefing-2013-12-13.pdf>). No less than a month before that testimony to Congress stated that the security operations center which would detect these types of attacks hadn't yet been completed or started (<http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Amsler-OI-ACA-Healthcare-Website-2013-11-19.pdf>). This first shows that monitoring and detection capabilities hadn't even been created or started prior to the launch of the healthcare.gov web site, and had not started by November 19th, 2013. It is possible that there had only been only 32 "Information Security Incidents" detected, but only due to the lack of advanced capabilities of actually detecting attacks on the web site. Monitoring and detection is not just the creation of automatic rules for firewalls or other technologies, its understanding how attacks look and being able to respond to them with a formal incident response capability.

TrustedSec has documented below a detailed phased rollout of monitoring and detection capabilities:

Recommendation:

TrustedSec has detailed recommendations on developing the monitoring and detection capabilities for the healthcare.gov infrastructure. What TrustedSec finds is by early warning indicators and blocking an attacker in the early stages of an attack, an infrastructure can better handle threats towards an infrastructure and minimize the damage. TrustedSec has created a diagram of the standard flow of information, which incorporates the highest risk areas for an organization to protect. INFOSEC cannot protect everything within an environment, but having detection capabilities on the critical pieces of an infrastructure can better reduce a large exposure.





Note that the above is just an example of a centralized approach to monitoring and detection capabilities. High-risk geographies may be entry points into other government agencies, and the protection of places where personal identifiable information (PII), sensitive data, and/or intellectual property reside.

3.1 Short-Term Objectives

In the short-term objectives, developing specific use-cases that can help better detect as well as triaging the current (if any) security assessments to better develop monitoring and detection capabilities should occur. Additionally, standing up a formal security operations center, which was noted back in the November testimony, would be highly beneficial for the detection of attacks.

3.2 Mid-Term Objectives

As the monitoring and detection program continues to expand to the entire infrastructure, it will continue to need tweaks and additions in order to better gain visibility into the organization. This could be getting more visibility into web applications or backend databases, but ultimately the goal is to develop a central repository where all information resides and detect anomalies in the network. The mid-term objectives are primarily focused on once the short-term objectives have been accomplished. The strategy around the mid-term objectives is to further expand the reach of the monitoring and detection program. Initially the focus is basic attacks but grows to more advanced and targeted attacks.



Secondly, focusing on enhancing the overall detection capabilities in new and different types of attack vectors would be desirable in this phase.

3.3 Long-Term Objectives

A monitoring and detection program is a continual program that requires adequate testing and continuous monitoring. Most organizations fail to staff accordingly to identify threats. A monitoring and detection program is one of the most important areas of an information security program as it is the last line of defense if an attacker has circumvented the security controls you have in place and has access to the organization.

Once the short and mid term objectives are complete – a larger focus on continual expansion for full coverage of the architecture should be considered. This would include having full monitoring and detection capabilities across the entire infrastructure. This type of detection ratio will give full visibility in the different anomalies and patterns of attack within the organization. While it may not be applicable to address every system within the organization, key strategy points of attack and the identification of those will be the most challenging part of the deployment plan. As the monitoring and detection program expands, there will need to be considerations on places where detection does not make sense. Most specifically if short and mid term objectives were completed, this would be more of a maintenance and addition of systems versus rapid expansion.

4.0 End-To-End Testing

Appropriate security testing on the healthcare.gov web site and its supporting infrastructure was not fully completed by MITRE (<http://abcnews.go.com/blogs/politics/2013/12/exclusive-security-risks-seen-at-healthcare-gov-ahead-of-sign-up-deadline/>) and contained significant exposures, which had a long-term remediation date (late 2014 and 2015). This is apparent through testimony and documents released

Testimony from Teresa Fryer, the Chief Information Security Officer at CMS (<http://oversight.house.gov/release/cms-officials-launched-healthcare-gov-warning-agencys-top-cybersecurity-official/>) - "told the House Oversight and Government Reform Committee during a transcribed interview that, even after a launch she refused to support, her agency continues to find security problems that threaten the privacy of user information, contradicting administration officials' statements that the site has been continually secure."

It was also indicated that Fryer recommended against the October 1st 2013 deadline "Fryer, citing high risk security concerns, recommended against the October 1, 2013, launch of HealthCare.gov due to security test results that administration officials have furiously fought to keep out of the public view. Fryer told Committee staff that she recommended "a denial of an [Authority to Operate] ATO" for HealthCare.gov to the top IT officials at CMS and the Department of Health and



Human Services (HHS) days before the website launched. Fryer made the recommendation on September 20, 2013, "during the security testing when the issues were coming up about the availability of the system, about the testing in different environments." Asked by Committee investigators, "Did you make it clear that you were not agreeing with the decision to for the ATO when you signed this document [an acknowledgement of risk that noted a mitigation plan on September 27]?", Fryer responded affirmatively."

From the evidence presented in the public as well as the research from TrustedSec and independent security researchers, security best were not followed and continue to not be followed in the development of the healthcare.gov web site and its supporting infrastructure. In order for a deployment to be successful and to adequately protect the information and the integrity of the web site, security must be integrated in the very early stages of the application development and through the software development lifecycle. It is extremely difficult to go back after the fact and place small patches and fixes on the system in order to repair inherently flawed software and architectural designs.

In order for an Software Development Lifecycle (SDLC) process to work appropriately and to ensure no new risks are introduced, it is vital that adequate security testing is performed. This should be a combination of source code analysis as well as dynamic testing of the application (testing different use cases). Below is a description of the SDLC process with descriptions of each of the different steps within the security SDLC (SecSDLC).

The process for integration in security requires the ability to work with the SDLC in multiple areas. The first is during the initial requirements analysis phase, which begins to bring in inputs from multiple areas. In this phase, it may be additional functionality for an existing application or it could be a completely new application. In this process, security needs an understanding of what the application is, how it will function, and what type of application this will be (based on sensitive data, regulated, IP, etc.) and the risk associated with it.

The design phase is an important process both architecturally as well as programmatically. TrustedSec recommends utilizing the Open Web Application Security Project (OWASP) as a foundation for secure coding practices. When designing the application and performing programming, ensuring that the foundation is built from security early on will ensure that risks aren't introduced into the application during the design process.

When building and implementing the application, ensuring that all security components are in place and that any additional required security measures need to be implemented would occur during this phase. This could be additional technologies such as monitoring and detection capabilities, web application firewalls, or additional controls to ensure the protection of the application based on risk.



The testing phase is one of the most important steps of the whole process. When performing testing on the application, a combination of source code analysis as well as dynamic testing should be performed. This would include testing specific use cases and the business logic of the applications to ensure that there haven't been any major exposures created through the SDLC process. This phase is the most important because it should catch any mistakes or problematic code that may have been introduced in prior phases.

Lastly the evolution phase is enhancements to the application that should undergo the same type of process for security testing. In most cases, visual enhancements (not features) wouldn't require a security review however, when adding new functionality or features, the testing should be quick to identify what exposures that may have been introduced to the web application.

A solid standard for understanding application security is the Open Web Application Security Project (OWASP) as a framework and understanding secure code. OWASP contains a number of best practices on secure coding as well as proper programming techniques. OWASP is the largest consortium of open-source application security community in existence. TrustedSec recommends adopting OWASP as a framework for healthcare.gov.

Lastly, Application Security isn't the only measure to protect an organization. It relies on a functioning information security program that ensures adequate controls are in place to protect an infrastructure such as healthcare.gov. End-to-end testing needs to be performed at this very moment to identify what the risk level is currently with the healthcare.gov infrastructure. This would include source code analysis, penetration testing, risk assessments, and architectural reviews in order to understand the current risk associated with the overall healthcare.gov system. From there, a roadmap to remediation and action plan to address the risk accordingly should be developed. TrustedSec highly recommends this be performed immediately and by an independent research company.



5.0 Recommendations for Healthcare.gov

A number of recommendations have already been presented in this document; this section is dedicated to summarizing them or adding additional recommendations not covered in this report.

5.1 Quick-fixes on security risk

Fix the current security problems on the web site, which pose a high or critical risk to the confidentiality or integrity of the infrastructure. Develop a "2.0" version which incorporates the new Security Software Development Lifecycle (SecSDLC) process and ensures appropriate end-to-end security testing.

5.2 Develop the SecSDLC Process

Develop the SecSDLC process that focuses on proactive security measures for protecting the information and infrastructure on healthcare.gov.

5.3 Monitoring and Detection

Develop a security operations center and ensure effective controls are in place to monitor attacks against the healthcare.gov infrastructure and supporting sites.

5.4 End-To-End Testing

Perform end-to-end testing to benchmark the existing risk towards the healthcare.gov infrastructure and take appropriate action to reduce the risk as appropriate and acceptable.



6.0 Long-Term Federal Security Adoption

As mentioned earlier, the federal government isn't known for having super secure web sites or even having adequate security to protect U.S. related sensitive data. More sweeping legislature is needed to put the federal government into the 21st century regarding security and technology. This stems from the initial contracting and developing process of any new contract as well as ongoing security measures. Recently the House of Representatives passed a bill (<http://democrats.energycommerce.house.gov/sites/default/files/documents/Bill-Text-HR-3811-Health-Exchange-Security-and-Transparency-2014-1-3.pdf>) that would require breach disclosure in the event of a loss of personal identifiable information (PII). In addition, a bill was drafted by Congresswoman Black which was similar (<http://black.house.gov/sites/black.house.gov/files/Federal%20Exchange%20Data%20Breach%20Notification%20Act%20of%202013.pdf>).

While this is a start and a good step forward, the problems don't solely reside on healthcare.gov. There needs to be an even broader effort to include the entire federal government. 49 states currently have breach disclosure laws for personally identifiable information and the same should be proposed in the federal space as well. Additionally, while healthcare.gov contains no actual Patient Healthcare Information (PHI), acts such as the Health Insurance Portability and Accountability Act (HIPAA) should be extended to the federal government as well.

Also in the security community is someone highly respected, Alex Hutton, who proposed establishing a function for the Center for Disease Control and Prevention (CDC) with oversight for Information Security related issues and the enforcement of information security best practices. This would be a central point in the United States government that could communicate with the public on information security related issues as well as ensure a governance structure around adequate security measures in the federal government.

Alex Hutton was quoted in saying directly to TrustedSec "Typically, when our government has needed to rely on the practices of the industry to ensure the safety of its citizens, there has been some oversight function. The CDC, NTSB, FDA, EPA, SEC, etc. have all been created to ensure that industry is serving the greater good of the citizens. In many cases, in order to understand the right policy - these organizations have needed to collect data and conduct research.

The time has come for similar oversight in the cyber arena. Much of our critical infrastructures and economy depend on organizations operating safely in cyberspace. As such, the United States Government has the same (if not greater) interest in understanding the outbreaks and causes of incidents in cyberspace as they do for the nature and spread of diseases, food-borne



illness, or the root causes of airline accidents. A National Cyber Safety Center can help business prevent, detect, and respond to serious cyber threats - creating a resilient national infrastructure."

TrustedSec supports this approach and believes that in a time where breaches are occurring in both the public and private sector, there has never such a prime opportunity as now to protect assets of the federal government and its people from attack.

Lastly, TrustedSec recommends a unified approach for disclosing flaws within government web sites or a "bug bounty" program that allows the centralization of bug one central place. This would be similar to what Katie Moussouris has established at Microsoft with the bug bounty program, which invites security researchers to find flaws and disclose them to help better the product. Microsoft is an excellent example of an entity that has established a program that meets and exceeds even industry norms.





TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

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.
Mr. Krush.

**TESTIMONY OF MR. WAYLON KRUSH,
CO-FOUNDER AND CEO, LUNARLINE, INC.**

Mr. KRUSH. Chairman Smith, Ranking Member Johnson and Members of the Committee, thank you for this opportunity to testify on the important topic of cyber security.

I am Waylon Krush, Founder and CEO of Lunarline. We are one of the fastest-growing cyber security companies. I am also a founder of the Warrior to Cyber Warrior program, as stated earlier.

I have been asked to speak on cyber security today as it relates to HealthCare.gov, and just listening to Mr. Kennedy, I actually have some very simple points I want to make right away.

First of all, if none of us here built HealthCare.gov, if we are not actively doing not a passive vulnerability assessment but an active vulnerability assessment and doing penetrations and running that exploitable code on HealthCare.gov, we can only speculate whether or not those hacks will work. So anything that has been said thus far, if we are talking about any type of dot gov or dot mil site just identifying passively a vulnerability and not actually working on the site, knowing how the protocols work in the back end, what type of defense in depth, how each one of the assets are locked down, nobody here at this table can tell you that they know that there is vulnerabilities.

Another thing I would like to talk about today is in the federal government, something a little bit different than we have in the commercial organizations is, we use something called the risk management framework, and you know, this Committee has actually helped develop that as part of NIST, and I will tell you, that is one of the most rigorous processes as it relates to cyber security and privacy in the entire world, and when I say the entire world, most security standards are just a subset of the risk management framework. It is one of those areas from a security control perspective that has been taken to build other security standards or it is basically copy, cut, pasted to create new security standards. This is a six-step process. It includes categorization, selection, implementation, validation, authorization and, most importantly, continuous monitoring of all the controls. You know, just looking at it, you might think well, there is about 360 controls in NIST Special Publication 800-53, revision 4. When you dig a little bit deeper, there is actually several thousand information security controls that our federal information systems must undergo from a security architecture perspective including they must be continuously testing.

Another point I would like to make is that if anybody here actually went out to these websites, and I am not talking about passive, but if we have extracted addresses, if you went to the website and done anything outside the bounds of what is allowed in the federal government, you are basically breaking the law. You can't just go out and say I found this vulnerability and then exploit it to try to get, you know, media attention or anything like that. If you do that, you are breaking the law. It is pretty simple.

And last but not least, you know, HealthCare.gov is one of many hundreds or even thousands of federal information systems out

there in websites, and you know, I have worked in the threat area. I can tell you, my background is not only a soldier but was on the U.S. Army's Information Operations Red Team, Blue Teams, information system security monitoring teams, protocol analysis, signals analysis, and including working in critical infrastructure protection for AT&T for a few years all across the world. If you go out and tell someone—and this is just the truth when we are out actively taking down websites—I can sit here all day and speculate about a vulnerability but until I have actually exploited that vulnerability, there is no way to tell whether that attack will actually work. There is a lot more going on in the background that everybody needs to understand.

Another note, and last but not least, about HealthCare.gov that everyone needs to understand is that with all of the media attention it is currently getting, you would think it is most high payoff target in the entire federal government. You would think that HealthCare.gov is something that everybody would want to go after. That is truly—that is media spin, if anything. HealthCare.gov is one of many websites that have personal information in it. It is connected to other systems but saying it is interconnected directly to all these systems and that leaves them vulnerable also shows kind of a lack of knowledge of the backend system capabilities, meaning that those connections are very secure and they are authorized on both sides.

And you know, I have actually been lucky enough to work within CMS and HHS on cyber security deployments and configurations so out of everybody here at least at this table, I probably have the most hands-on knowledge but I can't come here and just speculate about what is actually vulnerable to the system and what is not. And the truth is, once again, on the threat side, as we have seen in media, you can probably tell that, you know, HealthCare.gov is not the one getting attacked. Most cyber criminals, especially those with advanced capabilities, they go where the money is, right? They are going to go after the Targets, they are going to go after the Neiman Marcus, they are going to go after these places that contain lots of data related to intellectual property because it just makes fiscal sense, right? If the U.S. government spends billions of dollars on our research and development and we don't protect it and some other country takes that, you just saved them billions of dollars. Thank you.

[The prepared statement of Mr. Krush follows:]



Waylon Krush

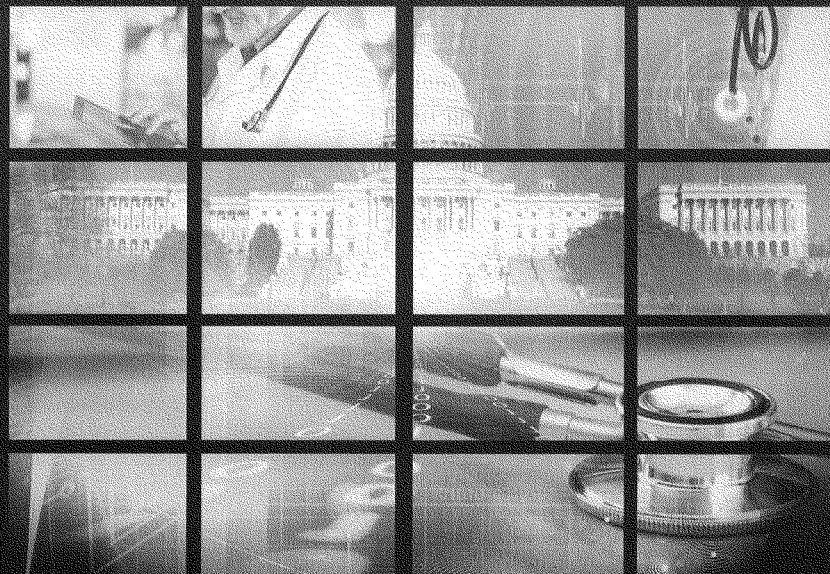
Chief Executive Officer of Lunarline Inc.

Founding Member of Warrior to Cyber Warrior

Testimony to the United States House of Representatives

Committee on Science, Space and Technology

January 16th, 2014



Contents

<u>1. FULL TESTIMONY OF MR. WAYLON KRUSH</u>	<u>1</u>
<u>2. SUMMARY OF TESTIMONY TO THE US HOUSE OF REPRESENTATIVES</u>	<u>4</u>
2.1. SUMMARY OF MR. KRUSH'S TESTIMONY	5
2.2. MR. KRUSH'S QUALIFICATIONS	5

1. Full Testimony of Mr. Waylon Krush



Written Testimony of

Waylon W. Krush

Co-Founder & CEO, Lunarline, Inc. (www.Lunarline.com)

Co-Founder & Board of Directors, Warrior to Cyber Warrior (www.W2CW.org)

Before the Committee on Science, Space and Technology

U.S. House of Representatives

"Healthcare.gov: Consequences of Stolen Identity."

January 16, 2014

Waylon W. Krush

Testimony

"Healthcare.gov: Consequences of Stolen Identity."

January 16, 2014

Chairman Smith, Ranking Member Johnson, and members of the committee; thank you for this opportunity to once again testify on the important topic of cyber security as it relates to Healthcare.gov. I am Waylon Krush, founder and CEO of Lunarline, a leading provider of cyber security products, services, and training to federal and commercial clients.

I am also a founding member of the Warrior to Cyber Warrior program, a free six-month cyber security boot camp for returning Veterans. This program equips Veterans, or if a Veteran is unable to participate because of service related injuries, their spouses, with the skills, training and certifications they need to thrive in the cyber security world.

I have been asked to speak today on the topic of cyber security as it relates to recent events surrounding the Healthcare.gov website and associated systems. I want to make clear that I am not here to weigh in on the political debate surrounding the Patient Protection and Affordable Care Act. That is above my pay grade. Instead, I am here in my capacity as a cyber security professional, one who has contributed to the

defense of our nation's IT infrastructure, both as a soldier in uniform and as a leader of one of our country's fastest-growing cyber security companies.

I have read the previous testimony from several academic and security professionals emphasizing Healthcare.gov's security issues. I see some significant credibility issues with their testimony, and I am here to set the record straight.

Federal information systems are some of the most intricate on the planet. To truly understand system risk – particularly for a system as complex as Healthcare.gov – you have to know a system inside out. Speculating, that specific attacks threaten the security of Healthcare.gov is just that. Speculation.

My service to the Army Information Operations (IO) Red and Blue teams, my award-winning work in advanced cyber signals and protocol analysis, and my experience running some of the most successful military and commercial penetration testing teams has taught me a valuable lesson: never, ever make assumptions about cyber attacks. Presuming that an attack will be successful before studying the target, executing an attack and successfully taking over a system is purely academic and, most of the time, just flat wrong.

This is worth repeating: large IT systems are complicated. This complexity makes it difficult to predict an attempted attack's effectiveness. Unless critics of the site actually executed an attack and successfully penetrated Healthcare.gov, they cannot profess to know how an attack attempt will play out.

On a related note, to be very clear, if someone actively tries to exploit vulnerabilities on a government system – say, for marketing or political reasons – and they do so without the explicit permission of the government, they are breaking the law.

Now, I do want to make sure that I do not make the same mistakes of speculating. Just as security critics lack the hands on knowledge necessary to make dramatic claims about the site's weaknesses, I cannot claim to understand all of Healthcare.gov's security intricacies. Like many of the previous witnesses, I only have access to the public record, a record that tells of findings that, while significant, are addressable with a strong mitigation strategy. I did not work on Healthcare.gov. So I will not come in here as a cyber security professional and say that the site is 100% foolproof, cyber-safe, and running at a normal level of risk. If I did that I wouldn't be a security professional.

However, unlike some of those who have testified before you, I do have hands-on experience with CMS security systems and practices. As a result I am very familiar with the many of the cyber security tools deployed within CMS. I have also provided and taken cyber security training at CMS and I have worked side by side with the exceptionally talented and hardworking cadre of cyber security professionals at HHS headquarters.

I can provide you with insight into the Risk Management Framework (RMF) used to secure Federal Information Systems. This is the process that was used to identify and mitigate vulnerabilities within Healthcare.gov. The RMF process is extensive and provides a security depth and rigor that is unmatched by even the most secure commercial organizations. In fact, many emerging security standards and baselines are simply a subset and rewording of what is included in the RMF. I can say this with confidence as I have applied these standards to many of the nation's most sophisticated and secure systems. I have also co-authored a book on the RMF and supported the writing of the very guide we use to assess Government systems – NIST SP 800-53A.

The RMF is a six step process that governs the categorization, security control selection, control implementation, control assessment, authorization and continuous monitoring of all federal IT systems. I will briefly describe each step and provide some insight into how each one relates to the security of

healthcare.gov. I will however caution the committee that any internal vulnerabilities related to Healthcare.gov should **absolutely not** be publicly released until HHS or CMS has time to mitigate or remediate these issues

The first step, Step 1, is called categorization. During system categorization we analyze all the information stored, processed or transmitted by any component of the system. We classify all data by data type and sensitivity, and set the protection level as "Low," "Moderate," or "High" to meet the requirements of the most sensitive system data. Based on what I have read publicly thus far, Healthcare.gov is most likely categorized as a Moderate system.

The second step, Step 2, governs the selection of security controls to meet the protection requirements defined in Step 1. As a "Moderate" level system, Healthcare.gov is required to implement, at minimum, several hundred security controls. Additional controls may be selected based on any unique system security requirements, such as the presence of personally identifiable information (PII).

