Heathcare.gov
Security Expert Testimony

Version 1.4 FINAL

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

Disclosure Statement: This report is for public use and contains no restrictions for distribution or disclosure.

Addressed to:
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

Greetings Mr. Smith and Ms. Johnson, January 16, 2014

Since my last testimony on the healthcare.gov web site, only two issues have been reported fixed from an overwhelming number of critical flaws that still exist on the web site. Instead of just myself leading the charge to bring notice to the alarming security threats towards the healthcare.gov web site, I have worked with several other well known and highly respected members of the security community to formulate statements based on the already existing research that I as well as many other security researchers have performed.

I have placed these security researchers and experts under non-disclosure agreement (NDA) to protect existing exposures from being publicly released, I engaged Ed Skoudis, Kevin Mitnick, Kevin Johnson, Lares Consulting (Chris Gates, Eric Smith, and Chris Nickerson), and John Strand, who are all well known and highly regarded in the Information Security field, to give their expert opinion on to what extent these exposures pose a threat to healthcare.gov, and more importantly the personal information to which the web site has access.

Please note that we, as security researchers, take no political stands regarding the current issues facing the web site. These statements are purely based on our expertise in the Information Security field and the level of risk these exposures as well as symptomatic problems of a much larger risk pose to the United States and its citizens.

Contained in this document are the responses back following the information being shared with the security experts. 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.

Sincerely,

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

1.0 Executive Summary

This document contains the testimony and comments from multiple well-known and highly respected members of the Information Security industry. Many perform work for the federal government and private sector on a regular basis. The purpose of this document is to gauge the opinion of the security of the web site healthcare.gov and it's supporting infrastructure. Based on the comments and feedback unanimous agreement exists that there is, to this date, still serious concern around the security of the web site and there was a lack of security testing of the web site prior to the launch.

Our goal for this report is to bring awareness of Information Security to the federal government, which has had a track record of not providing adequate protections for sensitive information. A larger consensus in the federal government around how to build secure code and protect information has to be met in order to deal with the threats of today and tomorrow. It is our belief, as members of the Information Security field, that a larger focus on protecting the United States infrastructure, its web sites, and people are of the utmost importance moving forward.

2.0 The Security Researchers

TrustedSec contacted well known, highly respected, and extremely talented individuals in the Information Security field who have a proven record for being the industry's top security professionals. Following is information about each of the experts and their extensive experience and clout within the security industry:

Ed Skoudis, Founder of Counter Hack

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions, which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (Security 560) and incident response (Security 504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing.

Kevin Mitnick, Founder and CEO of Mitnick Security Consulting

Kevin Mitnick (born August 6, 1963) is an American computer security consultant, author, and hacker. In the mid nineties, he was "The World's Most Wanted Hacker". Since 2000, he has been a successful security consultant, public speaker and author. Kevin does security consulting for Fortune 500 companies, performs penetration testing services for the world's largest companies and teaches Social Engineering classes to dozens of companies and government agencies. His last book 'Ghost in the Wires: My Adventures as the World's Most Wanted Hacker' was a New York Times bestseller late 2011.

In 2000, Miramax made a movie made about Kevin's life, which was based on the book Takedown by John Markoff and Tsutomu Shimomura. The DVD was released in September 2004. An independent documentary was made that corrected many errors in the Miramax movie.

Kevin Mitnick wrote two computer security books with William L. Simon:
- The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers
- The Art of Deception: Controlling the Human Element of Security

In 2012 a book came out called The Path of Least Resistance that Kevin wrote with Brad Sagarin.

As the world's most famous (former) hacker, Kevin has been the subject of countless news and magazine articles published throughout the world. He has made guest appearances on numerous television and radio programs, offering expert commentary on issues related to information security. In addition to appearing on local network news programs, he has made appearances on 60 Minutes, The Learning Channel, Tech TV's Screen Savers, Court TV, Good Morning America, CNN's Burden of Proof, Street Sweep, and Talkback Live, National Public Radio, and as a guest star on ABC's spy drama "Alias". Mitnick has served as a keynote speaker at numerous industry events, hosted a weekly talk radio show on KFI AM 640 in Los Angeles, testified before the United States Senate, written for Harvard Business Review and spoken for Harvard Law School.