In Step 3, we take the controls identified in Step 2 and implement them. This is where the rubber hits the road. HHS and CMS have both authored comprehensive information security policies that govern their approach to cyber security. These policies are backed by significant investments in enterprise detection and protection capabilities, including security operations centers, enterprise end-point technologies, border and gateway filtering, incident response teams, and enterprise continuous monitoring capabilities. For Healthcare.gov, these enterprise-level controls are combined with system specific ones to support the implementation and maintenance of an effective security posture.

After selecting and implementing controls, Step 4 of the RMF mandates frequent security control assessments. These are tests that are conducted to determine whether or not to allow a system to continue operation. However, let me be clear: **there is no such thing as a clean assessment**. An assessment, of any system, federal or otherwise, will always reveal some security risks. It is **not** possible to have a completely secure system.

At this point, everyone here is probably familiar with the "Tavener memo" I discussed previously. This memo described some components of the "Federally Facilitated Marketplace" that had not yet undergone thorough re-testing due to continued system development. It was determined that this uncertainty represented a "high risk."

Now, there is no denying that this does indeed represent a significant system risk. Had the memo ended with that finding we would have every right to be deeply concerned. However, the memo continues to outline a comprehensive mitigation strategy designed to mitigate this risk. This includes the establishment of a dedicated security team to monitor the system, weekly testing of all border and web-facing assets, daily / weekly scans using continuous monitoring tools and a promise to conduct a full Security Control Assessment within 90 days.

While Healthcare.gov's political sensitivity has cast a spotlight on this process, these types of risk analyses are common place across the federal government. **Again, security assessments always reveal risks, no matter what system is being assessed.** How those risks are managed ultimately determine whether or not a system can be labeled "secure." There is a reason it's called the "Risk Management Framework," rather than the "No Risk Framework." It is designed to ensure that Risk Executives conduct precisely these types of tradeoff analyses.

The Tavenner memo is also an example of Step 5, called System Authorization. Simply put, this step requires a management decision on how, when and under what conditions a federal system may be authorized to operate. Like Healthcare.gov, most federal systems are authorized with conditions and pending the implementation of an effective mitigation strategy. This is exactly what you are reading in the Tavenner memo.

Finally, during Step 6 we continuously monitor security posture throughout the entire system lifecycle. This is the most important step in the process. This is why I have publicly stated that I would trust my own personal data to Healthcare.gov. I know as well as anyone that as soon as a system is developed you are in a race against time to find and mitigate vulnerabilities. This is particularly true for high value targets such as government IT assets.

That being said, if HHS follows through with their ongoing daily and weekly scanning and more importantly – quickly remediates and mitigates security issues as they are discovered, we can be assured our data is safe as possible.

However with all of the media attention, it may seem like Healthcare.gov is one of the highest pay-off targets from a threat perspective. But that is simply media spin. Healthcare.gov may be a great political target, but we as a nation have much more tempting targets. Our government is full of high pay-off targets. Nationally sponsored organizations are constantly looking for jump points into our government's infrastructure, so all federal systems' security should be taken very seriously. I get very nervous when I hear that a new critical technology or weapon system has been deployed with security as an afterthought. None of these systems are getting the kind of press Healthcare.gov has received...but they should. As far as personal identity issues the recent coverage of retail demonstrates some of the high-payoff targets criminals are interested in.

In closing, committees prior to this hearing witnesses said they would not use Healthcare.gov. I would use it without hesitation.

2. Summary of Testimony to the US House of Representatives

On Wednesday, January 16, 2014, Mr. Waylon Krush will appear before the United States House of Representatives' Committee on Science, Space, and Technology to discuss the security issues surrounding Healthcare.gov. To facilitate the Committee's review of Mr. Krush's testimony, he respectfully submits the following summary of his prepared remarks.

2.1. Summary of Mr. Krush's Testimony

- Without a real understanding of systems security architecture, and the vulnerability and penetration results, inferring what an exploit or malware could do to a system is simply speculation.
- The Federal Government has adopted a comprehensive and rigorous set of processes and procedures, collectively called the Risk Management Framework, to manage the risk to federal systems. This is not called the "No Risk Framework;" instead it provides detailed guidance to security professionals on the proactive and effective *management* of risk to federal IT infrastructure.
- There is no such thing as a 100% secure system. Cyber security professionals seek to manage risk.
- Mr. Krush has publicly stated that he would entrust his personal data to Healthcare.gov. He stands by this statement.

2.2. Mr. Krush's Qualifications

- **Mr. Krush is the CEO of Lunarline**, an award-winning, Service-Disabled, Veteran-Owned Small Business that provides cyber security and privacy products, services, and training to federal and commercial clients. Lunarline is consistently ranked by *Inc. Magazine* as one of the nation's fastest growing companies.
- He is also a founding member of the non-profit organization **Warrior to Cyber Warrior**. Warrior to Cyber Warrior provides a free six-month cyber security boot camp for returning Veterans to equip them for the challenges of the civilian cyber world and obtain careers in the cyber security and privacy industries.
- A Veteran of the U.S. Army, Mr. Krush is a **recipient of the Knowlton Award – one of the highest honors in the field of Intelligence – for his advanced cyber security work**. For his outstanding contributions to U.S. National Security, he was also recognized as the **718th Military Intelligence Soldier of the Year** and NSA Professional of the Quarter. He also received the Voice of America Award and is a two-time winner of the American Legion Award, as well as many other technical and military impact awards related to cyber security and operations.
- Mr. Krush was awarded a military, commercial, and government impact awards for his direct work in cyber security, has been the subject matter expert (SME) on critical infrastructure protection (CIP) assessments around the world, and actively works on advanced cyber security projects in the government and commercial industry.
- As founder of Lunarline, Mr. Krush has developed a reputation for being a **cyber security thought leader**. He has appeared as a cyber security expert on CNBC, NPR, Fox Business, AP, and other news outlets. A **published author**, Mr. Krush has been featured in *Military IT Magazine*, *Government Health IT*, *SmartCEO*, and numerous other publications. Mr. Krush was also the **co-author of the cyber security book**, *The Definitive Guide to the C&A Transformation*,

NIST Special Publication 800-53A, The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) version 3.0, and several other cyber security and privacy publications.

- Mr. Krush holds a B.S. in Computer Information Science from UMUC, is a Certified Information Systems Security Profession (CISA), Certification and Accreditation Professional (CAP), Certified Information Systems Auditor (CISA), and has more than 3,000 hours of training from the National Cryptologic School.

Chairman SMITH. Thank you, Mr. Krush.
Mr. Gregg.

**TESTIMONY OF MR. MICHAEL GREGG,
CHIEF EXECUTIVE OFFICER,
SUPERIOR SOLUTIONS, INC.**

Mr. GREGG. Thank you, Chairman Smith, thank you, Ranking Member Johnson, Members of the Committee, for having me here today.

My name is Michael Gregg. I am really going to break down my speech into three pieces and my presentation: first, how HealthCare.gov could potentially be hacked, why HealthCare.gov needs independent review by third parties, and also, what would be the result of this, what could be the potential impact.

My concern is that HealthCare.gov is a major target potentially for hackers looking to steal not only personal identities but also information that could be used to steal their identity. Although I understand HealthCare.gov does not store that information, it passes that information back and forth between third-party government sites and other organizations. While there are many different ways that the site could be hacked, there are some prominent ones, and these are the same ones listed by prominent websites like OWASP. It could be things like cross-site scripting, SQL injection. It could be LDAP injection, it could be buffer overflow. There are many different ways that this could be done.

Now, while that sounds foreign to many of you, the fact is, these are known attacks that are used against known sites every day from Target to Neiman Marcus to Google to many others. Some of the things that concern me are in the past we have seen, for example, the 834 data. That is data that is passed to the back end of the insurance companies. We have seen and we have heard reports of this information being corrupted and not being correct when it is being received. That indicates at some point the data is not being handled correctly, and all input data, all process data, all output data has to be correct. If not, there is some type of problem, meaning that data is not being properly parsed. That same kind of situation could lead to an attacker putting in some type of data and misusing that in some way or launching an attack.

Also, as I said, HealthCare.gov is a very large attack service. This is a very large program or application. It was built very quickly. A large attack surface makes it very hard to secure. So I find it hard to believe that during the release and also the update of the site that all the items that our previous speaker spoke of as far as FISMA, FIPS 199, FIPS 200, were actually taken care of and it actually passed all those requirements that they are required to by law, and that those were properly completed.

Microsoft, think of those folks, for example. They have spent almost 30 years trying to secure their operating systems and still we see Microsoft products or operating systems being brought under attack. To think that HealthCare.gov could be built so quickly and then be secured to me is very hard to believe.

When we have a large application or website to be reviewed, typically we do it a couple of different ways. We start at the very beginning before the site is actually developed. We do things as far

as audits. We do vulnerability assessments. We also do PIN testing. All three of these things are required to actually look at and examine the site. PIN testing is a very important part of this process because PIN testing means we are looking at the site the same way the attacker would. We are saying what would the attacker see, what could they use, what could they do with this and how could they leverage this potentially for attack. I don't believe those types of assessments have been done to this day and have been properly completed.

So what has been reported currently is that when we see with HealthCare.gov that they are running weekly assessments, that they are potentially patching the site, but a lot of that activity we are talking about is reactive in nature. That means when we are finding a problem, we are actually fixing it. That doesn't mean we have already gone out and we have found all possible problems or all potential ways that an attacker may leverage that and get access to the site.

Some might argue that if HealthCare.gov is actually vulnerable, why hasn't it already been attacked? Well, if you think about it from an attacker's standpoint, we have seen that attackers have the fortitude and also the patience to wait until the right time. Look at Target. Did they attack immediately? No, they waited until the right time and the right moment to actually do this. This could be the same thing. They are going to wait until after March. They are going to wait until the deadline. They are going to wait until there is a trove of information for them to go after. Then they are going to target it.

So what could be the impact on consumers? Potentially reduced credit ratings. It could be increased difficulty getting loans, could be criminal issues. It could be emotional impact. It also could be very damaging as far as medical information that could be lost. It could be potentially people don't get hired for a job. It could be they get the wrong treatment because someone else has obtained treatment under their name for some other type of disease or some other type of problem that they didn't have. It could be potentially them being denied an application or job for some reason.

And in closing, I would just like to say this. When our organization builds applications, we bring everybody together. We bring the end users, the developers. We bring everyone together, the security professionals, to make sure the site is secure and that security can be built in from the very beginning. I do not believe that has been done in this case. Hacking today is big business. It is no longer the lone hacker, the individual in their basement. Today is organized crime. It is very large groups potentially out of places like Russia and Eastern Europe. We can fix these problems, but for these problems to be fixed means that we need an external assessment of this site by independent third parties.

Thank you very much for your time.

[The prepared statement of Mr. Gregg follows:]

HealthCare.gov: Consequences of Stolen Identity

Testimony of Michael Gregg before the US House Committee on Science, Space, and Technology.

Rayburn House Office Building, Room 2318

January 16, 2014

My name is Michael Gregg and I am the CEO of Superior Solutions, Inc., a security assessment firm which performs security assessments, penetration tests, and audits. Superior Solutions helps companies secure critical assets as well as works with organizations after security breaches have occurred to determine what happened to prevent future breaches.

I have more than 20 years of IT security experience. I also work with organizations such as ISSA and ISACA to help educate security professionals. I have authored more than 15 books on IT/cyber security. I have taught for Villanova University and other educational institutions. I have also served as an expert witness. My testimony is divided into three parts. I have done so as I believe these are the three critical areas the committee should consider.

- How might HealthCare.gov be hacked?
- Why does HealthCare.gov need to be reviewed by an independent 3rd party?
- What would be the result of HealthCare.gov being exploited?

How might HealthCare.gov be hacked?

My analysis of the HealthCare.gov website was gathered from passive analysis of readily available information and my personal knowledge of web applications and web design. Under no circumstance did I or any employee of Superior Solutions conduct any type of “hacking” efforts or attempt to exploit any weaknesses in the HealthCare.gov website.

While functionality has been the main focus thus far in the scrutiny over the HealthCare.gov website, my concern is that a much bigger issue is looming in that individuals enrolled at the HealthCare.gov website could have their personal information and/or medical records stolen.

My concern is that the HealthCare.gov website is a major target for hackers who are looking to steal personal identities. Although HealthCare.gov doesn't store this information directly on the website, it only links to it through a maze of third-party government sites such as the Internal Revenue Service, Department of Homeland Security, Social Security Administration, Department of Veterans Affairs, and others. While there are many ways that the HealthCare.gov website may be hacked, I have described five potential ways that this could occur:

1. Code Injection Attacks - When a website is poorly designed, it's often vulnerable to what is referred to in the security industry as "injection attacks." This means a hacker can go onto the website and write malicious code which he/she then tricks the website into accepting and running as its own code. One of the most widely used code injection attacks is SQL injection. The best example of poor input validation is the fact that some 834 files are corrupted and are unusable when passed to insurance companies. The transport of this data via Electronic Data Interchange (EDI) might be targeted when being passed back to the insurer and being mapped to the Qualified Health Plan (QHP). Such errors point to the fact that input is not being handled correctly.
2. Cross-Site Scripting - This attack can occur when a hacker goes in and (as in cases stated above) tricks the website into accepting malicious code through an input field such as a web request or form field. The next time a person visits the site, a cross-site scripting attack will run against their web browser, stealing saved passwords, cookies, or other sensitive information from the user.
3. Insecure or Weak Authentication - Websites that are poorly designed often struggle with inadequate "authentication" and "session management" - these are important security features that, when done right, protect the integrity of your account. When they are weak or inadequate, a hacker can impersonate users and take over their accounts.
4. Clickjacking - In this type of attack, hackers take advantage of poor security on a website to slip invisible frames over seemingly innocuous items or features on a webpage such as an entry form, a video, or a "like" button. When individuals click on this button (for instance, "submit form"), they're actually clicking on the hidden link slipped over the real web page, so their information is redirected to a malicious website or sensitive information is stolen.
5. Sensitive Data Exposure - Websites that are not properly secured can leak sensitive data or fail to properly encrypt it. We've seen this before even with well-designed commercial websites and mobile apps. For example, the site does not properly encrypt its users' passwords or transmits information in clear text. Twitter and Gmail used to have this problem before they switched to default SSL encryption for all users. In the case of HealthCare.gov, the real risk is likely to be in how it relays data back and forth between the various third-party websites it is linked to (e.g., IRS, Veterans Affairs, etc.) and how well it encrypts those communications.

Why does HealthCare.gov need to be reviewed by an independent 3rd party?

While the types of attacks previously discussed may sound foreign to many, the threat is real. HealthCare.gov has a large attack surface that is very complex and that makes it very hard to secure. Why does the site need an external review? Let's start with certification and accreditation. With my expert knowledge of certification and accreditation, I find it hard to believe that during the release and update to the

HealthCare.gov website, that all the requirements of FISMA, FIPS 199, and FIPS 200 were properly completed. Even if, for the sake of argument, we assume such testing was performed, this is not enough when we are talking about the potential loss of millions of individuals' personal information.

The website itself is large. HealthCare.gov is reported to be about 500 million lines of code. This pales in comparison to others such as Microsoft Windows. Windows 8 is reported to be no more than 80 million lines of code. Microsoft has spent almost 30 years attempting to secure their operating systems. It's illogical to believe such a large site such as HealthCare.gov, could be secured in such a short period of time. To believe that this has occurred would mean that the contractors responsible for the development of this site have been able to do what no other major company (Microsoft, Apple, Facebook, and Google) has ever accomplished.

It's considered a "security best practice" that the individuals that write the code and develop the site are not the same individuals that test the security features of the site. Think of it as "separation of duties."

When a large application or website is reviewed, it is typically performed in one or more of three ways. These three categories include: audits, vulnerability assessments, and penetration testing.

1. Audits - Reviewing a checklist of criteria of things that should be completed. As an example, credit card numbers should be encrypted.
2. Vulnerability assessments - Typically software packages that perform scans looking for common problems, misconfigurations, and missing patches/updates. As an example, using a software tool such as Nessus or Retina.
3. Penetration testing - This type of assessment examines what an insider or outsider can access, how that can be leveraged, and what would be the resulting impact. Typically, organizations bring in external, third parties to perform these types of penetration tests. Such tests are much different than certification and accreditation testing in that they examine the site in much the same way as a hacker would.

All three are required for a well developed, robust application.

What has been reported is that currently, the HealthCare.gov website is only being scanned and patched after problems are discovered. As an example, Mr. David Kennedy, previously testified that he had found issues and reported them to the site administrators to be addressed. Such an approach is detective in nature. Think of it in this way, the site administrator must find and secure all problems yet a hacker only needs to find one vulnerability to exploit the site. Hackers now work in organized groups out of places such as Russia and Eastern Europe. Should these hackers find problems in the site, they *would*

not report them. Such information would be used to exploit HealthCare.gov and expose US citizens to undue risk.

What would be the result of HealthCare.gov being exploited?

There are two areas of concern if/when hackers exploit HealthCare.gov which include loss of personally identifiable information (PII) and healthcare information. If these attacks were to occur, they could be devastating. Just consider the following attacks and the number of personal information lost:

- Adobe - 38,000,000 accounts exposed
- Sony - 77,000,000 accounts exposed
- T.J. Maxx - 94,000,000 accounts exposed
- Target - 120,000,000 accounts exposed
- Heartland - 130,000,000 accounts exposed

Source: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

A successful attack against HealthCare.gov could expose many more individuals than the exploits previously listed. It could very well be the largest ever. Some might argue that if HealthCare.gov is vulnerable, why hasn't it already been exploited? One reason is timing. Hackers have shown that they have the patience and fortitude to spend a considerable amount of time waiting if there is a big reward. Since the deadline for open enrollment is not until March 31, 2014, hackers would be foolish to exploit the site now. Think of how many social security numbers a breach of the HealthCare.gov website might offer cyber criminals at that time.

Some of the items that an individual might have to deal with as a result of identity theft:

- Reduced credit ratings - An individual's credit rating can be seriously impacted by identity theft.
- Increased difficulty obtaining loans - A theft flag can be added to your credit report which means that you must take additional steps to prove you are the person you claim to be.
- Criminal issues - An identity theft might result in someone using your identity and being arrested or charged with a crime. The victim might be identified with traffic tickets or even criminal charges that are hard to disprove.
- Emotional impact - Dealing with identity theft can be time consuming and emotionally draining. Victims may also be denied employment or forced to deal with collection agencies.

While these items are a scary thought, the second real threat is healthcare/medical identity theft. Such attacks are on the rise. A study by the Ponemon Institute found that a whopping 94 percent of polled healthcare organizations have suffered "data breaches" that exposed patient records. This is a 65 percent increase since 2010-2011. Backing up this study is a 2012 report from the U.S. Department of Health's Office of Civil Rights, which found that in just three years nearly 21 million patients became the victims of medical record data breaches.

Losing a patient's medical record puts a person at risk of identity theft, medical identity theft, and other crimes. Why would hackers target personal health records? Why, because these records are seen as the latest gold mine to organized cybercrime. Medical records can contain social security numbers, birth dates, information about someone's family members, and billing information that could include credit card numbers. Electronic medical records can potentially allow hackers to spoof personal identities and wreak havoc in the lives of many. Medical records are just like any other hacking target in that it can offer a payout or financial reward.

Such information is targeted by hackers. As an example, here are just a few of the medical record hack attacks from 2012:

- 780,000 patient records stolen from Utah Department of Health
- 315,000 records from Emory Healthcare
- 228,000 records from South Carolina Department of Health
- 116,000 records from Alere Home Monitoring, Inc.
- 102,000 records from Memorial Healthcare System Florida

What might be the result of medical record or health care information being stolen from the HealthCare.gov website? Some possible scenarios include:

- Not getting hired for a job - Some companies check medical records.
- Getting the wrong treatment - If someone has had treatment under your identity, you could receive the wrong medication.
- You are denied life insurance - Someone using your stolen identity may have been treated for AIDS or cancer.

Some real life examples include:

- A woman in Utah was contacted by the state's child protective services unit and told that they were going to take her children away because her newborn baby had tested positive for methamphetamines.
- A pilot from Colorado was billed \$41,000 for surgery by a Denver hospital despite the fact that he had not ever been in that particular hospital. He then spent years disputing the charges and nearly filed for bankruptcy because of it.
- A hacker demands 10 million dollars for 8 million patient prescription records stolen from the Virginia Department of Health Professionals in 2009.

Source: http://www.megapath.com/megapath/assets/File/PDF/WhitePapers/WP_MedIDTheft.pdf

In the end, the most frustrating aspect of medical record theft is that patients feel powerless to stop it.

Closing

When my organization builds applications, we bring all the people together: end users, developers, and security professionals so that security can be built in to the design from

the point of inception. The HealthCare.gov website was designed and built quickly without the oversight for security that is required. As a result, this site offers hackers a substantial payday if/when they are able to breach the security of the site. There are many ways in which this might be accomplished such as cross site scripting, SQL injection, URL misdirection, etc. Regardless of how this is accomplished, the end game is the same, in that it will result in a massive loss of personal information.

Hacking has become “big business” today. The era of lone hackers in their basements targeting websites has passed. Today, hacking a site such as HealthCare.gov offers organized crime groups, rogue nation states, and even terrorists a huge potential reward. This problem can be addressed by bringing in a team of external security consultants to review the security of the site and make an independent assessment of its current state. I ask this committee to consider the importance of this activity before it is too late. As Winston Churchill stated, *“I never worry about action, but only inaction.”*

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

Michael C. Gregg

Mr. Michael Gregg is the CEO of Superior Solutions, Inc. (www.thesolutionfirm.com), a Houston based IT security consulting firm. His organization performs security assessments and penetration testing for fortune 1000 firms. He has consulted and led assessment activities for many organizations. He has more than 20 years experience in the IT field. He holds two associate's degrees, a bachelor's degree, and a master's degree and some of the certifications he maintains include: CISSP, CISA, CISM, MCSE, CEH, CHFI, CGEIT, and SSCP. Michael has authored/co-authored more than 15 books; some include: *CISSP Exam Cram 2*, Que; *Inside Network Security Assessment*, SAMS; *CEH Exam Prep 2*, Que; *Hack the Stack*, Syngress; *Security Administrators Street Smarts*, Sybex; *Emerging Threat Analysis 2006*, Syngress; *CHFI Study Guide*, Syngress; *Que CISA Exam Prep 2*, Que; *Security+ Study Guide*, Syngress; *How to Build Your Own Network Security Lab*, Wiley.

Michael is frequently cited by major and trade print publications as a cyber security expert and has appeared as an expert commentator for network broadcast outlets and print publications such as FOX, CBS, NBC, ABC, CNBC, local broadcast television, The New York Times, Kiplinger's, and Women's Day. He has also spoken at major security conferences. Michael is an adjunct instructor for a leading University and has led the development of 20 training classes, courses, and programs used by training vendors, developers, colleges, and universities. He focuses on presenting topics in ways that people can understand the complex issues surrounding IT security. He is also an Expert Q&A for TechTarget.com and also serves on the TechTarget Editorial Board of Advisors. Michael enjoys giving back to the community and serves as a cyber security program advisor for Devry University Houston and as Board Member for Habitat for Humanity of Southern Brazoria County.

Chairman SMITH. Thank you, Mr. Gregg.
And Dr. Ponemon.

**TESTIMONY OF DR. LAWRENCE PONEMON,
CHAIRMAN AND FOUNDER,
PONEMON INSTITUTE**

Dr. PONEMON. Thank you, Mr. Chairman, and thank you for inviting me.

Well, first, let me just start off by saying that I am the research wonk to this panel. These people are absolutely brilliant and they understand the technical aspects and the security issues. What I would like to do is talk a little bit about the consequences of identity theft and medical identity theft. That is really my focus, and the basis of my comments is research, research that my institute conducts. And sometimes, by the way, they call my institute the Pokemon Institute. It is actually Ponemon Institute, which is my last name.

So I understand the purpose of my testimony today is to provide assistance in understanding the potentially devastating consequences of a data breach to individuals, to households and society as a whole. For more than a decade, we have studied the cost and consequences of data breach through extensive consumer studies as well as benchmark research on the privacy and data protection practices of companies in the private and public sectors. In the area of healthcare, we have conducted four annual studies on medical identity theft and patient privacy and security protections within hospitals and clinics. We also survey consumers on their perceptions about the organizations they trust the most to protect their privacy. Among the U.S. federal government sector, for example, we are pleased to report some good news, that the USPS, the Postal Service, gets very high marks for trust. Another, and this might be a little surprising, the IRS actually is trusted for privacy, not for anything else—no, just joking—but definitely for privacy practices, as well as the Veterans Administration, and they were a bad guy, right? You right remember, they lost a lot of data. I am a veteran and I was on that list of 26 million. But they turned things around and they are trusted for privacy.

So today I have been asked to testify about the possibility of like identity theft on the HealthCare.gov website and the potential consequences to the American public. Identity theft and medical identity theft are not victimless crimes and affect those who are most vulnerable in our society such as the ill, the elderly and the poor.

So beyond doing these numerous research studies that I just mentioned, this is an issue that really struck home for me. Last year, my mother, she is 88 years old, she lives alone in Tucson, Arizona, and she suffered from a stroke. She was rushed to a hospital and admitted immediately, and unbeknownst to her, an identity theft was on the premises and made photocopies of her driver's license, debit cards and credit cards that were in her purse. And by the way, she also has all the passwords to everything in a little Post-It note in her purse as well. She doesn't listen to me. That is the problem. The thief was able to wipe out her bank account and there were charges on her credit card and debit card amounting to thousands and thousands of dollars. In addition to dealing with her

serious health issues, she also had to cope with the stress of recovering her losses and worrying about more threats to her finances and medical records.

The situation with my mom in the hospital and those who are sharing personal information on HealthCare.gov are not dissimilar, and let me explain. My mother had a reasonable expectation that the personal information she had in her wallet would not be stolen, especially by a hospital employee, and those who visit and enroll in HealthCare.gov have an expectation that people who are helping them purchase health insurance will not steal their identity. They also have a reasonable expectation that all necessary security safeguards are in place to prevent cyber attackers or malicious insiders from seizing their personal data.

Now, in my opinion, the controversy regarding security of the HealthCare.gov website is both a technical issue, as we heard from these gentlemen but it is also an emotional issue. In short, security controls alone will not ease the public's concerns about the safety and privacy of their personal information. Based on our research, regaining the public's trust will be essential to the ultimate acceptance and success of this initiative.

So following are some key facts that we learned from our consumer research over the more than a decade of doing these kinds of studies. First, the public has actually a higher expectation that their data will be protected when they are dealing with government sites than commercial sites. In other words, when I am going to the Veterans Administration, I have a higher expectation of privacy. Whether it is rational or not, that is basically what we see. Second, the loss of one's identity can destroy a person's wealth and reputation and in some cases their health. Further, the compromise of credit and debit cards drives the cost of credit up for everyone, thus making it more difficult for Americans to procure goods and services. Third, medical identity theft negatively impacts the most vulnerable people in our Nation. Beyond financial consequences, the contamination of health records caused by imposters can result in health misdiagnosis and in extreme cases could be fatal. Because there are no credit reports to track medical identity theft, it is nearly impossible to know if you have become a victim.

So what is the solution? Let me just give you three ideas. First, on the trust issue, let us think about accountability. It is important to demonstrate accountability, and the best way to do that, in my mind, is rigorous adherence to high standards, and I think we mentioned NIST. NIST is a great standard but very high standards above the bar and showing the American people that this particular website or any website that collects sensitive personal information is meeting or exceeding that standard.

Number two is ownership. What I would like to see is the chief information security officer is your chief executive officer. That is good news when the CEO steps up to the plate and does what needs to be done, and in this case, I would love to see our President take ownership of the website and ensure that good security and privacy practices are met as a priority, not just by HealthCare.gov, but across the board.

And third is verification. Now, I am an auditor. I have to admit this, so I am a little bit biased, or I used to be an auditor at

PriceWaterhouseCoopers. You know, we can say that we are doing all of these good things, but having a third-party expert telling us that we are meeting and exceeding the standards is a very good idea and a noble idea.

And with that being said, I think I am actually the first person concluding giving you some time back on the clock.

[The prepared statement of Dr. Ponemon follows:]



**Committee on Science, Space and Technology
United States House of Representative**

Dr. Larry A. Ponemon: Testimony

My name is Dr. Larry Ponemon and I am the founder and chairman of Ponemon Institute. Our Institute was established in 2002 and we are headquartered in Traverse City, Michigan. Our mission is to advance responsible information management among business and government through independent research on privacy, data protection, information security and information ethics. Our studies are widely disseminated and have been cited in more than 50 countries across the globe.

My background represents nearly 40 years of professional experience and knowledge about privacy, compliance and information security. My career started in the Navy during the Vietnam War era. I earned a Ph.D. in accounting ethics from Union College and a Masters degree from Harvard University. Prior to the founding of our Institute, I was a tenured university professor, the executive director of information ethics at KPMG and the global managing partner for compliance risk management at PriceWaterhouseCoopers. I have served on the Advisory Committee for Online Access and Security for the U.S. Federal Trade Commission and the Data Privacy and Integrity Advisory Committee (DPIAC) for the U.S. Department of Homeland Security. I also had the privilege of serving on various privacy advisory committees at the U.S. state level.

I understand that the purpose of my testimony today is to provide assistance in understanding the potentially devastating consequences of a data breach to individuals, households and society. For more than a decade, we have studied the cost and consequences of data breach through extensive consumer studies as well as benchmark research on the privacy and data protection practices of companies in the private and public sectors. In the area of healthcare, we have conducted four annual studies on medical identity theft and patient privacy and security protections within hospitals and clinics. We also survey consumers on



their perceptions about the organizations they trust the most to protect their privacy. Among U.S. federal government sector, we are pleased to report that consumers consistently rank the United States Postal Service as the most trusted government entity for privacy. Other notable departments include the IRS, Census Bureau and Veteran's Administration.

Today I have been asked to testify about the possibility of identity theft on the Healthcare.gov website and the potential consequences to the American public. Identity theft and medical identity theft are not victimless crimes and affect those who are most vulnerable in our society – such as the ill, elderly and poor.

Beyond doing numerous empirical studies on this topic, this is an issue that really struck home. Last year my 88-year-old mother who lives in Tucson, suffered a stroke. She was rushed to the hospital and admitted. Unbeknownst to her, an identity thief was on the premises and made photocopies of her driver's license, debit card and credit card she had in her purse. The thief was able to wipe out her bank account and there were charges on her credit card amounting to thousands of dollars. In addition to dealing with her serious health issues, she also had to cope with the stress of recovering her losses and worrying about more threats to her finances and medical records.

The situation with my mother in the hospital and those who are sharing personal information on the healthcare.gov website are not dissimilar. My mother had a reasonable expectation that the personal information she had in her wallet would not be stolen – especially by a hospital employee. Those who visit and enroll in healthcare.gov also have an expectation that the people who are helping them purchase health insurance will not steal their identity. They also have a reasonable expectation that all necessary security safeguards are in place to prevent cyber attackers or malicious insiders from seizing their personal data.



In my opinion, the controversy regarding security of the healthcare.gov website is both a technical and emotional issue. In short, security controls alone will not ease the public's concerns about the safety and privacy of their personal information. Based on our research, regaining the public's trust will be essential to the ultimate acceptance and success of this important initiative.

Following are some key facts that we have learned from our consumer research on privacy, data protection and information security:

- First, the public has a higher expectation of the protection of their personal information when using or browsing government websites such as the USPS or IRS than when accessing commercial websites such as Amazon.com or ebay.com.
- Second, the loss of one's identity can destroy a person's wealth and reputation. Further, the compromise of credit and debit cards drives the cost of credit up for everyone, thus making it more difficult for Americans to procure goods and services.
- Third, medical identity theft negatively impacts the most vulnerable people in our nation. Beyond financial consequences, the contamination of health records caused by imposters can result in health misdiagnosis and in extreme cases could be fatal. Because there are no credit reports to track medical identity theft, it is nearly impossible to know you have become a victim.

Based on our Institute's research, I would like to recommend a three-part approach to raising the trust and confidence of Americans when using healthcare.gov to buy health insurance.

- First, is accountability. It is important to demonstrate to the public that the government is accountable for the security of the information and can be trusted. This translates into standards that do not just meet basic practices but exceeds them to ensure the website is safe and secure. As an example,



one requirement should be to encrypt all personal data at rest in backend systems.

- Second, is ownership by the CEO. In this case it is the president of the United States who should take ownership of the website and ensure good security and privacy practices are met as a priority.
- Third, is independent verification or audit of the website to ensure all areas and underlying systems meet high security standards.

Thank you for the opportunity to be part of this hearing.

Respectfully,

LA. Ponemon

Dr. Larry Ponemon
Founder & Chairman
Ponemon Institute



Abbreviated resume: Larry Ponemon, Ph.D.

Dr. Larry Ponemon is the Chairman and Founder of the Ponemon Institute, a research "think tank" dedicated to advancing privacy, data protection and information security practices. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management or RIM framework. Dr. Ponemon was named by Security Magazine as "Most Influential People for Security."

Ponemon Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a various industries.

Dr. Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy, data protection and cyber security including financial services, healthcare, pharmaceutical, telecom and Internet.

Dr. Ponemon was appointed to the Advisory Committee for Online Access & Security for the United States Federal Trade Commission. He was appointed to the Data Privacy and Integrity Advisory Committee for the United States Department of Homeland Security. Dr. Ponemon was also an appointed to California State task forces on privacy, data security laws and medical identity theft.

Dr. Ponemon was a member of the National Board of Advisors of the Eller College of Business and Public Administration, University of Arizona. He serves as co-chairman of the Government Policy Advisory Committee and co-chair of the Internet Task Force for the Council of American Survey and Research Organizations (CASRO).

Dr. Ponemon was a global managing partner at PricewaterhouseCoopers, where he founded the firm's compliance risk management practice. He also established the firm's privacy risk management practice. Prior to joining Price Waterhouse as a partner, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG Peat Marwick, and was appointed Executive Director of the KPMG Business Ethics Institute.

Dr. Ponemon has held chaired (tenured) faculty positions and published numerous articles and learned books. He has presented hundreds of keynote speeches or learned presentations at national or international conferences on privacy, data protection, information security and responsible information management. Dr. Ponemon is a member of the International Association of Privacy Professionals, having served as a founding member of the Certified Information Privacy Professional (CIPP) Advisory Board.

Dr. Ponemon is a frequent commentator on privacy, data breach and cyber security for CNN, Fox News, MSNBC, Wall Street Journal, New York Times, Washington Post, USA Today, Financial Times, Bloomberg, Business 2.0, Newsweek, Business Week, U.S. News & World Report, CIO Magazine, Industry Standard, Boston Globe, InfoWorld, InformationWeek, Forbes, Fortune, CFO Magazine, Dow Jones News, Harvard Business Review, NPR and others.

Dr. Ponemon earned his Ph.D. at Union College in Schenectady, New York. He has a Master's degree from Harvard University, Cambridge, Massachusetts, and attended the doctoral program in system sciences at Carnegie Mellon University, Pittsburgh, Pennsylvania. Dr. Ponemon earned his Bachelors with Highest Distinction from the University of Arizona, Tucson, Arizona. He is a Certified Public Accountant (inactive license) and a Certified Information Privacy Professional.

Dr. Ponemon is a veteran (Vietnam War era) of the United States Navy. He is married and has two sons. Dr. Ponemon is an instrument rated private pilot.

I would be pleased to provide professional and personal references upon request.

Respectfully,

L.A. Ponemon

Dr. Larry Ponemon
Chairman & Founder
Ponemon Institute LLC

Chairman SMITH. Well——

Dr. PONEMON. Oh, no.

Chairman SMITH. —not exactly.

Dr. PONEMON. I wasn't watching the time. I am sorry.

Chairman SMITH. Thank you, Dr. Ponemon. I appreciate your testimony. I will recognize myself for questions. Let me direct my first one to Mr. Kennedy.

Mr. Kennedy, the Administration maintains that there has not been a successful security attack on HealthCare.gov. Is that an accurate statement?

Mr. KENNEDY. Thank you, Mr. Chairman. Basically what we know for the monitoring and detection capabilities within the HealthCare.gov infrastructure is as of November 17th, they had not stood up a security operation center or had the capabilities to even detect an actual attack. So it also stated that they detected 32 attacks overall. However, if you have no monitoring detection capabilities, period, how are you detecting all the different attacks that are happening? So I would say that the statement is accurate because they don't necessarily know the actual attacks that are occurring in there.

In addition, I would like to also mention that the Chief Information Security Officer from HHS, Kevin Charest, also said that, "I would say that the HealthCare.gov website did not follow best practices." So as a testament to Mr. Krucsh's testimony, the 800-53 and best practices were not followed and did not meet best practices when it was implemented.

Chairman SMITH. And Mr. Gregg——

Mr. KRUSH. Let me talk to——

Chairman SMITH. I am sorry, Mr. Krush. You can get time from someone else. I would like to ask a question to Mr. Gregg.

Do you agree generally with the assessment by Mr. Kennedy that they don't have the capability? And furthermore, let me say that you did have Administration officials say in November that there was 16, I think, security breaches or incidents and then 32 in December. Are those figures plausible, and where do they get them?

Mr. GREGG. Well, they are potentially plausible if they either weren't monitoring or they didn't pick up the attacks. For most of the sites we look at, and companies we work with, we see anywhere from hundreds potentially, a thousand or more hits a day. Now, a lot of that stuff is scripted but for a number to be that low, I would either think, one, they are not detecting it, or two, their detection capability is not correct.

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

Dr. Ponemon, do the security standards, protections and breach notification standards for Obamacare even meet the minimal standards put in place for the private sector?

Dr. PONEMON. I think the private sector for the most part has—and it does vary quite a bit. There are industry standards, for example, that actually are much higher than the standards we see in the government. But NIST, for example, and the need to comply with certain standards, for example, around cloud computing and fed ramp, and there are standards that exist that are actually fairly reasonable. For the most part, though, I think if you are looking

for best practices, you probably would be looking at industry versus the government.

Chairman SMITH. Thank you, Dr. Ponemon.

Mr. Kennedy, another question for you. Is Mr. Krush right in what he said in his oral testimony that passive reconnaissance of HealthCare.gov is not sufficient to raise concerns about the website's security?

Mr. KENNEDY. Thank you, Mr. Chairman. I would like to address that direct on, which would be, passive reconnaissance, you have the ability to enumerate exposures and vulnerabilities. Any security researcher or tester that has been in the industry for a number of years, especially in the technical side, will be able to collaborate that. In fact, all seven of the security researchers also said the same exact thing, that the website itself is vulnerable. This isn't speculation. These are actual exposures that are on the website today that could lead to personal information being exposed as well as other critical flaws of actually attacking individual people just by visiting the website.

To answer your question, by doing passive reconnaissance, you can absolutely identify exposures. There are absolutely techniques out there without actually attacking the site for doing it, and I would question that the other seven security researchers that also testified that looked at the same type of research, came to the same exact conclusion as myself.

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

Mr. Krush, I do have a question for you. Apparently you have contracts with a company that does work for CMS. Is that accurate?

Mr. KRUSH. That is accurate.

Chairman SMITH. And what is the amount of those contracts, both past and present?

Mr. KRUSH. I actually don't know that off the top of my head but I have—

Chairman SMITH. Okay. I think—

Mr. KRUSH. —tens of millions of dollars of contracts in the federal government right now.

Chairman SMITH. All right. Okay. So you have tens of millions of dollars of business with CMS directly or indirectly?

Mr. KRUSH. Not CMS.

Chairman SMITH. With a company that does work for CMS?

Mr. KRUSH. No, that—those amounts are very high. I am talking across the government. I am not—I just don't know specifically with CMS. That is why I can actually talk from a technical perspective and not speculate on some of the—

Chairman SMITH. With CMS, according to your Truth in Testimony that you filed, I think it is \$1.5 million that you do have in those contracts.

Mr. KRUSH. Okay. That sounds good.

Chairman SMITH. If you will take my word for it?

Mr. KRUSH. Yes.

Chairman SMITH. In that case, isn't it natural that we might suspect that your testimony is a result of your being paid by—directly or indirectly by CMS and here you are not going to actually testify

against them if you have \$1.5 million worth of contracts with them? Isn't that a reasonable assumption?

Mr. KRUSH. Well, Chairman Smith, actually as it relates to CMS, if you look at the GAO docket, I actually have been protesting with them. You know, on the contracting side, me and CMS are not necessarily best of friends. I am here to talk about the cyber security in what—

Chairman SMITH. I know what you would rather be talking about but it still seems to me \$1.5 million in contracts does perhaps influence your testimony. That is all I have to say on that. My time is up, and the gentlewoman from Texas is recognized for her questions.

Ms. JOHNSON. Thank you very much. Very interesting hearing.

Mr. Krush, you were cut off earlier when you were going to make a comment on Mr. Kennedy's testimony. Would you like to make that now?

Mr. KRUSH. I actually have a few here, so just across the board. Earlier Mr. Gregg talked to the fact that, you know, the HealthCare.gov didn't implement what we call FIPS 199 and FIPS 200. Just to clarify what that is for everyone here, FIPS 199 is Federal Information Processing Standard 199. It requires you to categorize an information system in accordance with the confidentiality, integrity and availability of an information system. We know that that was completed because there was a letter from Ms. Tavenner out as part of the authorization process that 200 is the baseline controls for all federal information systems. We also know that that was completed because they had an ATO letter that specified some of the vulnerabilities and what actual the process dealing with the healthcare.gov was. So I just wanted to talk to that point.

And, you know, talking about also waiting, from Target's perspective, waiting until, you know, a certain time to act. I don't think any of us here have also worked on the Target.com website or the backend database, and I would tell you that a lot of the advanced attackers, you know, unless you have done the forensic sampling and you have actually picked up the crumbs, you don't know when they actually attacked, and I think that that is under investigation right now.

HealthCare.gov, Mr. Kennedy brought up the point that there was no security operation centers. Some of those one point whatever million dollars that have been allocated to my company was actually related to those early on. There is actually two security operation centers within HHS you might want to know. They have a centralized one which does monitoring of the entire enterprise, and on top of that, CMS has its own security operation center, and I can tell you from a technology perspective, some of the technologies they have implemented is, you know, top notch. It is what you would expect in a top-tier security operations in the U.S. federal government.

Ms. JOHNSON. Thank you. According to Mr. Gregg's testimony that this site is a major target, but the attacks won't be accurate or of interest or of value until after March, what do you anticipate that March will bring?

Mr. KRUSH. Nothing. You know, the truth is, when it comes to March, if an attacker wants something off the site, they are going to continuously do whatever they can to gain access. I think one of the things that was also said is that, you know, there is a certain number of incidents, and those numbers do sound low, but once again, everybody here, none of us have worked in the security operations center, which does exist within CMS, and so we don't necessarily know what the escalation requirements are. So, for example, most government websites literally are enumerated passively, meaning—and this is still considered an incident via DHS. If you go through and you do scans on a website, meaning that you are looking for open protocols and services, that is considered an incident. Now, does every organization report those? No, because you would have hundreds of thousands of reports a day.

However, some of the—I got a call last night from actually a news reporter and they called me up to talk about Mr. Kennedy's, you know, analysis he had done on the website, and I just want to be clear that, you know, if him and his security researchers actually did go to a dot gov, they did passively enumerate and actually pulled data in an unauthorized manner, then that is a very significant issue. I went to the course while I was in the military for the FBI, and I can tell you that that is of grave—it is great concern to us when anybody goes out to federal government website without permission and is actually passively enumerating then executing something to pull data off that website.

Ms. JOHNSON. Thank you very much.

Dr. Ponemon, you indicated that your mother had this incident happen with her identity. What about that stolen information affected her healthcare?

Dr. PONEMON. You know, in the case of my mom, she would fall into the category of an identity—she is an identity theft victim but not a medical identity theft victim because really, her medical records were not exposed, and so that would be a different crime, and thank goodness she is a medical identity theft victim because that is bad news. It is really hard.

Ms. JOHNSON. Thank you.

Dr. PONEMON. Thank you.

Ms. JOHNSON. My time is expired but I hope someone will ask the value of someone having hacked the HealthCare.gov.

Chairman SMITH. Thank you, Ms. Johnson.

Mr. Hall has said that because Mr. Broun has a time commitment that is almost immediate, he is going to allow Mr. Broun to go ahead of him in the questioning, so Mr. Broun is recognized.

Mr. BROUN. Thank you, Mr. Chairman, and thank you, Mr. Hall, for giving me this opportunity.

It has come to the Oversight Subcommittee of this Committee's attention that there is or at least was an Affordable Care Act Information Technology Exchanges Steering Committee chaired by senior White House officials, established back in May 2012, almost a year and a half before the rollout of HealthCare.gov. The White House steering committee's charter explicitly directed the formulation of working groups, including one on security. It also turns out that a chairman of this Obamacare website steering committee is the U.S. Chief Technology Officer in the White House Science Of-

fice, who also happens to be the immediate past CTO of the Department of Health and Human Services.