Kevin Johnson, CEO of Secure Ideas

Kevin Johnson is the Chief Executive Officer of Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises and penetration testing everything from government agencies to Fortune 100 companies. In addition, Kevin is an instructor and author for the SANS Institute and a faculty member at IANS. He is also a contributing blogger at TheMobilityHub.

Kevin has performed a large number of trainings, briefings and presentations for both public events and internal trainings. Kevin teaches for the SANS Institute on a number of subjects. He is the author of three classes: SEC542: Web Application Penetration Testing and Ethical Hacking, SEC642: Advanced Web Application Penetration Testing and SEC571: Mobile Device Security.

Kevin has also presented at a large number of conventions, meetings and industry events. Some examples of these are: DerbyCon, ShmooCon, DEFCON, Blackhat, ISACA, Infragard and ISSA.

Kevin is also very involved in the open source community. He runs a number of open source projects. These include SamuraiWTF; a web pen-testing environment, Laudanum; a collection of injectable web payloads, Yokoso; an infrastructure fingerprinting project and a number of others. Kevin is also involved in MobiSec and SH5ARK. Kevin was the founder and lead of the BASE project for Snort before transitioning that to another developer.

Lares Consulting, Information Security Firm

Chris Gates, Partner and Principal Security Consultant at Lares Consulting
Eric Smith, Partner and Principal Security Consultant at Lares Consulting
Chris Nickerson, Founder and Principal Security Consultant at Lares Consulting

Chris Gates joined Lares in 2011 as a Partner & Principal Security Consultant. Chris has extensive experience in network and web application penetration testing as well as other Information Operations experience working as an operator for a DOD Red Team and other Full Scope penetration testing teams. Chris holds a BS in Computer Science and Geospatial Information Science from the United States Military Academy at West Point and holds his CISSP, CISA, GPEN, GCIH, CEH, and Security+. In the past, he has spoken at the United States Military Academy, Derbycon, BlackHat, DefCon, Toorcon, Brucon, Troopers, SOURCE Boston, OWASP AppSec DC, ChicagoCon, NotaCon, and CSI. He is a regular blogger carnal0wnage.attackresearch.com and is also a contributor to the Metasploit project.

Eric Smith Eric Smith is a highly qualified, trained, and certified Ethical Hacker with over 15 years of experience in the IT/IS industry. Eric possesses an in depth focus on helping companies to design, implement, and improve their security controls resulting in better protection of their critical information assets. He is well versed in a variety of Risk Assessment services helping clients to meet compliance with local laws, government regulations, and corporate initiatives. Eric is experienced in network and application level vulnerability assessments, penetration testing, social engineering, Red Team/physical security, wireless audits, architecture review, system hardening, risk/compliance assessments, and policy/procedural development. Eric has presented at numerous security conferences including DEFCON, Security B-Sides, DerbyCon, HackCon, and DakotaCon. Eric holds a BS in Information Security Systems along with active CISSP and CISA certifications.

Chris Nickerson is Certified Information Systems Security Professional (CISSP) whose main area of expertise is focused on Information security and Social Engineering in order to help companies better defend and protect their critical data and key information systems. He has created a blended methodology to assess, implement, and manage information security realistically and effectively. At Lares, Chris leads a team of security consultants who conduct Security Risk Assessments, which can cover everything from penetration testing and vulnerability assessments, to policy design, computer forensics, Social Engineering, Red Team Testing and regulatory compliance.

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing and coaching. Lares is committed to identifying the key assets of your unique business and creating a customized strategy to protect you in today's volatile business environment and beyond. Our approach allows our clients to make informed decisions about their information security programs and effectively "secure what matters most".