Upon learning this, I, as Chairman of the Oversight Subcommittee, along with the full Committee Chairman, Mr. Smith, and Research and Technology Subcommittee Chairman, Dr. Bucshon, sent a letter to the White House requesting that Mr. Todd Park, the U.S. CTO and HealthCare.gov's steering committee chairman, make himself available to the Committee to answer questions regarding the security issues with HealthCare.gov by January 10th, last Friday.

The White House has ignored that letter and the Committee's request until just yesterday when it provided a last-minute response that rebuffed this Committee—let me repeat: rebuffed this Committee. And that letter did not come from the Senate-confirmed President's Science Advisor, to whom the letter was addressed, but from the politically appointed OSTP Legislative Affairs Director.

My question for the panel simply is this: don't the American people deserve answers from those who are in charge of overseeing implementation of the Obamacare website's security protocol? After all, Mr. Park is an Assistant to the President. As the Chief Technology Officer of the United States and the chair of HealthCare.gov's steering committee, wouldn't Mr. Park, or shouldn't he, know and be involved in the security details of the website? Starting with Mr. Kennedy.

Mr. KENNEDY. Thank you, sir. When we look at a website and its security, there are multiple people that need to be involved to understand the progress of it. I would agree with your assessment that there should be some involvement in that case.

In addition, I also would like to clarify that a lot of information that we are getting around these security exposures has actually been vast. The Chief Information Security Officer from HHS saying it didn't follow best practices. You have a number of other individuals saying the security operations center hadn't been started yet. You have the HealthCare.gov infrastructure, which is completely independent and was started completely independent of HHS being part of that. So this is a mismanaged issue. I don't understand how we are still discussing whether or not the website is insecure or not. It is. There is no question about that.

Mr. BROWN. It is insecure?

Mr. KENNEDY. It is insecure, absolutely 100 percent. There is no questioning that. People from HHS have said that. You know, it is not a question of whether or not it is insecure. It is what we need to do to fix it.

And just to point to Mr. Krush's point, he also said to Reuters, which is the article that he also mentioned earlier, Krush said he has not reviewed Kennedy's findings or done any work on HealthCare.gov's site itself. So, you know, this is all purely speculation. It is a bunch of hogwash, and personally, it seemed to be politically biased, unfortunately.

Mr. BROWN. Thank you, Mr. Kennedy. I appreciate your long answer but this is actually a yes or no answer.

Mr. Krush, do the American people deserve to know?

Mr. KRUSH. Yes.

Mr. BROWN. Okay. Mr. Gregg?

Mr. GREGG. Yes, they do. However, I would like to add, I understand the NIST process and others quite well. I co-authored a book on it, also developed a course for Villanova University on certification and accreditation. Finally, his statement ends to a scan. A scan is not passive. A scan is active. But yes, they do deserve an answer on this.

Mr. BROUN. Doctor?

Dr. PONEMON. Ditto, yes.

Mr. BROUN. And I agree, the answer is yes. I am very disappointed with the Administration. We have asked for information. The American people deserve to have that information, and I will do everything that we can to try to get Mr. Park to give us that information or the Administration.

Mr. Chairman, my time has run out so I yield back.

Chairman SMITH. Okay. Thank you, Dr. Broun. The gentleman from Maryland, Ms. Edwards, is recognized for her questions.

Ms. EDWARDS. Thank you, Mr. Chairman, and thank you to our witnesses today.

Just very quickly, Mr. Kennedy, do you have any federal contracts for security? Any?

Mr. KENNEDY. As of right now, no.

Ms. EDWARDS. Have you had?

Mr. KENNEDY. Yes, I have.

Ms. EDWARDS. And what were they?

Mr. KENNEDY. Working for the federal government?

Ms. EDWARDS. Yes, federal security contracts.

Mr. KENNEDY. Yes.

Ms. EDWARDS. What were they?

Mr. KENNEDY. I would be happy to disclose those.

Ms. EDWARDS. I would appreciate it in writing, if you would.

Mr. KENNEDY. Sure.

Ms. EDWARDS. If you would tell us the federal contracts that you have had in dealing with information security in the areas that you claim to be an expert in.

Mr. KENNEDY. I would be happy to write that.

Ms. EDWARDS. And Mr. Krush, I just want to ask you really briefly if you could tell us security standards, compare those that are used for the federal government as to the private sector. You have alluded to that a bit, if you could just very quickly?

Mr. KRUSH. Sure. So one thing to understand, and just to go back to Mr. Gregg, you know, I have also co-authored a book on, we have taken over 10,000 pages of information from the National Institute of Standards and Technology, the Department of Defense instructions, the intelligence community directives and also, you know, some of the SAP programs and consolidated that, and that book is actually used in places such as Syracuse University to teach people that actually want to understand this very rigorous federal process. I am also co-author of NIST Special Publication 800-53 alpha. That is the process where we actually do the assessments per se. So—

Ms. EDWARDS. I trust your expertise. I just want to know the rigor of the standards for the federal government compared to the private sector.

Mr. KRUSH. Sure. So that is a great question, Ms. Edwards. One of the things to understand is that NIST Special Publication 800-53 starting at revision 2, and we are now up to revision 4, integrated all of the commercial standards. At rev 3, so meaning, you know, the most ISO, Carnegie Mellon, a lot of these organizations that had kind of best practices out there, they were integrated into that revision. By revision 4, we have actually integrated the Department of Defense standards, the intelligence community standards, also a lot of standards that are kind of outside the realms, they are threat-based. As you will find, most auditing organizations don't look for those.

Ms. EDWARDS. So are the—

Mr. KRUSH. There is definitely rigor compared from a commercial organization to what you will get in the government, and I have worked on both sides. Fifty percent of my contracts are with Fortune 50 and 100 companies, so I can tell you the depth and rigor that you implement on a federal information system, as it should be, is just more much intense than what you see in the commercial markets.

Ms. EDWARDS. And is HealthCare.gov, is the rigor attached to HealthCare.gov any different from any of these other federal systems that you have indicated?

Mr. KRUSH. No, this process is the same across the U.S. government.

Ms. EDWARDS. Thank you. So I wonder if the standards that you described are above—and I think you said this—are above those that you would find in the commercial sector?

Mr. KRUSH. I would say yes.

Ms. EDWARDS. Thank you.

Mr. Gregg, you mentioned some information or speculation about medical records vis-à-vis HealthCare.gov. Are you aware of any medical record that is maintained on HealthCare.gov?

Mr. GREGG. No, the information is simply passed through.

Ms. EDWARDS. Exactly. Is there any medical record, personal medical record, contained on HealthCare.gov?

Mr. GREGG. No.

Ms. EDWARDS. Thank you.

And then Dr. Ponemon, just out of curiosity, you talked about your mother's experience, which just sounds really horrible, but she didn't experience identity theft through HealthCare.gov. Isn't that correct?

Dr. PONEMON. Absolutely not.

Ms. EDWARDS. Right. Thank you.

And I just wonder, Mr. Krush, if you could help me, if you will. Of the experience that you have had in developing and working on federal information systems, is it your conclusion that you would feel safe in putting your personal information through HealthCare.gov?

Mr. KRUSH. Ms. Edwards, I actually put that in my testimony. I would put my personal information on HealthCare.gov. I said this more than once, and you know, I continue to stand by that.

Ms. EDWARDS. Thank you.

And Mr. Kennedy, lastly, I want to go back to your federal work I mean that I can find disclosed. I know that you got a small busi-

ness loan from the Small Business Administration for “businesses that do not qualify for credit in the open market.” Again, what is the other federal security work that you have done?

Mr. KENNEDY. I would be happy to disclose that in written testimony.

Ms. EDWARDS. Can you just give me an example right here on the record?

Mr. KENNEDY. I would need to get permission from my customer. I work on non-disclosure agreements and confidentiality of information.

Ms. EDWARDS. Okay. What I would like to do, I will write you a letter. Your financial disclosure that you have submitted in this record requires that. Did you put that in your financial disclosure?

Mr. KENNEDY. No. No, I—listen to me. My experience—

Ms. EDWARDS. Did you—

Mr. KENNEDY. The question you asked me was, did I have federal experience in the—

Ms. EDWARDS. It is my time, Mr. Kennedy.

Mr. KENNEDY. Yes, ma’am.

Ms. EDWARDS. Did you put that financial disclosure information in the record as required by our Committee?

Mr. KENNEDY. I am not required to put that in there.

Ms. EDWARDS. Thank you very much.

Mr. KENNEDY. Thank you. It is not on behalf of TrustedSEC. Thank you.

Chairman SMITH. Thank you, Ms. Edwards. The gentleman from Texas, Mr. Neugebauer, is recognized for his question.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

So, Mr. Gregg, I ask you this question: could a security breach of HealthCare.gov result in people’s medical files being accessed?

Mr. GREGG. Yes, sir, it could. The information could be accessed, and then the real damage would come afterwards, how that information could be used. It could be used potentially to gain information of financial data. It could be used for identity theft. It could be misused many different ways. And that damage, as Mr. Kennedy alluded to earlier, is not just something as simple as replacing a credit card. This can be long-term. It can be very damaging to an individual.

Mr. NEUGEBAUER. Now, there was a recent GAO report that documented that there was a 111 percent increase in federal agency data breaches in the past three years. Specifically, the GAO report noted that there were 22,156 incidents revealing sensitive personal information since 2012, up from 10,000 in 2009. Interestingly enough, the Centers for Medicare and Medicaid Services, the HealthCare.gov operator, had the second-most breaches in the report for Fiscal Year 2012. Mr. Krush said that the hackers are going where the money is and not necessarily interested in these government sites, but yet we see a substantial increase in the number of incidents that are happening. Mr. Kennedy, do you agree with Mr. Krush that people really aren’t interested in these government sites or what is your opinion on that?

Mr. KENNEDY. Thank you, sir. I do not agree with Mr. Krush’s testimony there. I believe that the hackers move where the money is and there is a lot of money to still be made in the personal infor-

mation side as well as other government agencies that look to do demise to us, especially on our information technology-related issues. Having direct access into DHS, IRS is a treasure trove for additional attackers out there. There is a lot of money for the organized crime, there is a lot of money for what we call state-sponsored attacks, so I would not agree with his assessment. There is plenty of money to be made in the government space and there are breaches happening all the time there.

Mr. NEUGEBAUER. If I go to a government site and I am a hacker, what are the treasures out there that I am going to glean that are going to help me do whatever bad thing I have in mind?

Mr. KENNEDY. Sure. I think that is in the question. It depends purely on the motivation of the attacker. So you have really three criteria of the attackers. You have your average black hat that may be politically motivated to prove a specific point or street credibility. You have your organized crime, which is specifically looking for monetary value or persistent access into organizations. There is also a huge black market right now that surpassed the credit card industry for what we call carders. Selling compromised infrastructures and organizations is a huge market right now. If I can say, hey, I compromised Government X or HealthCare.gov, I can sell that to an attacker for thousands of dollars to make a big buck off of it.

Additionally—so you have that portion of it, the identity theft, the fraud, other areas there. Then you have the state-sponsored element, which is other government entities attacking infrastructure in order to infiltrate, gain access and intelligence on us, and that is a huge business right now. We see it obviously happening off of different, multiple other government entities, as well as Eastern European countries.

Mr. NEUGEBAUER. Would you feel comfortable putting your personal information in HealthCare.gov?

Mr. KENNEDY. Absolutely not.

Mr. NEUGEBAUER. Yes. Mr. Gregg?

Mr. GREGG. No, sir, I would not.

Mr. NEUGEBAUER. Dr. Ponemon, would you?

Dr. PONEMON. I am not sure.

Mr. NEUGEBAUER. You know, I want to go back to you, Dr. Ponemon. One of the things that, you know, you talked about was that you wanted to talk about the consequences of stolen identity.

Dr. PONEMON. Sure.

Mr. NEUGEBAUER. Yes. So one of the things I think might be helpful is people that are forced to go to access their healthcare through government—HealthCare.gov, what would you advise them to do? You know, they are going to have to access that. As they are filling out that information, are there some preventative things that they can do that would minimize some of the potential consequences if the system is breached?

Dr. PONEMON. Well, obviously, if the site is secure, that is a good step, right, but as an individual, whether we are doing it on HealthCare.gov or whether it is a website like Amazon.com, we need to be smart. We need to understand that our data could be at risk. The bad guys are really smart. For example, we should not be using the same password over and over again. Our computer

should have the most current version of antivirus or anti-malware technology. These commonsensical approaches do make a difference and that should be across the board.

But again, if you have data that is extremely sensitive and confidential, then basically your guard, your level of concern should go up. And a lot of people don't think about these issues well enough or they don't think that they will become a victim. But as we know, with 110 million records here and 90 million records there, everyone, every single person in this room is a victim of some data loss and probably at least had one data breach notification in the last five years. So it is a big problem.

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

Chairman SMITH. Thank you, Mr. Neugebauer.

The gentlewoman from Oregon, Ms. Bonamici, is recognized for her questions.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you to our witnesses for being here today.

This hearing is ostensibly about HealthCare.gov but I just want to make a big picture comment that the Affordable Care Act is certainly about more than a website; it is about an issue of great importance, which is about the availability of healthcare to all Americans.

Now, when I saw the title of this hearing, I was pretty interested. I actually have a background in consumer protection. I used to work at the Federal Trade Commission, have worked on identity theft issues. I was a little baffled frankly about why we are doing this in the context of HealthCare.gov and in the Science Committee.

That being said, we all acknowledge that there have been some serious technological problems rolling out the Affordable Care Act, but I am really concerned that some people listening, our constituents, might really be concerned that there are risks involved in enrolling through the website that aren't really there. So I want to clarify a couple of things.

First of all, I want to make it clear to our constituents that identity theft is already a federal crime, that if someone knowingly commits identity theft, that is a federal crime. If they do it—aggravated identity theft, there are enhanced penalties. So I want to make clear that if there is identity theft, that is already against the law. The Department of Justice prosecutes that. The Federal Trade Commission has several laws dealing with it. So identity theft is an issue we should be concerned about but I am baffled about why we are talking about it in the terms of HealthCare.gov.

So, Mr. Krush, I want to ask you a couple of questions. First, I want to acknowledge and thank you for your service to this country. I understand, Dr. Ponemon, you are a veteran as well. Thank you for your service.

Mr. Krush, you talked about how some people are suggesting that HealthCare.gov is a major target for hackers. Based on your background, your military and cyber security background, could you discuss the range of hackers and their different motives and talk about where HealthCare.gov is on the scale of high payoff targets. And you mentioned this in your testimony, but will you talk about that range just a bit, please.

Mr. KRUSH. Yes. Actually, it is very interesting in that, you know, we are here on the Committee of Science, Space, and Technology, and I will tell you something from a high payoff target perspective, especially when you are dealing with advanced attackers, the more a nation—nation-sponsored attackers and those even on the criminal organizations, they are after some very specific targets. And, you know, I am not going to go into those but I will tell you from a government perspective in all reality if you are looking at the .mil and the .gov kind of domains, you know, HealthCare.gov is not really a huge high payoff target.

Space systems, technology related to weapons systems, intellectual property stores, information related to clearances, information related to quite possibly not only personal information on a person that may be weaknesses such as relationship issues where they can be played on or through blackmail. There is—websites that include information on criminals that are actually part of the court systems, literally we keep all of this information online now. As you can imagine from an attacker's perspective, you could literally, you know, not delete the paper but there are ways that you can get into a system and change an outcome of quite possibly, you know, cases or what actually you have done in the past. So there is lots of high-profile targets.

Ms. BONAMICI. Thank you. Thank you so much. I want to follow up a little bit. It is my understanding that we have already established that there aren't medical records on HealthCare.gov, and Mr. Gregg confirmed that in response to Representative Edwards' question. Do you agree with that, there are no medical records on HealthCare.gov?

Mr. KRUSH. Correct. Those would be at the providers.

Ms. BONAMICI. And would you agree that there is more personal information in a federal tax return than there is in a HealthCare.gov insurance application?

Mr. KRUSH. I agree.

Ms. BONAMICI. Mr. Kennedy, do you agree with that?

Mr. KENNEDY. I do agree.

Ms. BONAMICI. Mr. Gregg?

Mr. GREGG. I do agree.

Ms. BONAMICI. Dr. Ponemon?

Dr. PONEMON. I agree.

Ms. BONAMICI. Terrific. Okay. So about 80 percent of the people in this country file their tax returns online. Mr. Krush, do you file your tax returns online?

Mr. KRUSH. I do.

Ms. BONAMICI. Mr. Gregg, do you file your tax returns online?

Mr. GREGG. No.

Ms. BONAMICI. Dr. Ponemon, do you file your tax returns online?

Dr. PONEMON. I am old-fashioned. No.

Ms. BONAMICI. Mr. Kennedy?

Mr. KENNEDY. I am old-fashioned as well.

Ms. BONAMICI. So when you understand that about 80 percent of the people in this country file their tax returns online, we are talking about security with HealthCare.gov when there is more personal information on a federal tax return. I just want to highlight

that, that we are talking about security with HealthCare.gov when the majority of people file their tax returns online.

All of you call for third-party—third parties to conduct security testing, and the MITRE Corporation, Blue Canopy, and Frontier Security have all been doing that for months. In your opinion, are those companies competent to do the work, yes or no? Dr.—or Mr. Krush?

Mr. KRUSH. Yes.

Ms. BONAMICI. Mr. Kennedy?

Mr. KENNEDY. Yes.

Ms. BONAMICI. Mr. Gregg?

Mr. GREGG. Yes.

Ms. BONAMICI. Dr. Ponemon?

Dr. PONEMON. I only have knowledge of MITRE and the answer is yes.

Ms. BONAMICI. Thank you. Mr. Krush, to be clear, there have been no cases of a person's identity being stolen through HealthCare.gov at this point, is that correct?

Mr. KRUSH. That is correct.

Ms. BONAMICI. Okay. I just want to clear that up because the title of the hearing suggests that one of the consequences of signing up through HealthCare.gov is going to be identity theft. So I wanted to clarify that.

So I—my time is expired. Thank you, Mr. Chairman. I yield.

Chairman SMITH. Thank you, Ms. Bonamici.

The gentleman from Texas, the Chairman Emeritus Mr. Hall, is recognized for questions.

Mr. HALL. Thank you, Mr. Chairman, and thank you for the hearing and the witnesses. I like old-fashioned people. I don't know why. But I will ask my fellow Texan there, Mr. Gregg. There has been talk about March the 31st, and I think you mentioned that since the deadline for open enrollment is not until March the 31st, wouldn't hackers be kind of foolish to exploit the website now because they potentially would have the opportunity to retrieve a heck of a lot more information after that date?

Mr. GREGG. Well—

Mr. HALL. Do they think like that or is that too—

Mr. GREGG. No, sir. They do in many ways look for the big payoff, and as was mentioned earlier, cybercrime can be broken down into two areas. One is the individuals looking for military, looking for that type of information, but a big other portion of it today is monetarily driven. We see a lot of that out of places like Eastern Europe. We see it out of places like Russia. And those individuals are looking for personal information. They are looking for things that they can make a financial payoff from. And to wait until the time was right would very much be to their advantage. While it is true information is not held on HealthCare.gov, information is passed through that site that they could potentially manipulate or take advantage of.

Mr. HALL. Thank you. And I have heard of a lot of problems, but given the problems of the website to date, would you say it is highly likely that there will be breaches to the healthcare website?

Mr. GREGG. Yes, sir. I do believe it is very possible or it is probable at this current state of the site that that could happen.

Mr. HALL. And once one has occurred, how quickly can experts find out about the breach?

Mr. GREGG. That all depends. We have seen in previous cases with things like Gh0st RAT, GhostNet Trojan. We have seen in cases like with Google and Aurora and others, in some instances those organizations didn't know until weeks or months later.

Mr. HALL. How quickly should the American people be notified in the event of a breach?

Mr. GREGG. Immediately.

Mr. HALL. Within hours, days, weeks, or just right now?

Mr. GREGG. Right now.

Mr. HALL. That is pretty clear. Once a breach has occurred and people have been notified, what actions should people take?

Mr. GREGG. Immediately start to do things like Dr. Ponemon mentioned as far as change passwords, change IDs, especially notify and talk to your credit card companies—

Mr. HALL. Now is—

Mr. GREGG. —look at your credit card statements, also check your credit rating and look at the credit rating organizations because many times, just like a period of about a week ago I got an email from Amazon that someone tried to open up an account under my name and I immediately called my credit card provider and found out someone had charged about \$5,000 worth of merchandise under my name because someone had stolen my credit card. So you immediately need to take action for that stuff to put a stop to it if the credit card company doesn't catch it.

Mr. HALL. This is not like Target where you can check with your bank or your credit card company for even suspicious activity or something you think might be happening and that—

Mr. GREGG. That—

Mr. HALL. I think that is what you are telling me.

Mr. GREGG. Yes, sir, that is correct.

Mr. HALL. And how do you find out if—how did you find out if your Social Security number—is that the way they got to you?

Mr. GREGG. No, sir, they got a credit card number from me.

Mr. HALL. Credit card?

Mr. GREGG. Yes, credit card.

Mr. HALL. And if medical information had been compromised, what would you do about it?

Mr. GREGG. It would be very tough. With medical information or someone has intentionally obtained medical services under your name, you may not find out until you actually get the bill, or if they have sent that to another address, you may not find out until you maybe get denied for a job because they said you had a pre-existing condition they didn't know of.

Mr. HALL. Well, just briefly, what are the steps involved in repairing a breach?

Mr. GREGG. It is very tough.

Mr. HALL. And should a website be shut down while these remedies are being considered?

Mr. GREGG. I would say yes, it should, and I mean it is very tough because, first, you have to contest those charges. And if it is related to medical, as soon as you contest it under HIPAA and other laws, then you have no access to the records or information

because it is not your information anymore. So it can be very difficult.

Mr. HALL. Well, my time is almost gone. I believe that all of you would agree that while no website can be 100 percent safe, every precaution needs to be taken to ensure the security of the site.

Now, Mr. Chairman, there are far too many questions surrounding the launch of the healthcare website, and until these are resolved, the security of Americans' personal information is going to remain at risk. That is your understanding. Is that why we are having this hearing?

Chairman SMITH. That is exactly correct, Mr. Chairman.

Mr. HALL. And I thank you for the work on this issue and I thank each of you. And thank you, Mr. Chairman, for a good hearing.

Chairman SMITH. Thank you, Mr. Hall. Would you yield me the balance of your time?

Mr. HALL. I yield my balance of my time today, tomorrow, or next week or any time.

Chairman SMITH. Mr. Kennedy, I would like for you to reemphasize the point you made in response to my initial question about why the government doesn't even know whether it has been hacked or not—that is HealthCare.gov. Why the government really can't say or state credibly that there had been no successful security attacks.

Mr. KENNEDY. Yes, sir. So if you look at the HealthCare.gov infrastructure, it was built independently of HHS, including the Security Operations Center piece. There is contractual language on that. There is testimony from the Congress that also states that as well. So the Security Operations Center, as of November 17, had not been built or implemented, which means that they didn't have the security monitoring or detection capabilities to detect the attacks that are being mentioned here today. So to reemphasize, they don't know.

Chairman SMITH. And they don't know. That is why they can say there hasn't been any. They are not in a position to know one way or the other.

Mr. KENNEDY. That is correct.

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

Mr. KENNEDY. Yes, sir.

Chairman SMITH. The gentleman from California, Mr. Takano, is recognized for his questions.

Mr. TAKANO. Thank you, Mr. Chairman.

Mr. Krush, would you like to respond to that?

Mr. KRUSH. Sure, I would love to. Actually, we have been talking about all of these supposed breaches that have been going on related to HealthCare.gov. If they couldn't monitor those, how in the world do you have a number? The number would be zero if there was no capability to actually look at what kind of attacks are coming through the ether.

Mr. TAKANO. Okay. Thank you very much.

Mr. Gregg, I would like to focus on a couple of areas of your testimony. First, you argue that the site HealthCare.gov really needs a third party working to probe the system for weaknesses; and second, you assert that medical records are at risk on HealthCare.gov

and you list the kind of damage that can be done with stolen medical records. And you state previously in a post—Huffington Post post that “however, the United States has some of the very best minds in the world when it comes to cyber security and there is no doubt that HealthCare.gov can be fixed if the right people are given the chance to test it.” Do you still feel that way?

Mr. GREGG. Yes, sir. That is one of the reasons why I am here today—

Mr. TAKANO. Okay.

Mr. GREGG. —is because I believe with independent third-party assessment and the right assessment done, we can get to the bottom of this.

Mr. TAKANO. Okay. Well, thank you. I just want know were you aware prior to your testimony today that MITRE, Blue Canopy, and Frontier Security were all working on third-party verification?

Mr. GREGG. MITRE, yes; the others, no.

Mr. TAKANO. Okay. You were aware that MITRE was aware, so I don’t understand how, you know, in your testimony you still assert that third-party work needs been done but you had knowledge that a third-party audit was actually being conducted by MITRE?

Mr. GREGG. Yes. One, the article was written before that. It was written before that time. And two, I do not know if MITRE has finished their research or not or what the findings of those are.

Mr. TAKANO. Okay. But you did raise this question as if third-party verification—I was led to the impression that third-party verification wasn’t being done, but in fact, you had knowledge it was being done?

Mr. GREGG. Not at the time of the article.

Mr. TAKANO. Okay. But in your testimony you lead us to believe that you raise it as a concern but it has—

Mr. GREGG. You quoted the article and you quoted a statement directly from the article that I said that needed to be done. At that time nothing had been done.

Mr. TAKANO. But it is not in your—

Mr. GREGG. Is that the question?

Mr. TAKANO. The testimony that you submitted for this Committee doesn’t acknowledge it but yet you are telling me here you had knowledge of it that it was being done.

Mr. GREGG. I—

Mr. TAKANO. Your testimony leads us to believe that it was not being done.

Mr. GREGG. As of this hearing, I do have knowledge.

Mr. TAKANO. Okay. But your—but you—

Mr. GREGG. At the time of the article, no.

Mr. TAKANO. Okay. Okay. Very well. You know, Dr. Ponemon, you talk about the medical records, you know, and identity theft, and a lot of your work has shown that 95 percent of the people who commit these sort of deeds are motivated by Robin Hood motivations. Would you explain about that a little bit?

Dr. PONEMON. It is not 90 percent but it is a large percentage. I think it is 29 or 30 percent, but it is still pretty significant. A Robin Hood crime, as we define it in the research, is where someone, for example, has a family member or friend who basically has an illness and they are not insured and basically they will kind of

look the other way if you will and allow that person to use their insurance credentials so that when they show up at a hospital or clinic, they are getting better treatment than just right off the street.

Mr. TAKANO. Well, common sense would sort of tell me if that is sort of the big motivation, what would motivate someone to go and——

Dr. PONEMON. Sure.

Mr. TAKANO. —try to steal someone's identity, that expanding healthcare coverage, providing quality coverage for more and more people would reduce this—the likelihood of this sort of crime.

Dr. PONEMON. You have to understand I will be biased in that because I think we all deserve good healthcare. So if basically you had good healthcare, the value of a credential would be meaningless, right, because we all have that credential. So there is no value if you will in stealing someone's credential because everyone is going to have a credential that will give them reasonable healthcare.

Mr. TAKANO. So actually, if we made this healthcare website—you know, if it was very successful and more and more people got enrolled, the actual—we would reduce the risk of the misuse of medical records?

Dr. PONEMON. It could work one way or another. It is really hard to determine that. In theory, you are right. I mean you could basically say that 29 or 30 percent, the Robin Hood portion of the crime, the medical identity theft might actually be nonexistent.

Mr. TAKANO. So we would remove—we could possibly remove a huge motive for people to try to hack into this system if they were trying.

Dr. PONEMON. Well, yes, but remember, the value of a medical record is more than just getting the insurance. You see, that is only a very small part of it. There is a lot of information, rich information, and you—we have done studies and the Russian Federation, other parts of the world, and if you had a look at the most valuable piece of information right now on an individual basis, it would be a medical record. And in fact, just yesterday in Fox News, business news, they did an article on the value of different types of information, and medical information in the black market is much, much more valuable than, say, credit or debit card information or authentication data.

Mr. TAKANO. Okay. Well, thank you very much, Dr. Ponemon.

Dr. PONEMON. And thank you.

Mr. TAKANO. Thank you.

Chairman SMITH. Thank you, Mr. Takano.

The gentleman from Indiana, Mr. Bucshon, is recognized for his questions.

Mr. BUCSHON. Well, thank you all for being here. It is a fascinating hearing. We had a previous hearing, which was also very fascinating. And we were four for four no one would get on the website last time, but we are three for four this time.

In my view, this is about confidence the American people have in their government and whether or not their government is doing everything they can to protect their privacy. It is not about healthcare at all. We could be talking about any other website that

the federal government has. And we know the GAO came out and reported thousands of breaches across the federal government, so to argue that this website is going to be secure and that nothing is going to happen I think is a false argument because it is going to be breached. There is going to be information stolen.

I think from my perspective—I was a medical doctor before. I think when you throw in the healthcare part of it, it becomes very personal for people. I understand people out there in my district are concerned about the Department of Defense being hacked, maybe a few people, but when you start talking about the potential for information that they perceive, whether it is real or whether it is perceived, is personal information. I think all of us in hearings like this and across government and the Administration, in both political parties, need to recognize the fact we need to do whatever we can to regain the confidence of the American people that we are protecting their personal information as best we can. Even though I do recognize the website itself doesn't have that on there, it does have portals that people that are smart can potentially access that.

And this is actually one of the biggest problems in electronic medical records, that we have. My medical practice established an electronic medical record in 2005. I love electronic medical records but there are two issues. There is of course security issues and then there is compatibility issues about getting medical information across different types of electronic medical records.

So, I think it is unfortunate that all of you are somewhat subjected to a national discussion about healthcare, and I appreciate all of you trying to confine your comments to the security aspects and not the larger national debate about how we provide quality affordable healthcare to all our citizens, which I think is a goal we all have and certainly as a medical doctor I have. So it really doesn't matter if HealthCare.gov is a low-propensity target by some hackers out there. In the minds of the American people when you mention their healthcare, this is the biggest target in the federal government in their minds. Whether that is real or perceived doesn't really make a difference.

So Mr. Krush, the GAO came out with this report, as you know, in 2012, saying there were 22,156 data breaches, 4,000 at CMS alone. And you have a relationship with CMS so you have to recognize that we can't make the case that any website is going to be secure to try to make a political argument to prove that the way we are managing healthcare is the right way to go. I mean that is not the discussion, is it? The discussion is how do we protect information? You would have to agree with that, wouldn't you?

Mr. KRUSH. I absolutely agree with that. I will just say that I agree with that and with the idea that the process that we use, you know, to secure the data on federal information systems is just very rigorous, and that is my complete argument here.

Mr. BUCSHON. Yes. And I would agree with that. I think when it comes to the confidence, I know we have discussed third-party people out there looking at this. And I will be honest with you. I am a Member of Congress and I have no idea whether there is a third-party person out there—and there obviously is—looking at this. So our charge is to get that to the American people, because if the American people don't know—and I can tell you as a political

person trying to get a message across to 700,000 people is difficult and that is just 700,000 people. We need to do better getting the information out that there are actually people that are in government that are looking at this to preserve people's personal records. That is my view. Mr. Kennedy, how do we do that?

Mr. KENNEDY. Well, I think if you look at the broader picture here and not just HealthCare.gov but just in the federal space, end-to-end testing, proactive security measures, things that are definitely outlined as being best-of-breed security practices need to be performed. And I am not saying that NIST doesn't have those. It is just that they are loosely followed. And, to comply with FISMA is not necessarily a rigorous process.

So what I have to say to that is, we have to focus on putting security in the very forefront, in the very beginning stages of what we hire a contractor or we go after an organization, throughout the entire process of that. HealthCare.gov is a prime example of the failures of being able to implement security in a rigorous manner or in a process that includes security throughout the entire life cycle. And if you do that, you have a better product. You have something that people can stand by and say, listen, we are doing our reasonable amount of assurance here and we are protecting your information, not just, kind of slapping it together and throwing it out there.

Mr. BUCSHON. My time is expired. I would like to say let's all of us work together to regain the confidence of the American people. Thank you.

Ms. EDWARDS. Parliamentary inquiry—

Chairman SMITH. Thank you.

Ms. EDWARDS. —Mr. Chairman.

Chairman SMITH. Thank you, Dr. Bucshon.

I am sorry?

Ms. EDWARDS. Mr. Chairman, I have a parliamentary inquiry.

Chairman SMITH. The gentlewoman is recognized for her parliamentary inquiry.

Ms. EDWARDS. Thank you. Mr. Chairman, isn't it true that the Committee and House rules require witnesses to submit factually correct financial disclosures forms?

Chairman SMITH. There are certain limitations to that, but within those limitations, I think that is the case and I think all of our witnesses have done so today.

The gentleman from—

Ms. EDWARDS. Mr. Chairman?

Chairman SMITH. Yes. The gentlewoman continues to be recognized.

Ms. EDWARDS. Mr. Chairman—

Ms. JOHNSON. Point of order—

Ms. EDWARDS. —I yield to—

Ms. JOHNSON. Point of order, Mr. Chairman.

Chairman SMITH. The gentlewoman is recognized.

Ms. JOHNSON. I make a point of order that the witness testifying today has not complied with the House Committee's rules regarding financial disclosure. And under those circumstances, I request that the testimony be stricken from the record. I am very—

Chairman SMITH. Obviously, I object to that and—

Ms. JOHNSON. I expected that.

Chairman SMITH. —I am afraid that the gentlewoman is not the one to make that determination.

Ms. JOHNSON. I am not finished.

Chairman SMITH. Well, does the gentlewoman have—

Ms. JOHNSON. I am recognized, Mr. Chairman, and I have—

Chairman SMITH. Does the gentlewoman have something to say that is pertinent to her inquiry?

Ms. JOHNSON. —not finished my statement. I am very concerned about the testimony we heard from Mr. Kennedy a moment ago. He testified on the record that he did not disclose government contracts in his truth-and-testimony form that he and his company have received, and our Committee Rules require—

Chairman SMITH. He also said he was not—

Ms. JOHNSON. —a witness disclosure—

Chairman SMITH. —required under the—

Ms. JOHNSON. —requirement to be filed out by each—filled out by each witness. On that form Mr. Kennedy answered the question saying “not applicable.” This means that he did not comply with the rules of our committee, and as such, I ask that he be removed—

Chairman SMITH. That is not necessarily—

Ms. JOHNSON. —from—the testimony from the Committee—

Chairman SMITH. —a legitimate—

Ms. JOHNSON. —until he accurately and fully discloses the federal grants and contracts that the entity he represents have received on or after October 1, 2011—

Chairman SMITH. Mr. Kennedy, do you want to respond whether you were required to disclose that or not?

Mr. KENNEDY. Thank you, sir. The question was have I done work in the federal space prior in the past or currently. The answer to that is on behalf of TrustedSEC, we do not work in the public sector or government, which is what I disclosed in the statement there. In addition, I have worked for NASA as well as other federal government agencies in my capacity as a Chief Security Officer for a Fortune 1000 company, as well as my prior roles as a security consultant for former entities. So to answer the question there on what was submitted, I do not do work for the public sector. I am plenty busy in the private sector keeping everybody else protected. Thank you.

Chairman SMITH. Thank you, Mr. Kennedy. I think you have answered the question.

And I would like to continue our questions. And the gentleman from Massachusetts, Mr. Kennedy, is recognized for his.

Mr. KENNEDY OF MASSACHUSETTS. Thank you, Mr. Chairman, and thank you to the witnesses for being here today.

I want to start out by saying I know—I think Teresa Fryer was mentioned earlier in this hearing, and I know that she is actually testifying I think at this moment or just moments ago in front of the Committee on Oversight and Government Reform. And her testimony before was referenced about—some of the—her remarks on HealthCare.gov and she just recently said today that the HealthCare.gov website is secure based on a December 18 security assessment. She stated that the system exceeds the best practices

to ensure security and that the risk mitigation policies are being implemented and executed as planned. As a result, attacks have been successfully prevented. She recommends that a new ATO should be given when the current one expires just to make sure that we are all up to date on the current testimony.

Now, a couple of, I think, points of clarification: Mr. Kennedy, I think one of us here supports the ACA, but I will leave that up for the gallery to decide. The—now, I noticed at the—I think in your initial testimony and the initial testimony of the witnesses, you were nodding your head when Mr. Krush said that unless you are actually able to dive into the inner workings of the website, which you have made clear that you did not hack into, you did not do anything illegal, but that you would not have any way of knowing in detail what part was vulnerable to attack unless you had done so. Is that accurate?

Mr. KENNEDY. We can't tell the inside of HealthCare.gov without actually testing it. That is 100 percent accurate. What we can see are symptoms of a much larger issue. And if you wouldn't mind for just—if I can read a—one of the things that I submitted from Ed Skoudis just as an example if you are okay with that, sir.

Mr. KENNEDY OF MASSACHUSETTS. Yes, go ahead.

Mr. KENNEDY. Thank you. Mr. Skoudis said, "I have worked on dozens of large-scale breach cases over the past 12 years looking at the root cause of vulnerabilities of attacker methods. Reviewing the security issues discovered in HealthCare.gov, I can tell you this is a breach waiting to happen. Or given the numerous vulnerabilities, perhaps a breach has already happened. These are exactly"—and he emphasized on that—"the kind of security flaws bad guys exploit on large-scale breaches."

Mr. KENNEDY OF MASSACHUSETTS. So, Mr. Kennedy—and I appreciate that, but the point is—and I think we have heard it actually reiterated a number of times here—is that we don't know. You don't know. You testified before that HHS doesn't know. If HHS doesn't know, you don't know, so much of this is in fact—it is a concern but it is speculative, right?

Mr. KENNEDY. It is an underlying portion of HealthCare.gov, absolutely, yes.

Mr. KENNEDY OF MASSACHUSETTS. Okay. So—now—thank you. And, Mr. Krush, do you—out of your expertise, can you just give me off the top of your head what you believe to be the biggest data breaches—recent data breaches? This is something that is fairly common. Obviously, Target and Neiman Marcus in the news today. How many—are you aware of others?

Mr. KRUSH. Well, interestingly enough, you know, the thing—when it comes to data breaches, I think Target is a perfect example of someone that had the capability to identify a breach. The thing that is of most concern to me is that there are a lot of industry and even government organizations that don't have the capability to do that.

Mr. KENNEDY OF MASSACHUSETTS. So, sir, Target, Neiman Marcus obviously in the news now. Do you recall Heartland Payment Systems data breach back in 2008? Does that ring a bell with you?

Mr. KRUSH. It does.

Mr. KENNEDY OF MASSACHUSETTS. At least from some estimates 134 million credit cards exposed. How about TJX Companies in 2006, 94 million credit cards exposed; Epsilon, which exposed the emails of millions of customers stored in over 108 different retail chains; RSA Security, top-notch security firm; Sony Playstation Network, over 77 million Playstation Network accounts exposed, all private sector, yes?

Mr. KRUSH. Yes.

Mr. KENNEDY OF MASSACHUSETTS. This is something the private sector invests billions of dollars a year in trying to protect, yes?

Mr. KRUSH. Yes.

Mr. KENNEDY OF MASSACHUSETTS. This is something that is very difficult and has to be on the cutting edge in order to defend against, yes?

Mr. KRUSH. Yes.

Mr. KENNEDY OF MASSACHUSETTS. Are you aware of how many times the House of Representatives has voted to cut funding or appeal the Affordable Care Act this Congress?

Mr. KRUSH. I am not.

Mr. KENNEDY OF MASSACHUSETTS. Would the number close to 50 seem accurate to you?

Mr. KRUSH. Unfortunately, I just don't have that insight.

Mr. KENNEDY OF MASSACHUSETTS. Okay.

Mr. KRUSH. I can talk about risk assessment—

Mr. KENNEDY OF MASSACHUSETTS. Well, take my word for it.

Mr. KRUSH. —if you like.

Mr. KENNEDY OF MASSACHUSETTS. Take my word for it.

I yield back the balance of my time.

Chairman SMITH. Thank you, Mr. Kennedy.

The gentleman from Oklahoma, Mr. Bridenstine, is recognized for his questions.

Mr. BRIDENSTINE. Thank you, Mr. Chairman. I appreciate the time.

I would like to start by asking our witnesses a question. Are you familiar with Tony Trenkle? He was the Chief Information Officer for the Centers for Medicare and Medicaid Services. And his job was to oversee the development of HealthCare.gov and his job was to,—as—you know, the last thing before launching the website he had a security waiver he was supposed to sign. Do you guys remember any of this by chance? And he didn't sign it. He refused to sign it and he resigned. His boss, Marilyn Tavenner, CMS Administrator, who is not a Chief Information Officer, who arguably would not be qualified to sign off on a security waiver, she signed it. He didn't. He is qualified. She did, she is not qualified. She is an appointee of the President of the United States.

Interestingly, her boss, Secretary of Health and Human Services Kathleen Sebelius, testified before Congress that she had no idea that a security waiver was supposed to be signed, that it didn't get signed, and that her subordinate, another Barack Obama appointee, signed it. She didn't know. It would seem to me you have a qualified person not signing it and then having to resign, and the Administration was not clear about why that person had to resign, namely Tony Trenkle. In fact, they didn't answer the question why. But it would appear—and this gives me concern—that people are

making decisions for political reasons, not in the best interest of security of our citizens.

And so some of you on this panel are CEOs, I think three of you. And then, one leads a research institution. Just a quick yes-or-no answer, in your institutions if this was going on, would you guys have an issue with it? Would somebody in your organization be fired? We will start with you, Mr. Kennedy, and just go down the row.

Mr. KENNEDY. Coming from being a Chief Security Officer for a Fortune 1000 company, I would say the answer to that would be yes. That would raise a major concern for me.

Mr. KRUSH. I would just talk to the point that the authorizing official, if it was the CSO and he or she was the one authorized to sign for the system, you know, this is actually one of the breakdowns in the risk management framework right now. You have what is called—you usually have the CIO or the director that are in charge of maybe a program, an organization, and they are directed as the authorizing official. I would say if we are going to look at one of the weaknesses in the process government-wide is that that Chief Information Security Officer should be where the buck stops always. Right now, there is—

Mr. BRIDENSTINE. So you are acknowledging that he should have signed it if it was secure, and his refusal is a big breach of trust here with the American people?

Mr. KRUSH. I acknowledge that under the current process—

Mr. BRIDENSTINE. And then he was forced to resign, arguably.

Mr. KRUSH. The current process allows for the authorizing official to be whoever is directly in charge of the entire information system. So, that being said, I think that that is a weakness in the process. Right now, it should be the Chief Information Security Officer where it stops. They are supposed to know the system, the security capabilities, and they are supposed to be the ones that should be responsible, but that is not the process that we are currently using in the government.

Mr. BRIDENSTINE. Well, it was the process that was supposed to be used until he refused and then resigned. Going down the line?

Mr. GREGG. I would also say yes and I would add to that that, as we talked about earlier, with external third parties looking at this, that is just a piece of it, them looking at it. The other part is those items are actually implemented and they are signed off on.

Dr. PONEMON. It is my turn, I suppose. Yes, it is a big ethical issue in my opinion. I think the key variable is that the security of our country and the citizens of our country should be more than a political issue.

Mr. BRIDENSTINE. Agreed.

Dr. PONEMON. But I don't think the solution is to have local CSOs, people who are middle-level management. It should be a major, major function of the government to have a CSO for the entire United States and then—

Mr. BRIDENSTINE. I am going to bring back my time. I have only have 30 more seconds but I appreciate your answer and you can submit it for the record.

Dr. PONEMON. Absolutely.

Mr. BRIDENSTINE. But I would like to just say that I am not going to put this in for the record, Mr. Chairman, because I don't want it to create any issues on the other side of the aisle, but this comes from an article from CBS News dated November 6, 2013. So people watching at home have access to it. It is on the internet. It has all been disclosed.

And I would like to say, finally, in my last five seconds this is exactly why the American people have lost trust in their government. This is exactly why the American people have lost trust in their government.

Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. Bridenstine.

The gentleman from Illinois, Mr. Hultgren, is recognized for his questions.

Mr. HULTGREN. Thank you, Mr. Chairman. Thank you all for being here. This is such an important topic and something I am certainly hearing from my constituent as I travel around my District of great concern and wanting answers and so I appreciate you being here.

I have got a couple of different questions. I am going to address the first one to Mr. Krush if I could. According to your written testimony, you say that based on what you have read publicly thus far, "HealthCare.gov is most likely categorized as a moderate system referring to the National Institute of Standards and Technology or NIST's security levels of low, moderate, and high." I wonder, is that an appropriate categorization for this kind of personal data that we are talking about here being available and accessible through the HealthCare.gov website, including people's medical files?