John Strand, Senior Security Analyst and Principal at Black Hills Information Security

John Strand is Senior Security Analyst/Principal of Black Hills Information Security. Before BHIS, John started the practice of computer security with Accenture Consulting in the areas of intrusion detection, incident response, and vulnerability assessment/penetration testing. John then moved to Northrop Grumman specializing in DCID 6/3 PL3-PL5 (multi-level security solutions), security architectures, and program certification and accreditation.

John teaches and authors classes for the SANS institute and PaulDotCom. John is the course author and instructor for SEC464: Hacker Guard: Security Baseline Training for IT Administrators and Operations with Continuing Education, and the co- author for SEC580: Metasploit Kung Fu for Enterprise Pen Testing.

He also teaches SEC504: Hacker Techniques, Exploits, and Incident Handling; SEC560: Network Penetration Testing and Ethical Hacking; for the SANS institute. For PaulDotCom, he is the author of Offensive Countermeasures: The Art of Active Defense. John has presented for multiple organizations and 'cons' including the FBI, NASA, NSA, RSA and DefCon. John is the host of Hack Naked TV with PaulDotCom and enjoys co-hosting PDC Security Weekly. John is one of the minds and leaders behind Offensive Counter Measures and Active defense, which he hopes will change the security industry for the better.

3.0 Expert Statements on Healthcare.gov

The below comments were from each individual security expert based on the findings that TrustedSec performed from our original testimony. As of today, a majority of exposures still exist (except two) and have not been fixed or remediated. The larger topic moving forward is how do we ensure that when the federal government produces websites that integrate security into the development process to fix these issues prior to them being released.

Ed Skoudis, Founder of Counter Hack Statement

“I've worked on dozens of large-scale breach cases over the past 12 years, looking at the root cause vulnerabilities and the attackers' methods. Reviewing the security issues discovered in the healthcare.gov site, I can tell you: this is a breach waiting to happen. Or, given the numerous vulnerabilities, perhaps a breach already has happened. These are _exactly_ the kind of security flaws bad guys exploit in large-scale breaches. Urgent action is required to fix these flaws, applying well-known, time-tested, industry-standard security defenses.”

Signed

Kevin Mitnick, Founder and CEO of Mitnick Security Consulting

“After reading the documents provided by David Kennedy that detailed numerous security vulnerabilities associated with the Healthcare.gov web site, it's clear that the management team did not consider security as a priority.

Healthcare.gov retrieves information from numerous third-party databases belonging to the IRS, Social Security Administration, Department of Homeland Security, and other State agencies. It would be a hacker's wet dream to break into Healthcare.gov and potentially gain access to the information stored in these databases. A breach may result in massive identity theft never seen before -- these databases house information on every U.S. citizen!

It's shameful the team that built the Healthcare.gov site implemented minimal, if any, security best practices to mitigate the significant risk of a system compromise or access to consumer proprietary information.

Based on the breaking news reports of huge security breaches and Target and Neiman Marcus where cyber-crooks lifted millions and millions of consumer credit and debit card numbers, it's clear our adversaries are continuing to target consumer financial and personal information.

This is a big wake up call for the Government: It's time for the Healthcare.gov to shore up their defenses by adopting best security practices, including   identifying and remediating security flaws that will be exploited by our adversaries."

Signed

Kevin Johnson, CEO of Secure Ideas

"As the CEO of Secure Ideas and a security professional for more than a decade, I was asked to review a series of security findings related to the healthcare.gov website. I was provided with a report of findings plus supporting documents that reveal a series of flaws that were found within the variety of pieces that make up the healthcare.gov application. In my professional opinion, these findings exhibit not only a basic lack of security testing, but also reflect signs that standard IT change management and validation practices are not being followed. These security findings are typical findings we see when an application has been written by developers who have not been introduced to basic security training, nor understand the importance of security within an application. The findings disclose a wide range of issues that could cause serious harm to both healthcare.gov as well as any individual using the application. These flaws are not even complex problems that would require advanced security knowledge to detect. Instead, they are issues that are detected with simple, standard techniques, of which any developer or QA professional should be aware.