Mr. KRUSH. So usually we reserve high for, you know, grave danger to national security, to the confidentiality, integrity, and availability could, you know—for most of the high systems. So usually to me when something is categorized with that, it is usually life or death. And since HealthCare.gov is not that, it—there are some areas where, depending on the organization, there is something called organizationally defined parameters. That allows the organization to say if they process, store, transmit, manage, or review privacy data, it allows them to make the recommendation to go to high. But from what I have read thus far about the site, because of the interactions with the other websites, meaning the handing off through the controlled APIs and the way that it deals with interconnections, it still would be moderate. If one of those interconnections are high, then they—then what they have to do is actually—they do—well, we are going to do this anyway. They have to develop what is called an ISA, an Interconnection Security Agreement. And what that requires both sides to do is agree on the cyber security rules, including on how quickly they report any instance related to those.

Mr. HULTGREN. Let me jump in here real quick. I would say again for my constituents this is of high concern to them and I think for us as well. And I would agree with my colleagues of how important this is in people's lives. And, boy, talking about medical care, it sounds like life and death to me oftentimes is making sure that our medical records are protected.

I am going to jump to Mr. Gregg. Is there any evidence that HealthCare.gov meets NIST's data security standards and who should certify that HealthCare.gov complies with the Federal Information Security Management Act?

Mr. GREGG. I have not seen that evidence as far as whether or not they have been certified so I cannot say on that.

Mr. HULTGREN. Okay. Let me open this up to any others. Mr. Kennedy, Dr. Ponemon, let me open this up to you all, any thoughts you might have. National Institute of Standards and Technology, NIST again, provides agencies with the guidance they need to develop and launch networks and websites that are fully and properly secure. Should NIST's role be expanded or increased with any new authority and responsibility specifically in regards to HealthCare.gov? Would NIST be best qualified to verify and certify how well agencies meet their security standards' compliance? And in today's case, should NIST review HealthCare.gov? Start with Mr. Kennedy.

Mr. KENNEDY. I would agree with that. I think if you look at not just technology-specific areas. You have the CDC, the Centers for Disease Control. Prevention, which is really about getting information to the American people about diseases, things like that. The same oversight needs to be there and the expanse of NIST needs to be there for more of a governance structure over our security practices inside the government. Again, NIST is more of a guidance role right now to adhere to. I think the expansion on this is really to bring more security integration throughout the whole government, the whole federal government, to really build best practices in. Right now, it is kind of intermittent not whether they do it or not. So I agree that, yes.

Mr. HULTGREN. Okay. Any other comments or thoughts?

Mr. KRUSH. They currently write the guidelines, the NIST—National Institute of Standards and Technology special publications and also they write different guidance on different types of technologies. I think just understanding systems from a risk perspective, if you have one organization that is in charge of the information security for every single government organization, it is—you will never come to the same risk decision. The problem lies in the fact that somebody at HHS is going to know about HHS systems and the security and the requirements better than someone, you know, in an office somewhere up at NIST.

Mr. HULTGREN. I think that my fear is accountability, too. Sometimes I see it in bureaucracies, there is a desire to protect, hey, if we have a breach, don't let anybody know. I want to make sure that doesn't happen.

Mr. Gregg, do you have any thoughts on this?

Mr. GREGG. No, but I would agree many times this stuff is covered up and it is not released immediately. We even see with Target that we are getting some information, but yet to see the full picture.

Mr. HULTGREN. Okay. Dr. Ponemon, real quick, what are some of the serious consequences that consumers face in the wake of medical identity theft? Are there financial consequences in addition to medical consequences?

Dr. PONEMON. Yes, and our research we find that a fairly large percentage of our sample suffered some financial consequences, and sometimes it is just staggering. It could be thousands or tens of thousands of dollars. Keep in mind that the people who are at risk are not necessarily wealthy people, people who are low income. And so on a proportional level it could be their total yearly income just basically the costs associated with cleaning up your medical record.

Mr. HULTGREN. Doctor, you are right, and I think that is my fear is those who are most vulnerable are right on the edge—

Dr. PONEMON. Absolutely.

Mr. HULTGREN. —something happens there, they don't have anything to fall back on. People with significant resources do.

Thank you again for being here. Chairman, I appreciate the opportunity and I yield back.

Chairman SMITH. Thank you, Mr. Hultgren.

The gentleman from Texas, Mr. Weber, is recognized for his questions.

Mr. WEBER. Thank you.

Mr.—is it Krush or Krush? I have heard it both ways.

Mr. KRUSH. It is Krush but in the Army I used to say Krush.

Mr. WEBER. It is Krush, okay. All right. Well, just call you for dinner is the main thing, right?

Mr. Krush, you said, I think, that you were lucky enough to have worked for the HHS or was it the CMS?

Mr. KRUSH. So I was fortunate enough to work early on on the central office at HHS.

Mr. WEBER. Okay.

Mr. KRUSH. I have also provided training actually related to the risk management framework and we develop online training for CMS.

Mr. WEBER. I want to draw attention to the word luck. You said you were lucky but then later you said you had contracts totaling around \$10 million? \$1 million? \$10 million?

Mr. KRUSH. \$1 million.

Mr. WEBER. \$1 million. Okay.

Mr. KRUSH. But I would say when I was talking about luck, I was actually talking about the individuals that are at the central office are probably some of the most talented cyber security people I have met. And that is just the truth. I have worked with them when they were contractors and now they are—

Mr. WEBER. Okay. And then you said I am working for the CMS—and I wrote it down—you weren't "best of friends" with—

Mr. KRUSH. That is correct, with CMS.

Mr. WEBER. —was the words you used.

Mr. KRUSH. We actually had a recent protest with them.

Mr. WEBER. Okay.

Mr. WEBER. But you had government contracts so you might not have been best of friends, but you weren't enemies, right?

Mr. KRUSH. Absolutely not.

Mr. WEBER. Yes, you weren't enemies. It wasn't maybe a marriage, but at that dollar rate, you might be interested in a long-term relationship? What do you think?

Mr. KRUSH. At those dollar amounts—

Mr. WEBER. Yes, sir.

Mr. KRUSH. —a long-term relationship? If it was a little bit more probably.

Mr. WEBER. Okay. I see. You are going to play hard to get. So were you hired on experience and good performance?

Mr. KRUSH. Absolutely.

Mr. WEBER. Okay. So you think performance is important?

Mr. KRUSH. Absolutely.

Mr. WEBER. So would you say that the performance in rolling out HealthCare.gov was sterling or problematic?

Mr. KRUSH. It was problematic.

Mr. WEBER. Very problematic. Can you understand how some Americans would question the ability of the company that put together HealthCare.gov?

Mr. KRUSH. I can.

Mr. WEBER. Sure, makes sense. So it is no surprise to you that their credibility has been called into question.

Mr. KRUSH. Um-hum.

Mr. WEBER. Do you fault us for doing our due diligence to try to protect the American public?

Mr. KRUSH. I do not.

Mr. WEBER. So you think it is a good thing what we are doing here?

Mr. KRUSH. I think that every time—unfortunately, we are as a nation fairly reactive, just like, you know, industry. We wait until something big happens before we talk about it. You know, cyber security—

Mr. WEBER. That is a yes or no. It is a good thing we are doing here because I am running out of time.

Mr. KRUSH. Oh, absolutely it is a good thing—

Mr. WEBER. Yes, good. Well, I am glad—

Mr. KRUSH. —to talk about it.

Mr. WEBER. Good. I am glad to hear you say that.

Mr. Kennedy, you also think it is a good thing?

Mr. KENNEDY. Absolutely I do.

Mr. WEBER. How about—Mr. Gregg?

Mr. GREGG. Yes, I do.

Mr. WEBER. Doctor?

Dr. PONEMON. Yes, I do.

Mr. WEBER. Okay. Well, I am glad to hear that we are finally doing something that is advantageous. You know, that is kind of rare for Congress.

Mr. Krush, on February the 19th, 2013, you tweeted “don’t just worry about China breaking into systems.” And then you went on Fox News and talked about it. Do you recall that?

Mr. KRUSH. I don’t remember that tweet but, yes, I am very—actually, I don’t tweet that much at all but I did go on Fox News related to the APT, correct.

Mr. WEBER. Yes, I know. You don’t do a lot of tweeting. I looked at them.

Mr. KRUSH. Yes.

Mr. WEBER. When you tweeted out “don’t just worry about China breaking into systems,” what did you mean by that?

Mr. KRUSH. Actually, I think, sir, that was probably—when I was tweeting, I just reposted a news article and that was probably just the title.

Mr. WEBER. But you recognize that we have a lot of cyber security attacks hitting our government, like a million a year.

Mr. KRUSH. Oh, absolutely. I have helped to develop many security operation centers in the government and industry, and there are organizations constantly knocking at our door and trying to knock it down.

Mr. WEBER. But China would only attack those military websites. They would never go for HealthCare.gov, would they?

Mr. KRUSH. Interestingly enough, most organizations, you know, state-sponsored organizations—and I put this in my testimony—they are always looking for jump points, .gov, .mil, period.

Mr. WEBER. So the people in China that are attacking us, is their level of proficiency low, medium, high?

Mr. KRUSH. Very high.

Mr. WEBER. So we are well advised to warn the American people that they are going to have information on HealthCare.gov that may be spread across the globe?

Mr. KRUSH. You are well advised to warn everybody in the federal government and even in industry that cyber security and privacy absolutely needs to be one of your top priorities.

Mr. WEBER. Okay. Well, I appreciate you understanding that, Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. Weber.

The gentleman from New York, Mr. Collins, is recognized for his questions.

Mr. COLLINS. Thank you, Mr. Chairman. And I find that it has been about two months since our last meeting. Mr. Kennedy, welcome back.

As one of the last witnesses, I tend to see that there are times people will try to defend the indefensible, and the best way to defend the indefensible is to confuse the issue and muck it up and raise other things. I have heard and seen some of that today. So I would like to come back here at the end and remind everyone that all four witnesses last time, including the Democrat witness, testified absolutely the website was not secure on October 1. They testified that absolutely the website was not secure on November 19. We couldn't get agreement as to whether we should shut it down immediately or not, but the testimony indicated that October 1 was a date certain set by the Obama Administration to launch HealthCare.gov irrespective of whether it was ready, and I think the American public know it was not ready.

So I think it brings into question if it was a date certain, it wasn't let's launch the website when it is ready. Let's launch it when it will do the job and handle the traffic. Let's launch it when it was secure. No. It was let's launch it on October 1 because we promised it would be October 1 whether it is ready, whether it is secure, doesn't matter. Launch it. And we did. And the American public in watching this hearing can see for themselves that that was the overriding concern, certainly not security.

So now, here we are today, and yes, we have a different witness, but I guess I would ask our witness, Mr. Krush, whether you think

the website was ready to be launched on October 1 or not? That is a yes or no.

Mr. KRUSH. That is a no.

Mr. COLLINS. And do you think it was secure then on October 1?

Mr. KRUSH. So if you have read my testimony and my previous testimony, you will see that I said the process was followed and a risk-based decision was made. That is why it is called risk management framework and not the no-risk process.

Mr. COLLINS. So I guess what I come back to here is that there are those today that tried to say this was a politicized hearing and so forth, which I don't think it is. I think we are just back to talking to the American public who are being told that, to sign up, they must share this delicate information, including Social Security numbers.

I think the fact that Target or Neiman Marcus happened to have had their issues doesn't defend this. Two wrongs don't make a right by any stretch of the imagination. But I am trying to point out and remind folks this website was launched on October 1 for only one reason: political reasons. It was not ready. The Administration knew it was not ready. If it is not ready, it is not secure. It wasn't secure. We know it wasn't secure. Now, we are being told today to trust the Administration and, Mr. Krush, to trust some of your judgment. Something happened in the last week or two or month. It is now secure. Well, I guess I am not quite ready to accept that just because you say it is so. That doesn't necessarily make it so. So, I am just trying to bring us back to where we were October 1, where we were on November 19, where we are today. And certainly, I am confident three of our witnesses today, Mr. Kennedy, do you think it is secure today?

Mr. KENNEDY. Absolutely not.

Mr. COLLINS. Mr. Gregg?

Mr. GREGG. No, I do not. And usually when sites are rolled out, they are rolled out in a beta first—

Mr. COLLINS. Right.

Mr. GREGG. —very small group, and then to a large group.

Mr. COLLINS. Mr. Ponemon, do you believe it is secure today?

Dr. PONEMON. You know, it is hard to tell. I am not—these people are the experts, but they simply—based on what I am hearing, again as a citizen of this country, I am concerned. I am not happy with what I am hearing here today.

Mr. COLLINS. Okay. And, Mr. Krush, I will let you answer that as well, please.

Mr. KRUSH. I think my testimony and everything I have been saying here is none of us worked on HealthCare.gov, so speculating that it is either secure or not is just not something I am willing to say.

Mr. COLLINS. So you would say today you would not state affirmatively to the American public that it is secure?

Mr. KRUSH. Based on the information that I have read, a risk-based decision was made. There was a mitigation strategy that was very clear. They are doing weekly scans. They are doing daily scans. They are doing mitigation and remediation.

Mr. COLLINS. Okay. I was kind of hoping for a yes or no.

Mr. KRUSH. I would say that is pretty secure.

Mr. COLLINS. So you are stating, yes, it is secure?

Mr. KRUSH. I am stating based on the information I have right now I would say it is secure.

Mr. COLLINS. Okay. Well, we can have that difference of opinion and I guess I will leave it at that for the American public to make their own decisions.

Mr. Chairman, I yield back.

Chairman SMITH. Thank you, Mr. Collins.

The gentlewoman from Illinois, Ms. Kelly, is recognized for her questions.

Ms. KELLY. Thank you, Mr. Chair.

Mr. Krush, unlike some of the other witnesses, you have extensive experience working on federal government websites from the inside developing countermeasures against potential attacks and ensuring that websites are as secure as possible. Is it true that what might appear like a security vulnerability or even a successful exploit from the outside does not actually always result in a security threat?

Mr. KRUSH. That is correct, Ms. Kelly. Actually, we like to set up things called honey pots meaning that we will set up—we want to know what the attackers are actually doing to our websites and our systems, so we set up ports, protocols, and services that may not have anything to do with the website to kind of find out who is coming in, what they are doing, and so that we can then build countermeasures internally to deal with those type of things.

Ms. KELLY. I have also been told that a site security team will leave the appearance of a weakness in place so that hackers will waste their time. There are other times, as I understand it, seeming weaknesses are purposely put in place and what IT professionals—like you just said, honey pots, where a genuine hack or even a white hacker gets caught trying to penetrate a system. And you just said that that was true. Do you imagine with HealthCare.gov that is—honey pots are in place or—

Mr. KRUSH. So, Ms. Kelly, because I didn't set up the honey pot, I can't speculate on that either, but it is a very normal practice and best practice in the government to set up honey pots so that we can understand what our adversaries or external organizations are trying to gain access to and what type of things they are actually doing to our websites.

Ms. KELLY. Okay. And lastly, the HealthCare.gov website uses remote authentication to help verify that the users are who they claim they are in order to help cut down on medical fraud. These sorts of security practices can sometimes make websites clunky and the user interface problematic. Can you address this issue for us? Is it possible that these sorts of kinks and glitches experienced on HealthCare.gov were due to its enhanced security measures by any chance?

Mr. KRUSH. The great thing about security is if it is done right, it won't work. No, I am joking. So a lot of times when we lock down systems in the federal government, if we followed every single security control that is put forward for us, we would turn that box or that system into a completely unusable, you know, locked-down box meaning I couldn't log into it as an administrator but neither could you. So what we do is we look at the controls from a security engi-

neering perspective and decide what are the best, you know, security controls to implement and how that is going to affect our operational user base. And so to answer your question that is a possibility but I didn't actually do the identity management system so, once again, I can't really talk to that fact.

Ms. KELLY. Thank you so much. I yield the rest of my time.

Chairman SMITH. Okay. Thank you, Ms. Kelly.

I don't see any other Members here to ask questions so this concludes our hearing today. Thank you all again for your contributions to the subject at hand. We heard a lot of good testimony and we will continue to be in touch.

We stand adjourned.

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

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. David Kennedy

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“Healthcare.gov: Consequences of Stolen Identity”**QUESTIONS FOR THE RECORD****Mr. David Kennedy****Chief Executive Officer, TrustedSEC, LLC****Questions submitted by Chairman Lamar Smith**

- 1) In what appears to be a contradiction of your testimony, the Administration claims that “when consumers fill out their online Marketplace applications, they can trust that the information that they are providing is protected by stringent security standards.”¹ How do you respond to such a claim?

Security was not built into this site or the supporting sites that support the healthcare.gov website. There is a serious concern around even the basic level of security that supposedly was built into the site. Just recently it was reported in the WeeklyStandard (<http://www.weeklystandard.com/blogs/opportunistic-marketers-exploit-opening-healthcaregov-775259.html>) that the data.healthcare.gov site was being used to deliver malicious software under the guise of being a legitimate site. This functionality has since been removed but shows the extent of the website's security vulnerabilities. Additionally, there are alleged ties to developers inside Belarus (a strong ally of Russia) and possibly placed backdoors into the code allowing foreign government access (<http://freebeacon.com/the-belarusian-connection/>). Regardless if this story pans out to be true or not – it's apparent that there isn't even knowledge of who developed portions of the website, where they originated from, and what code they actually developed. Another example of systematic failures to develop a website with security in mind.

- 2) HHS says they are conducting 24-7 system monitoring and constantly probing and scanning the system? What does this mean, and is it significant and adequate?

Unfortunately there is not much detail in what that means, if they have a dedicated monitoring and detection program that looks at all areas of the infrastructure (including web applications, network based attacks, and other intrusions), then it will be good. However, based on the vagueness, it is difficult to determine what “24/7 monitoring” means. I think more clarification needs to be made on what type of monitoring and detection capabilities is being performed and to what extent.

- 3) Do you know if Healthcare.gov encrypts its data at rest and when in motion, and if not, should it?

¹ <http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr3811h20140109.pdf>.

There hasn't been any public information released to my knowledge regarding the protection around personal information. Data at rest and data in transit/motion should be a mandatory step in the entire process. There are multiple points in when PII is stored including the front-end application as well as the integration into other government agencies and third parties. They need to be encrypted, utilize appropriate standards for encryption (FIPS as an example) and should be mandatory.

- 4) What is your understanding of the data hub and central storage facility for Healthcare.gov? Is the data stored on specific premises or within a cloud application?

My understanding is that PII is stored locally on the web application as well as verifications and information that pass to multiple other government agencies as well as third party systems to verify that the information is accurate and provide accurate quotes for insurance plans. Based on the information that's already public, it would lead me to believe that information is stored on site at the healthcare.gov application as well as within cloud applications

- a) Does a cloud application make the data more susceptible to security breaches by third parties? For example, is it possible for data to go offshore?

In a cloud infrastructure, a number of security controls go out the window. Typically you do not have access to the same types of logs, technology, reporting, and detection capabilities when you move to an outsourced provider. Additionally you cannot attest to the security controls in the environment itself other than what is provided by the cloud provider. I am and have been vocal around the security implications of moving to the cloud and believe it to lessen security in a number of ways.

- 5) A December U.S. Government Accountability Office (GAO) report on government information security documented a 111% increase in Federal agency data breaches in the past three years. Specifically, the GAO report noted that there were 22,156 incidents revealing sensitive personal information in 2012, up from 10,481 in 2009. The Centers for Medicare and Medicaid Services, the Healthcare.gov operator, had the second most breaches in the report for FY 2012 at 4,172. What do you conclude from these statistics?

That the federal and state governments are a high value target for attackers both from a state sponsored/actor perspective as well as organized crime. These statistics will continue to move up and continue to escalate due to the lack of formal security testing in our process in the federal and state levels. Based on the statistics and the Center of Medicare and Medicaid Services having the second largest number of incidents would indicate they are one of the top targets for attackers right now.

- 6) What is the most effective and efficient way to address security concerns on Healthcare.gov - should the website stay up or be taken down while being fixed?

I think before taking it down right now, a full review should be performed in order to identify the level of risk associated with the website. If my analysis is correct, the site has extensive and systemic issues that reach to the inner core of the environment and to the data hub environment and will be a critical or high-risk situation. If this is the case, we should consider taking it offline in order to address fully the identified security concerns.

- 7) The House recently passed legislation requiring the U.S. Department of Health and Human Services to inform individuals within two days if their personal information has been stolen or unlawfully accessed through an Obamacare exchange. Is this an undue burden on the government, or is such a requirement outweighed by the benefit given what can happen when one's identity is stolen or compromised?

I believe that this legislation is needed and should be expanded past the healthcare.gov infrastructure. Our personal information is at risk and there is little being said around what is occurring to address the issues with the website. This should be a mandate initially within the healthcare.gov infrastructure due to how large the population of PII is and to make sure people's information is protected. I do not believe that this is unreasonable or a burden on the government to provide this type of information – on the contrary, it's providing U.S. Citizens with the information they need to ensure their information is adequately protected.

- 8) In December, every Republican Member of this Committee sent a letter to the President requesting information and an explanation of the security risks and privacy concerns with the Obamacare website. The Committee has received no reply, nor even an acknowledgement.

I believe that these are reasonable questions and ones that should be answered in order to ensure that the security around the website and its infrastructure is adequate and within best practices. There still hasn't been a definitive answer on what exactly is occurring to protect the information that is placed on the system, and to me that is a large worry and concern because it's an indicator that there isn't anything there to adequately protect the information on the site.

The letter asks three questions:

1. "Since October 1, what explicit steps has the Administration taken to improve the security of Healthcare.gov?"
2. "Who in the Administration has been assigned to monitor, manage, and oversee the ongoing security needs of Healthcare.gov?"
3. "Has the Administration conducted thorough, on-going tests and monitoring of security and privacy vulnerabilities with Healthcare.gov – including hiring private sector 'hackers' to test the website's ability to guard against malicious attack and intrusion?"

Are these reasonable and important questions deserving of a response sooner rather than later?

- 9) What is the likelihood Healthcare.gov being attacked and breached in the next year? How about the next five years? Please provide your reasoning.

I believe it's highly possible that it's already been attacked or breached. I also think that it will continue to be the target for several years to come. Attackers move where the most data exists. There are different interests in the hacking community depending on where the location the attackers are originating. State sponsored for example is looking at it purely from an intelligence perspective whereas others look at it for monetary. The amount of information in the system and the tight integration into DHS, IRS, and others makes it a high value target for attackers let alone the amount of PII that's stored in the system, which could be used for fraud purposes. I believe that the healthcare.gov infrastructure will be one of the most attacked systems in the federal government and experience multiple breaches of personal information in addition to the breaches that may already have occurred.

- 10) The Administration recently fired lead website contractor CGI which was mainly responsible for building the flawed Healthcare.gov website. But the replacement contractor, Accenture, is not without problems either, having "signed a high-profile legal settlement with the Justice Department less than three years ago over its contracting practices."² Should Americans be concerned about this transition from CGI to Accenture?

I believe that regardless of the contractor, the ability to design an effective website under the current conditions is not obtainable. Accenture is a development company with skilled and talented individuals as well as novice to beginner individuals. If security isn't designed into the software development lifecycle of this organization, then when it fixes or changes or enhances healthcare.gov, it will be just as bad as the previous development organization, CGI. I do not believe in any capacity that switching out the company will have any impact on the design or security of the system unfortunately.

² Juliet Eilperin and Amy Goldstein, "Obama administration to end contract with CGI Federal, company behind Healthcare.gov," The Washington Post, January 10, 2014, available at: http://www.washingtonpost.com/politics/obama-administration-to-end-contract-with-cgi-federal-company-behind-healthcaregov/2014/01/10/001eb05a-719e-11e3-8b3f-b1666705ca3b_story.html

Questions submitted by Rep. Johnson and Rep. Edwards

1. In your appearance before the Committee on November 19, 2013, you stated:

Before answering the questions presented, I want to express my disappointment in the tactics being used by Rep. Johnson and Rep. Edwards. Regrettably, not one of their questions appears to address any security concerns affecting the healthcare.gov website or the associated infrastructure. Instead, the questions appear to be an effort to test my credibility. Instead of trying to shore up the website's security, the Congressional representatives attempt to distract the public by attempting to discredit the messenger. From day one, my conduct has been aimed solely at improving the website's security. Thankfully, notwithstanding the Representatives' efforts, progress is being made. Since my Congressional testimony, I have had the privilege of speaking to the HHS Chief Information Security Officer (CISO), Kevin Charest whom reached directly out to me to discuss the concerns. It appears now that a proper focus on security is becoming a high priority versus prior to the hearings, when it was not.

Some of the Representatives' questions lack factual accuracy and give the impression that a significant amount of time was spent trying to create issues designed to discredit my testimony versus taking proactive measures to fix the website. I find it alarming that if a U.S. citizen attempts to communicate with our Federal government on any legitimate issue, the individual is met with an effort to undermine their credibility and stifle their opinions. I for one feel like Rep. Johnson and Rep. Edwards have continued to go after me personally simply for providing accurate information. Additionally, Rep. Edwards intentionally left my military service out of the testimony record and would not recognize my years of service including two tours of duty in Iraq – just because I disagree with her point of view on the subject. As a veteran whom put my life in severe risk and danger during Operation Iraqi Freedom, and during the heaviest parts of the insurgency in the worst parts of Iraq (Sunni Triangle of Death) for the safety and freedom of this country, I find these actions particularly alarming. This is unnecessary and disconcerting given the power she exercises over matters of public interest.

Regardless of the above, I am willing (although not required) to answer some of these questions. Since the November hearing, out of the issues already open and those reported by other security researchers, only one half of one issue was fixed.

"I think we identified around 17 different direct exposures. A lot of these 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."

In your testimony on January 16, 2014, you wrote:

"Since the November meeting, there has been a half of one issue fixed (vulnerability still present with fix is easily bypassed) of the 18 issues identified through passive reconnaissance."

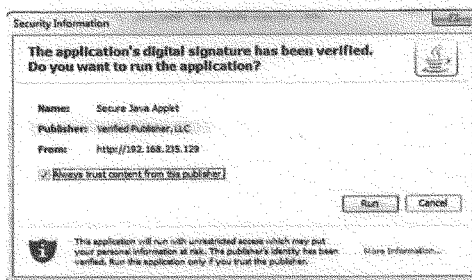
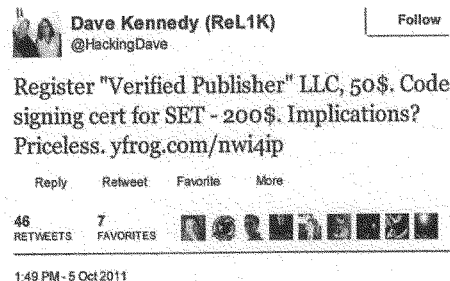
If "a lot" of the issues that you testified to in November (at that time you said the total was 17 issues) had already been addressed at the time of your appearance, how is it possible that the update on your testimony three months later states that only one half of one issue (out of 18) had been addressed? Please explain this apparent discrepancy. If you meant in the January testimony that you found 18 new issues, please indicate when and to whom you communicated those items.

2. In your financial disclosure forms for the two hearings at which you appeared, you disclosed that you were testifying on behalf of both yourself and TrustedSEC at the November 2013 and January 2014 Healthcare.gov hearings. However, public records show that you incorporated a company named Verified Publisher, LLC in Ohio on September 16, 2011 (see attached). One month later, on October 17, 2011, you filed articles of incorporation for TrustedSEC, LLC in Ohio as well. Both of these companies list you as its "Agent." In addition, the "purpose" of each company disclosed in the articles of incorporation are the same: "Any Lawful Act" and the address provided for each company appears to be your home address.

If you have a second company engaged in computer security work, it would seem materially relevant to reveal that to the Committee to understand both the basis of your expertise and your interests in the matters you testified to.

The Committee has been unable to determine what relationship may exist between your two companies, or what kind of work Verified Publisher engages in. However, according to public records on file with the Ohio Secretary of State's office, Verified Publisher, LLC is currently an "active" business. Additionally, staff have found that a second corporate registration for Verified Publisher, LLC was filed in the State of Virginia on June 7, 2012 by Christopher Gates, who appears to be both a personal friend and professional colleague (you coauthored a book together).

While staff have not been able to establish the nature of Verified Publisher's business, an October 5, 2011 posting by you on your twitter account suggests that one of the company's "lawful purposes" was to demonstrate how easily it could be used to steal digital certificates of other web sites. You tweeted (screen capture below):



In addition, in a presentation at “Hackcon2013”, titled: “Dirty Little Secrets They Didn’t Teach You in Pentest Class v2,” Chris Gates and a second man, Rob Fuller, included slides about “Stealing Certificates” that use the Verified Publisher LLC as a part of illustrating how to “steal” certificates. One of those slides is reproduced (screen capture below):

Stealing Certificates

- Mozilla certutil
- -L → List all the certificates, or display information about a named certificate, in a certificate database.

```
certutil.exe -L -d
C:\Users\CG\AppData\Roaming\Mozilla\Firefox\Profiles\6smdhwrw.default
r-1339854577637\
VeriSign Class 3 Extended Validation SSL CA ..
DigiCert High Assurance CA-3 ..
VeriSign Class 3 International Server CA - G3 ..
COMODO Extended Validation Secure Server CA 2 ..
Verified Publisher LLC's COMODO CA Limited ID u,u,u
Akamai Subordinate CA 3 ..
VeriSign, Inc. ..
--snip
```

- “u” → Certificate can be used for authentication or signing ☺
- <http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html>

Finally, there is a web-site (<http://verifiedpublisherllc.com>) that appears to be owned by Verified Publisher, LLC but is a blank web-site, providing no actual information.



Given all of the information outlined above regarding Verified Publisher, LLC please explain:

2a) Aside from engaging in “Any Lawful Act” what is the purpose of Verified Publisher, LLC?

Verified Publisher has no customers, book of business, or provides any security services. I am the sole owner of this company, which was formed in the state of Ohio. I would not know what other companies were registered in other states. Additionally, the website referred to is not owned by me. Lastly, it is mentioned that Chris Gates and I co-authored a book – that is not true. I have published one book and it was co-authored by three individuals, none of whom are with Chris Gates. Verified Publisher was a business idea for performing code signing on portions of code used during penetration tests. It does not have customers, no revenue, nor is it actively in use.

2b) Is Verified Publisher, LLC involved in information security, and if so please describe the company’s involvement or expertise in this area?

It is not actively in use at this time – although it may be in the future.

2c) Why didn’t you disclose your ownership of Verified Publisher, LLC to the Committee given its apparently close relationship with TrustedSEC?

The company is not used for anything related to performing information security consulting services nor does it do any revenue generation business.

2d) Please identify the clients that Verified Publisher has been involved with since 2011. Include the name of the company, Federal agency or other organization that has utilized Verified Publisher’s services, the date(s) of these transactions and a description of their purpose.

None

2e) What is the relationship between the Verified Publisher, LLC company incorporated in Ohio which lists you as its Agent and the Verified Publisher, LLC company incorporated in Virginia on June 7, 2012 by Christopher Gates?

I own the company in Ohio – if another company by the same name is registered in another state I had no involvement in such a registration.

2f) During your testimony at the January 16, 2014, hearing: “*Healthcare.gov: Consequences of Stolen Identity*,” you submitted a report from IT security experts who identified issues with the Healthcare.gov web-site and specifically supported some of the issues you claim to have identified on this website. In your signed transmittal letter you wrote:

“Under no circumstance did anyone working at TrustedSec (including myself) voice opinion on the matter or provide opinion regarding the issues. These are completely unbiased reviews of the existing and previous exposures on healthcare.gov, which simply are alarming and still on the web site today.”

Given the close relationship between Verified Publisher, LLC and TrustedSEC, LLC identified above, as well as the close personal and professional relationship with Mr. Gates, who contributed to your report, why did you assert to the Committee that the views recorded in that report were “completely unbiased”?

Again, neither Chris Nickerson nor Chris Gates is a co-author of any book with me. There were discussions previously in the past with Syngress, however it never actualized, as we are all extremely busy – no book was “published” as alleged nor would it matter either way. Individuals in the security industry, especially individuals that have dedicated their career to bettering it, commonly run into one another. I know these individuals from the industry and have spoken at conferences with them on a number of occasions, which is perfectly normal in such a small business niche. We do not have a personal relationship.

2g) Another of the “unbiased experts” who you included in your report (Chris Nickerson) is a coauthor of a book, along with you and Chris Gates. Again, this suggests a relationship that may not be entirely unbiased. Do you have any other business or personal relationship with the other IT security experts cited in your report that should be disclosed?

3. Mr. Kennedy, you have testified to the Committee that you worked for the National Security Agency and also for the National Aeronautics and Space Administration. Your Huffington Post biography says that you were,

“A former Marine who did two tours in Iraq, Kennedy played a key role in the Marines’ cyberwarfare unit -- including the computer forensics on Saddam Hussein’s sons and Ba’ath Party officials. He also spent four years as a ‘red-team’ trainer for the National Security Agency and is the past chief security officer of Diebold.”

However, your linkedin profile lists unbroken work at the Marines (2000-2005) where you identify yourself as the NCO in charge for Marine Corps Computer Security Operations, SecureState (2005-2009), Diebold (2009-2012) and then TrustedSec, LLC (2012 to present).

The official biography that you presented the Committee discusses your career development in this way,

“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.”

Please explain when you worked at the two government agencies you have testified you worked at (NSA and NASA), your title at each agency, where you were stationed, and a job description of your assignments.

In the United States Marine Corps I had many functions working in the intelligence community, including working for the National Security Agency for intelligence reporting. As far as NASA – being a security consultant you work with a number of government agencies. This work was prior to the disclosure period applicable to the truth in testimony form.

4. On January 24, 2014 Representative Edwards and I wrote to you about apparent discrepancies between your testimonies of November and January, as well as discrepancies in answers to questions during the January hearing (Attachment 1). Since these issues strike at the heart of your claims to expert knowledge about Federal web site security, we had hoped to clear the matter up through that correspondence. On January 29, you submitted a written response that failed to answer our questions and so I must put those questions to you again (Attachment 2). I would ask that in response you provide substantive answers to each and every question.

4a) What security penetration of Federal sites have you done since leaving the Marine Corps? Please be specific as to who employed you (including your affiliation or position with the company), what agency was involved, the contract the work was done under, and the dates of your work.

I am only required to comment for a designated period in the truth of testimony form, and my information was accurate based on the applicable disclosure date. As previously mentioned, since the U.S. Marine Corps I also have worked with NASA; but it was prior to the period designated in the truth in testimony form.

4b) Because you appeared as President and CEO of TrustedSEC, LLC, and your only clients are, according to your testimony on January 16, 2014, in the private sector, please provide the Committee with the gross earnings from penetration testing security work of private firms for each year since 2011. Do not include gross earnings from sales of books, pamphlets or tools; do not include gross earnings from conference fees; do not include gross earnings from media appearances or contracts.

I am not required to provide this information, as it would reveal publicly TrustedSec's confidential business information and has no relevance to the security of healthcare.gov.

4c) At the November 19, 2013 hearing you indicated that TrustedSEC, LLC has done "white-hat hacking" for Fortune 10, Fortune 500 and Fortune 1000 firms. Please provide the names and contact information for all private sector firms that you or your company have done penetration security testing for since 2011. (To be very clear, we are not interested in the results of your work, just the names of the firms so that we can validate your claims regarding your work. If companies will not waive non-disclosure agreements that may be in place, please note for each company and contact that they desire to see the information kept confidential and we will respect that agreement and not release the names of those firms.)

I am under Non-Disclosure agreement with these organizations and would risk breaching a contract if such information was disclosed and has no relevance to the security of healthcare.gov.

4d) In your November 19, 2013 appearance, you said you successfully extracted account information for tens of thousands of individuals on a site connected to HealthCare.gov. Subsequent to the hearing, exchanges occurred between you and Committee staff clarifying that you were on Data.HealthCare.gov; a site that is on a separate server and does not share a backbone or architecture with Healthcare.Gov. Data.Healthcare.gov is an initiative by Socrata Corporation of Seattle to provide a platform for dozens of government agencies and entities to place public data in a common open forum. Accounts on Data.HealthCare.gov are actually Socrata accounts, which give account holders privileges to all the data hosted by Socrata. In light of this information, you seemingly dropped the claim that you could find account information on HealthCare.gov and you did not testify about this in your appearance on January 16, 2014. However, in the days immediately following the January hearing, stories began to appear detailing your claims that you had successfully extracted 70,000 identities through a simple Google tool, representing a fundamental security flaw with HealthCare.gov.

i) Please provide the web address for the website which you say you were able to extract 70,000 (or more) identities.

Data.healthcare.gov, although there are plenty of other directly on healthcare.gov.

ii) Was your action a "hack" of the website or would you consider it something else? If you do not consider it a "hack", please explain your rationale for not considering as such.

The profiles were public information and viewable through a normal web browser. Additionally, the same site was riddled with fake profiles leading to malicious software sites

(http://www.weeklystandard.com/blogs/opportunistic-marketers-exploit-opening-healthcaregov_775259.html), websites created to coax victims into believing it was healthcare.gov, and other major issues and continues to be subjected to a number of attacks. It was actively being used to harm United States citizens and target them. It's a mess, and it's apart of the healthcare.gov infrastructure. People should be highly concerned to this day. In addition, it's apparent that even supply-chain control around developmental security was not followed based on the Belarus connection to developing the website (<http://freebeacon.com/the-belarusian-connection/>). We will see this continue to get worse before it gets better.

- iii) If the site was Data.Healthcare.gov, which you know to be a public access site designed to make user profiles available, how does your exposure of public identities for account holders show any actual security weakness for the separate site, Healthcare.gov?

When signing up for the site, it is not disclosed that your information will be public – including email addresses and other pieces of information that is most commonly protected. Major design and security implications here in itself. Again, more examples of the flawed start and continued flawed infrastructure that supports the website.

- iv) Finally, did you gather passwords for the accounts or any other information that is not publicly available for Socrata account holders in the user information you extracted?

No passwords or other information was viewed that would not be considered “public” – regardless, is a major security concern and privacy issue for individuals that registered for the website.

5. In your response to our letter of January 24, you replied that, “I want you to know that I have been working with HHS in communicating and addressing any issues that I had previously identified. The agency support has been good and I am very confident that the site security is moving in a positive direction.”

This statement is at odds with your testimony to the Committee, as quoted in Question #1 above. In fact, you said that in comparison to your November 19th testimony, security at the site “is even worse.” Your letter also stands in contradiction to your appearance on Fox News on January 19, 2014. Asked during your nine minute interview about the CMS Chief Security Officer’s testimony before the Committee on Oversight and Government Reform (in which she said she felt her prior concerns had been addressed and that she would now support certification of the site based on its security status) you said:

“I have to completely disagree with her...if you read the testimony and you read what she actually said, she said they did end-to-end security testing and she didn’t say what type of testing that is... what’s pretty evident right now is that the site is not secure. It’s much worse off.”

What did you learn subsequent to your testimony and appearance on Fox News that has lead you to your new evaluation? Please be specific about what you learned, when and how you learned it.

There has been no change to my testimony. The website was a disaster from the start with little to no security built into the site. My comments are stating that security appears to now be a focus and something of interest to HHS, which is a good start based on conversations with Kevin Charest. That does not mean by any stretch of the imagination that it is right now secure, but that it's heading in the right direction from a leadership standpoint with apparent visibility for fixing the security concerns with the website which where inherently lacking from its release and through my second testimony.

6. In that same response to our letter of January 24, you attempted to clarify the apparent contradictions in your November and January testimony as well as the confused statements made at the January hearing regarding your work for the Federal government. Your clarification in the letter is to assert that neither you nor TrustedSec did any work for the Federal government since the October 1, 2011 disclosure date. You then write,

“But TrustedSec performs that same type of work under contracts with local government entities and foreign governments (U.S. allies), including security work for healthcare related government exchanges in other countries.”

I note that this effort to clarify contradicts another part of your testimony before the Committee. Under questioning on January 16, 2014 regarding your government work you said,

“I do not do work for the public sector; I’m plenty busy in the private sector keeping everybody else protected.”

6a) Why did you exclude local governments and foreign governments as not being part of the “public sector” in your January 16 statement?

This question was never asked of me, only if I had worked for the federal government as requested in my truth in testimony form.

6b) Why did you not deem it relevant to mention this other public sector work, particularly for “healthcare related government exchanges in other countries,” when you were given the chance to clarify your expertise by Chairman Smith?

I am unaware of any requirement that I disclose a private companies entire customer list to the United States government or risk violating non-disclosure agreements to do so and has no relevance to the security of healthcare.gov.

6c) Please provide specifics regarding security consulting contracts with local and foreign governments you refer to in your letter of January 29, 2014. Please include client name, dates, type of work and a contact. Specifically identify those assignments that involved penetration security work for "healthcare related government exchanges in other countries".

I am under Non-Disclosure agreement with these organizations and would risk breaching a contract if such information was disclosed and has no relevance to the security of healthcare.gov.

Responses by Mr. Waylon Krush

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“Healthcare.gov: Consequences of Stolen Identity”

QUESTIONS FOR THE RECORD

Mr. Waylon Krush

Co-Founder and CEO, Lunarline, Inc.

Questions submitted by Chairman Lamar Smith

- 1) At our hearing, you stated, “Well, Chairman Smith, actually as it relates to CMS, if you look at the GAO docket, I actually have been protesting with them. You know, on the contracting side, me and CMS are not necessarily best of friends.”

Upon researching the Government Accountability Office’s (GAO) open and closed bid protest docket, it appears that there is only one file listed for Lunarline, Inc. (Lunarline), and it was dismissed in December. Have you had any other protests? If not, was there only this one instance that provoked you to say that you and CMS are not necessarily the best of friends? Why was the Lunarline protest dismissed?

Answer: Lunarline’s former lawyers did not turn in the artifacts requested by GAO in time. Another company also protested this contract, protests that were subsequently upheld by GAO. I have great respect for the CMS security personnel who were our former clients. However I do not agree with this specific contracting decision, a decision that had a significant and negative impact on my company.

- 2) In the Truth in Testimony that you provided the Committee, you mention that you subcontract with SphereCom Enterprises, Inc. (SphereCom) for Centers for Medicare & Medicaid Services (CMS). According to the June 2013 GAO Report on the Patient Protection and Affordable Care Act, SphereCom is listed as one of the contractors supporting the federally facilitated exchanges and data hub, specifically working with “federal healthcare exchange (HIX) technical assistance and support” and “IT security - security oversight, equipment, new systems testing, and security program support.”¹
 - a) Have you ever discussed the security of the Healthcare.gov website with anyone working on the project at SphereCom?
 - b) Has anyone at SphereCom asked for your expert advice on any security issues related to Healthcare.gov? If so, what were the security issues and what were your suggestions?
 - c) You list two open orders with SphereCom for CMS on your Truth in Testimony form totaling over one million dollars. What kind of projects are

¹ GAO report, “Patient Protection and Affordable Care Act: Status of CMS Efforts to Establish Federally Facilitated Health Insurance Exchanges,” June 2013, available at: <http://www.gao.gov/assets/660/655291.pdf>

you working on? Is any of that payment for your support or work on Healthcare.gov?

- d) You list two closed orders with SphereCom for CMS on your Truth in Testimony form. Was any of that money used as payment for your support or work on Healthcare.gov? If not, please describe the project(s) that you worked on.
- a. Answer: I have not been asked to discuss the technical aspects of Healthcare.gov with anyone at Spherecom. We currently work for them as a subcontractor. I, like most people who have worked with them, have a great deal of respect for them and their personnel. I did ask some questions of my staff to see if they could provide me additional information in preparation for my appearances. However, nobody on my staff was able to provide any additional details.
 - b. No, they have not. I would openly provide my expert advice if given all of the system information and data related to the authorization package.
 - c. We were working on Risk Management Framework (RMF) assessments, supporting the CMS Security Operations Centers (SOC) and providing Cyber Security and Privacy Training. The work could directly or in-directly affect the security program and therefore Healthcare.gov, but these are CMS Cyber- and Privacy-wide initiatives. I did see the online training, but it was not specific to Healthcare.gov.
 - d. No, please see my previous answer (2c.)
- 3) At our hearing, I referenced a letter to the Committee signed by Mr. Kennedy and several well-known and well-regarded security experts. To varying degrees, they all expressed concerns about the poor security of the website - in contradiction to your support for it given that you went so far as to specifically state that you would use Healthcare.gov without hesitation. Is it your professional opinion that Mr. Kennedy and the seven other signatories of the letter are wrong or misguided?

Answer: Mr. Kennedy has his opinion and technical expertise. I respect his expertise and military service, but I do not agree with his assessment.

- 4) You stated in your testimony that you get "very nervous when [you] hear that a new critical technology or weapon system has been deployed with security as an afterthought." Given your confidence in Healthcare.gov – going so far as to say that you would use it without hesitation – is it your position that security was not an afterthought in the planning and development phases of Healthcare.gov? Is it your professional opinion that CMS made website security a prominent and early feature of Healthcare.gov?

Answer: Healthcare.gov has experienced many technical issues. So does all public facing web infrastructure. But, once again, I did not work on the site, so I don't want to speculate. I know what it is supposed to do. I know, based on the information available to the public, the RMF was used to make a risk-based decision on the system. I know

vulnerabilities were identified and that CMS had a good mitigation strategy to deal with the vulnerabilities. If CMS followed through, then our data is as safe as it can be.