From a security perspective, items such as the JSON injection and the lack of access controls for eligibility reports are commonly seen in applications not scrutinized by any type of security assessment. These are the types of flaws that a security assessment should find with little effort. Given the existence of these flaws for such a prolonged amount of time after the release of the application, it is a certainty that security testing is either not being performed at all, not being performed well, or the results of the testing are not being made part of remediation efforts. Applications containing low hanging fruit such as these flaws typically also contain much more serious issues.

From a basic IT perspective, the problems and concerns discovered also reflect a lack of change validation and functionality testing that should be performed regularly throughout an application's lifecycle, an example of which is the error on the SPF record. Even in immature technology shops, when a feature or change is made to the system, such as when a DNS record is created, it is standard practice to verify that the change was made correctly. The fact that this SPF record is not correctly implemented in healthcare.gov indicates that no one verified the functionality.

These are the types of issues that security professionals would hope never to see in a government application. Given the industry standard application development lifecycle, these problems should simply not exist in this application. It is evidence of a lack of integrated security and quality assurance validation in the development lifecycle of healthcare.gov. Security and quality assurance are basic types of processes the federal government should consider essential and non-negotiable from its application developers."

Signed

Lares Consulting

Chris Gates, Partner and Principal Security Consultant at Lares Consulting
Eric Smith, Partner and Principal Security Consultant at Lares Consulting
Chris Nickerson, Founder and Principal Security Consultant at Lares Consulting

"David Kennedy, CEO of by TrustedSec (www.trustedsec.com), along with a group of knowledgeable security researchers identified significant critical security flaws in healthcare.gov and it's supporting web sites. These weaknesses, which were reviewed by Lares Consulting (www.lares.com), indicate that these applications were deployed into production and accessible to the public without following security best practices and industry standards. The presence of these weaknesses could allow for exploitation of healthcare.gov systems, visitors of the healthcare.gov websites and leakage of sensitive information for registered users of the healthcare.gov application. Many of these security flaws would have been identified and could be mitigated by performing routine application security assessments early in the development lifecycle along with following guidelines and best practices for system and application hardening.

Any web application, especially one of this criticality, must undergo vigorous hardening and security testing prior to deployment. The Open Web Application Security Project (OWASP) Top Ten (https://www.owasp.org/index.php/Top_10_2013-Top_10) provides application developers and implementers a list of the top security threats which web applications are exposed to. Many security researchers and consultancies, including Lares Consulting, feel that properly assessing a web application against the OWASP Top Ten constitutes bare minimum requirements and helps an organization identify security threats early in the development lifecycle, before it is released into production. Mr. Kennedy documented and presented a number of security flaws on healthcare.gov that fail to meet the requirements defined in the OWASP Top Ten. These findings are described in detail within the OWASP Top Ten under sections: Injection (A1), Broken Authentication and Session Management (A2), Security Misconfigurations (A5), Sensitive Data Exposure (A6), Missing Function Level Access Control (A7), Using Components with Known Vulnerabilities (A9) and Invalidated Redirects and Forwards (A10). "

Signed

Signed

Chris Nickerson
Signed

John Strand, Senior Security Analyst and Principal at Black Hills Information Security

“It is unfortunate that a website of this prominence, importance and visibility has such a large number of apparent vulnerabilities. It is also unfortunate that in information technologies today the level of security demonstrated in this report occurs far too often.

But that is the crux of the issue. If the healthcare.gov site is the devil we know. What about the devil we don't know? Where are the breach notification requirements for .gov sites? Where are the regular and continuous testing requirements for federal and state governments? It is truly unfortunate that rather than the government being the shining city on the hill when it comes to security and breach notification, it is the devil we don't know.”

Signed