- 5) You noted in your written testimony that you “have hands-on experience with CMS security systems and practices” and as a result you are “very familiar with many of the cyber security tools deployed within CMS.”
 - a) Given your relationship with CMS, what is your reaction to a December U.S. GAO report stating that in fiscal year 2012, agencies reported 22,156 data breaches – an increase of 111 percent from incidents reported in 2009, with over 4,000 incidents reported at CMS alone?
 - b) In your opinion, does this number exemplify that there are proper security systems in place, especially considering that data breaches can leave individuals vulnerable to identity theft or fraudulent activity - as noted in the GAO report?

Answer: See below

- a. I see both good and bad in this report. The bad is that CMS, like many government and commercial industries, is undergoing constant external and internal cyber attacks. These attacks are increasing in number and sophistication. Unless we get very serious about cyber security throughout our supply chain, the numbers are only going to get worse. The good news is that CMS and other organizations are doing a better job of identifying and reporting cyber incidents. When I started in this business, many organizations didn't even know they had been hacked. Some organizations that are sophisticated enough to identify attacks would try to cover them up as if nothing happened, rather than reporting and learning from them. Times have changed and the need to share these incidents is paramount. It would be worse if the reported attempts and success were actually going down because the data on vulnerabilities, threats, and malware would be contradictory.

- b. I need to know the definition of an incident to really answer this question. DHS includes scanning as an incident; if it's reporting active scans, the number is extremely low. If this is the number of times assets have been actively overtaken by an adversary -- the number of lost laptops, cellphones, etc. -- then the number is high. Most government organizations undergo hundreds if not thousands of security-relevant and reportable events every week. It's impossible to say whether the number is good or bad without knowing the context.

- 6) In a press release last November, Mr. Spence Witten, your company's Director of Federal Sales, states:

“Lunarline has worked with HHS and the Centers for Medicare and Medicaid Services (CMS) for years. Our federal partners at HHS are currently under fire due to the challenges of implementing HealthCare.gov, and it's fair to ask hard questions. But let's not forget that they already manage and maintain a robust enterprise security program that has successfully defended the sensitive

information of tens of millions of American citizens. We're fully confident that, at the end of the day, HHS is up to the challenge of defending HealthCare.gov."²

In contrast, a December GAO report on government information security documents over 4,000 data breach incidents revealing sensitive personal information in FY 2012 by CMS. So, is Lunarline's, and, based on your testimony before our Committee, your professional confidence in CMS as the operator of Healthcare.gov based on their capabilities, past performance and record, or on the fact that you do business with them?

Answer: Through my limited exposure to CMS via meetings, conferences, and my employees' tasking, I know that CMS takes cyber security seriously. I know it's investing in cyber infrastructure, personnel training, and working hard to ensure its systems are secure. To address the underlying intent of your question, if I wanted to do more business with CMS, wouldn't I want to make them feel as insecure as possible, to encourage them to invest yet more in cyber security? Instead I believe that too many cyber security companies take every opportunity to stoke fear in an effort to generate higher sales. The federal government indeed faces many security challenges, not least of which is the constant threat of government shutdown and budgetary pressure that makes it difficult to invest for the future. But there are fantastic, hard-working federal cyber professionals – at CMS and across the Government – who do an exceptional job fighting back against modern cyber threats.

- 7) In your testimony, you describe the Risk Management Framework used to secure Federal Information Systems. Are there certain documents that correspond with the various six-step processes of RMF that should exist within CMS as evidence of a step being addressed? If so, could you identify what they are specifically?

Answer: At a minimum it should have a Systems Security Plan (SSP) and all related appendixes, a Security Assessment Report (SAR), a Plan of Action and Milestones, and an Authorization letter describing the conditions of authorization. What's even more important is continuous monitoring of the system and constantly testing the security of the components, as well as mitigating and remediating the findings.

- 8) One of our other witnesses, Mr. Gregg, explained in his testimony that when a large website is reviewed, it typically includes an audit, vulnerability assessment and penetration testing by an independent entity not involved in writing the code or developing the site. Do you concur with his comments? Who would make an ideal independent candidate to review the Healthcare.gov website?

Answer: I concur. I have also seen documents that say CMS had several independent auditors conducting the work. In order to be independent, the auditor should not be part of the procurement, development, or on-going maintenance of Healthcare.gov.

² <http://www.prnewswire.com/news-releases/lunarline-ceo-addresses-healthcaregov-security-concerns-on-npr-morning-edition-230840011.html>.

- 9) HHS says they are conducting 24-7 system monitoring and constantly probing and scanning the system? What does this mean, and in your professional opinion, is it significant and adequate?

Answer: This means CMS has a security operations center that is monitoring security- and privacy-relevant events 24/7, 365 days a year. This also means it has a team conducting ongoing vulnerability scans of all of the Healthcare.gov components.

- 10) What is your understanding of the data hub and central storage facility for Healthcare.gov? Is the data stored on specific premises or within a cloud application?

- a) Does a cloud application make the data more susceptible to security breaches by third parties? For example, is it possible for data to go offshore?

Answer: I am not familiar enough with the architecture to provide a valid answer to this question.

- a. Cloud applications, if secured properly, can be just as secure as any on-premise application.

- 11) Multiple news stories exist about state-sponsored terrorism from countries such as India, China, and Russia to name a few. Could the amount of personal information of millions of Americans passing through Healthcare.gov have national security implications? Are there national security concerns about the other federal databases Healthcare.gov connects to?

Answer: There are always going to be nation-sponsored attacks against government websites and industry assets that provide intellectual property, finance, or competitive advantages to other nations. All government sites are important to our national security as they can become jump points to other .govs and possibly .mil domains. Healthcare.gov and the related sites are not the only places adversaries will find a significant amount of the United States' personal data.

- 12) The House recently passed legislation requiring the U.S. Department of Health and Human Services to inform individuals within two days if their personal information has been stolen or unlawfully accessed through an Obamacare exchange. Is this an undue burden on the government, or is such a requirement outweighed by the benefit given what can happen when one's identity is stolen or compromised?

Answer: If it is not politically driven, then I would require that for all PII data in the government. Why should we only go after Healthcare.gov? There are several sites where

I'm required to keep much more personal and important data, and these organizations -- both government and industry -- should follow those same guidelines.

- 13) In December, every Republican Member of this Committee sent a letter to the President requesting information and an explanation of the security risks and privacy concerns with the Obamacare website. The Committee has received no reply, nor even an acknowledgement.

The letter asks three questions:

1. "Since October 1, what explicit steps has the Administration taken to improve the security of Healthcare.gov?"
2. "Who in the Administration has been assigned to monitor, manage, and oversee the ongoing security needs of Healthcare.gov?"
3. "Has the Administration conducted thorough, on-going tests and monitoring of security and privacy vulnerabilities with Healthcare.gov -- including hiring private sector 'hackers' to test the website's ability to guard against malicious attack and intrusion?"

Are these reasonable and important questions deserving of a response sooner rather than later?

Answer: 13. These are all fair questions, but I would ask them of all .govs that process, store, transmit, manage, or review our private data. I would also expand them to commercial organizations that do the same. We all live online now -- whether we like it or not or we know it or not -- it is time that we protect all private data, not just some of it.

Responses by Mr. Michael Gregg

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Healthcare.gov: Consequences of Stolen Identity"

QUESTIONS FOR THE RECORD

Mr. Michael Gregg

Chief Executive Officer, Superior Solutions, Inc.

Questions submitted by Chairman Lamar Smith

- 1) Do you see any correlation between companies like Target and their security breach and HealthCare.gov?

Yes, hackers will target any online site that has data they can exploit. Such data includes names, addresses, phone numbers, email addresses or other types of PII (personally identifiable information). Hackers are also interested in exploiting systems that can be leveraged to obtain greater access. As an example, using HealthCare.gov to access IRS systems or Health and Human Services systems.

- 2) A recent report by Experian regarding data breaches in 2014 claims that healthcare will be a hotbed of consumer data breaches. Do you believe that Experian is right when it says that Healthcare.gov and the state healthcare security exchanges are "opening the floodgates" and making healthcare the most susceptible area for data breaches and identity theft?

Yes, I agree. This data has several uses. One, it can be used for identity theft. Two, it can be used for healthcare fraud. Healthcare fraud is a huge problem that continues to grow. As an example, former FBI Director, Louis Freeh, testified before the Senate Committee on Aging that cocaine traffickers in Florida and California were switching from drug dealing to health care fraud because it was safer, more lucrative and less likely to be detected.

- a) What long-term impact could this have on the health industry and the insured?

It could be devastating. The health industry depends on their customers having a feeling of trust and safety in bringing their problems and medical details to healthcare professionals. If people feel that their information is not safe, they will be less likely to reveal complete medical details or may use fake data. I agree with Mr. Rubin who had previously testified, "I have never seen an industry with more gaping security holes," adding, "If our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed."

- 3) A December U.S. Government Accountability Office (GAO) report on government information security documented a 111% increase in Federal agency data breaches in the past three years. Specifically, the GAO report noted that there were 22,156 incidents revealing sensitive personal information in 2012, up from 10,481 in 2009. The Centers for Medicare and Medicaid Services, the Healthcare.gov operator, had the second most breaches in the report for FY 2012 at 4,172. What do you conclude from these statistics?

There is a huge increase in medical fraud. Attackers typically go where the opportunity for money is and currently, healthcare is it! The rush to digitize information and make it available electronically has added to this problem. There needs to be mandates for encryption for data at rest and in transit. There is also a greater need for strong authentication and access control.

- 4) What are the ways in which Healthcare.gov could be hacked? What would a successful hack yield in terms of personal and medical identity theft?

There are many potential ways that HealthCare.gov could be hacked. What's most important is the information that could be exposed. Exposed information would include names, SSNs, age, address, DOB, etc. Cyber hackers, foreign governments, and terrorists could use this information to hurt the U.S. and its citizens.

- 5) What is the most effective and efficient way to address security concerns on Healthcare.gov - should the website stay up or be taken down while being fixed?

We need an independent, thorough security evaluation of this site. This should include a review of the code, the site and the application. There should also be a commitment from the administration that the findings will be acknowledged and promptly addressed.

- 6) Your testimony discussed some of the differences between audits and penetration testing. Can you elaborate on this topic?

A security audit is a structured evaluation of the security of an application. It is performed by measuring how well the application conforms to a set of established criteria. Think of it as a check list. A vulnerability assessment uses a program or application that examines or looks for potential security weaknesses, vulnerabilities, or misconfigurations. A penetration test is adversarial in nature. It asks, what can an attacker see, what can the attacker do, what would be the damage or result. All three types of tests should be performed on HealthCare.gov.

- 7) Given this Administration's repeated and vociferous pledges of transparency, would you consider the construction, management and current attempts at remediation of the

Healthcare.gov website to be in keeping with such pledges? What kind of security information would you expect to be made available to the American people?

I would expect to see reports from independent, third parties stating that HealthCare.gov has been fully reviewed, tested, and what the results of the tests were i.e. pass/fail.

- 8) Multiple news stories exist about state-sponsored terrorism from countries such as India, China, and Russia to name a few. Could the amount of personal information of millions of Americans passing through Healthcare.gov have national security implications? Are there national security concerns about the other federal databases this site connects to?

Yes, there are national security concerns. Just as reports with Target indicate that attackers may have gained access through HVAC systems, state sponsored terrorists are not picky in the means used to exploit critical government systems. In my opinion, there are national security concerns about other federal databases since they are connected to HealthCare.gov.

- 9) The House recently passed legislation requiring the U.S. Department of Health and Human Services to inform individuals within two days if their personal information has been stolen or unlawfully accessed through an Obamacare exchange. Is this an undue burden on the government, or is such a requirement outweighed by the benefit given what can happen when one's identity is stolen or compromised?

This is not an undue burden. Identity theft is a serious problem.

- 10) In December, every Republican Member of this Committee sent a letter to the President requesting information and an explanation of the security risks and privacy concerns with the Obamacare website. The Committee has received no reply, nor even an acknowledgement.

The letter asks three questions:

1. "Since October 1, what explicit steps has the Administration taken to improve the security of Healthcare.gov?"
2. "Who in the Administration has been assigned to monitor, manage, and oversee the ongoing security needs of Healthcare.gov?"
3. "Has the Administration conducted thorough, on-going tests and monitoring of security and privacy vulnerabilities with Healthcare.gov – including hiring private sector 'hackers' to test the website's ability to guard against malicious attack and intrusion?"

Are these reasonable and important questions deserving of a response sooner rather than later?

I consider these important questions that should be answered.

- 11) According to Mr. Krush's testimony, he stated that based on what he has read publicly thus far, "Healthcare.gov is most likely categorized as a Moderate system," referring to the National Institute of Standards and Technology (NIST) security levels of low, moderate, and high. Is this an appropriate categorization for the kinds of personal data available and accessible through the Healthcare.gov website?

NIST has a set of standards that are used to rank the criticality of a system. Regardless of the rating that has been issued, HealthCare.gov should receive additional review.

- 12) HHS says they are conducting 24-7 system monitoring and constantly probing and scanning the system? What does this mean, and is it significant and adequate?

No, this is not significant or adequate. Monitoring systems such as intrusion detection are detective in nature. While an attack may be detected with such systems, intrusion detection does not prevent an attack. Also, this detection may not be immediate. There could be some delay before logs are reviewed or attacks are detected; by then, the damage is already done.

- 13) Do you know if Healthcare.gov encrypts its data at rest and when in motion, and if not, should it?

First, it is important to understand that not all encryption systems are equal. Weak encryption is easily broken. All data, both in transit and at rest, should be encrypted.

- 14) What is your understanding of the data hub and central storage facility for Healthcare.gov? Is the data stored on specific premises or within a cloud application?

I do not have access to enough data to answer question #14.

- a) Does a cloud application make the data more susceptible to security breaches by third parties? For example, is it possible for data to go offshore?

While cloud applications are becoming more popular, there are many security concerns that must be addressed. These include:

- Is the data encrypted in transit?
- Is the data secured at rest?
- Where is the data center located? (i.e. in the US or aboard in another country)
- What security controls are in place in the data center?

As an example, NASA took seven months to reach its licensing agreement with Amazon before moving some of its data to a cloud based solutions; NASA wanted to be able to inspect the hardware it was using and that the information remained in the U.S.

- 15) Based on information presented at the hearing, and given what you know about Healthcare.gov post November 30th, should Americans take any specific actions to address identity theft threats and vulnerabilities?

In general, Americans should practice care when providing others with personal information.

- Individuals should guard personal information, shred old letters, bills, and other documents that are being disposed of.
- Passwords should not be common words or items that hackers can easily guess.
- Passwords should not be shared or written down for others to see.
- Passwords used for access to online healthcare accounts should be unique and not used for multiple sites.
- Monitor credit card bills and healthcare statements for unusual activity.
- Periodically, check credit reports.



House Committee on Science, Space and Technology

"Healthcare.gov: Consequences of Stolen Identity"

Responses to Chairman Lamar Smith's Questions

Dr. Larry Ponemon
Chairman and Founder, Ponemon Institute

1. Can consumers increase their risk of identity theft by signing up for coverage on Healthcare.gov?

Anytime personal information is provided on a website there is a risk of becoming a victim of identity theft. That is the case in both the public and private sector. Specific risks include a hacker or cyber criminal stealing information, a system glitch resulting in the loss or leakage of the information and negligent employees not following policies with respect to the handling of sensitive and confidential information. To minimize the risks, Healthcare.gov should follow strict security safeguards to ensure the protection of personal information. This includes having procedures and technologies in place as well as training and vetting of all employees who have access to the sensitive information.

2. Could a security breach of Healthcare.gov result in people's medical files being accessed? If so, is there a way for a hacker to ultimately corrupt people's medical records?

If a security breach occurred and personal information was obtained by criminals, they could use this information to assume the identity of individuals and possibly use it to access people's medical files. As shown in our research, criminals use their access to medical information to obtain medical services, including treatment, healthcare products or pharmaceuticals. In the course of obtaining these services, information about the patient can be changed to reflect the criminal's treatment and thus corrupted. This can put the real patient at risk if a healthcare provider bases treatment on the corrupted information.

Our latest study on patient privacy and data security¹ reveals that the Affordable Care Act (ACA) increases risk to patient privacy and information security, according to healthcare organizations. Sixty-nine percent of organizations that participated in the study say that the ACA significantly increases or increases the risk. The primary concerns are insecure exchange of patient information between healthcare providers and government, patient data on insecure databases and patient registration on insecure websites.

3. Can medical identity theft put victims' lives at risk?

As discussed above, the answer is yes. If medical files are corrupted because of a criminal assuming the identity of a patient, inaccurate information such as a wrong blood type or allergies to specific medications could jeopardize future treatments of the real patient. Another life-threatening consequence is the loss of healthcare coverage because the criminal used the stolen identity to obtain costly treatments and payments were not made. Should the medical identity victim require treatment, a lack of insurance might make medical services unavailable.

¹ *Fourth Annual Benchmark Study on Patient Privacy & Data Security*, conducted by Ponemon Institute and sponsored by ID Experts, March 2014.

4. Are Americans sufficiently aware of the dangers and consequences of medical identity theft?

Our research has found that the cases of medical identity theft are increasing. Most consumers we have surveyed are aware of medical identity theft. Many have had personal experience with this crime, either directly or through an immediate family member. However, most are not aware that medical identity theft can create inaccuracies in their permanent medical records.

Unfortunately we do not believe Americans are sufficiently aware of the dangers and consequences of this crime. As a result, they are slow to take steps to protect themselves and resolve the crime. Most victims do not take any steps to protect themselves from future incidents of medical identity theft. A very important step for consumers to take is to review their medical bills and explanation of benefits (EOB) statements for any inaccuracies and to report these to the healthcare provider immediately.

5. What kinds of out-of-pocket costs could victims expect to incur to resolve the issue of having their medical identity stolen?

Based on our *2013 Survey on Medical Identity Theft*,² typical out-of-pocket costs include the following: identity protection, credit reporting and legal counsel; medical services and medications because of lapse in healthcare coverage; reimbursements to healthcare providers to pay for services to imposters. The research reveals that the average out-of-pocket costs for victims that took care of their own costs could be as much as \$18,660.

6. Based on your experience and research, what are some of the best practices that leading companies implement to protect sensitive information and make their websites more secure.

A big risk to the security of websites is what is called business logic abuse. This results from the criminal discovering a flaw in the business logic or functionality of a website. In most cases, the criminal uses the legitimate pages of the website to perpetrate cyber attacks, hacks or fraud. One objective of this fraud is to steal money, confidential information or exploit the system for illicit gains. Business logic abuse poses serious risks to personal information. Not only are the attacks likely to occur they are also stealthy.

Based on our research here are some best practices leading companies have adopted:

- Assign responsibility for website security and ensure there is sufficient in-house personnel to minimize business logic abuses.
- Establish a partnership between website developers and IT to make sure a prevention and detection strategy is in place and enforced.
- Strive to have a strategy that minimizes the risk but does not frustrate legitimate consumers.
- Ensure ongoing monitoring of websites for business logic abuses.
- Check partner websites for business logic abuses.
- Invest in technologies that enable real-time visibility into website traffic.

We also recommend the following:

Invest in technology that improves the ability to prevent downtime or outages and detect fraud occurring in real time.

² *2013 Survey on Medical Identity Theft*, conducted by Ponemon Institute and sponsored by the Medical Identity Fraud Alliance, September 2013.



Centralize resources under one function to improve accountability for preventing and detecting Internet fraud and cyber attacks. Too many organizations say no one function is accountable for stopping Internet fraud and threats. Have a business continuity and disaster recovery plan in place to minimize downtime and data center availability in the event of an attack.

Based on the purpose of Healthcare.gov and the information it collects, assess what threats are most likely to target its websites. Prevent future fraud by understanding the root cause of the attack.

7. **Based on the information presented at the hearing and given what you know about Healthcare.gov post November 30th, should Americans take any specific actions to address identity theft threats and vulnerabilities?**

Some of the steps Americans should take include tracking all financial records and medical bills for any discrepancies or inaccurate charges. This also includes a review of EOBs. They should be closely monitoring their credit reports to make sure there are no changes to their status.

8. **A recent report by Experian regarding data breaches in 2014 claims that healthcare will be a hotbed of consumer data breaches. Is Experian right when it says that Healthcare.gov and the state of healthcare security exchanges are "opening the floodgates" and making healthcare the most susceptible area for data breaches and identity theft?**

It is very telling that healthcare organizations believe health information exchanges are not prepared to protect patient information. According to our study on patient privacy and security³, healthcare organizations' confidence in the security of health information exchanges (HIEs) is low and as a result they are reluctant to join these exchanges because of lack of security and privacy safeguards for patient data. The long-term impact will be costly due to the occurrence of data breaches, a lack of confidence in the overall healthcare system and disruption in the ability of healthcare organizations to deliver services.

9. **A December U.S. Government Accountability Office (GAO) report on government information security documented a 111 percent increase in Federal agency data breaches in the past three years. Specifically, the GAO report noted that there were 22,156 incidents revealing sensitive personal information in 2012, up from 10,481 in 2009. The Centers for Medicare and Medicaid Services, the Healthcare.gov operator, had the second most breaches in the report for FY 2012 at 4,172. What do you conclude from these statistics?**

Organizations in both the private and public sectors have data breaches and this will continue. The criminals are increasingly sophisticated and stealthy. In addition, well-meaning but negligent employees are at the root cause of many data breaches. It is a challenge to mitigate the risk to sensitive and confidential information. Therefore, it is not the issue of how many breaches these organizations are having but what are they doing going forward to reduce the risk and, in the event of a data breach, what are they doing to protect the victims.

10. **The House recently passed legislation requiring the U.S. Dept of Health and Human Services to inform individuals within two days if their personal information has been stolen or unlawfully accessed through an Obamacare exchange. Is this an**

³ Ibid.1



undue burden on the government, or is such a requirement outweighed by the benefit given what can happen when one's identity is stolen or compromised?

This is an absolutely ridiculous requirement and illustrates the HHS' lack of knowledge about how to respond to a data breach. To require a notification within two days of a data breach would not be enough time to conduct a thorough investigation to determine who was harmed and how they might be affected by the loss or theft of their personal information. When organizations rush to notify there is the risk that they are contacting individuals who will not be impacted by the data breach. Worse they may not understand the full extent of the data breach, the root causes and how best to remediate the affects of the data breach.

Respectfully,

L.A. Ponemon

Dr. Larry Ponemon
Chairman & Founder
Ponemon Institute, LLC