TrustedSec

INFORMATION SECURITY MADE SIMPLE

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 webvsite and that Accenture has been selected to perform future updates and rollouts of the webvsite (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/0B75Y2Pq4wn1RcmtEWnFENFdoaWc/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.

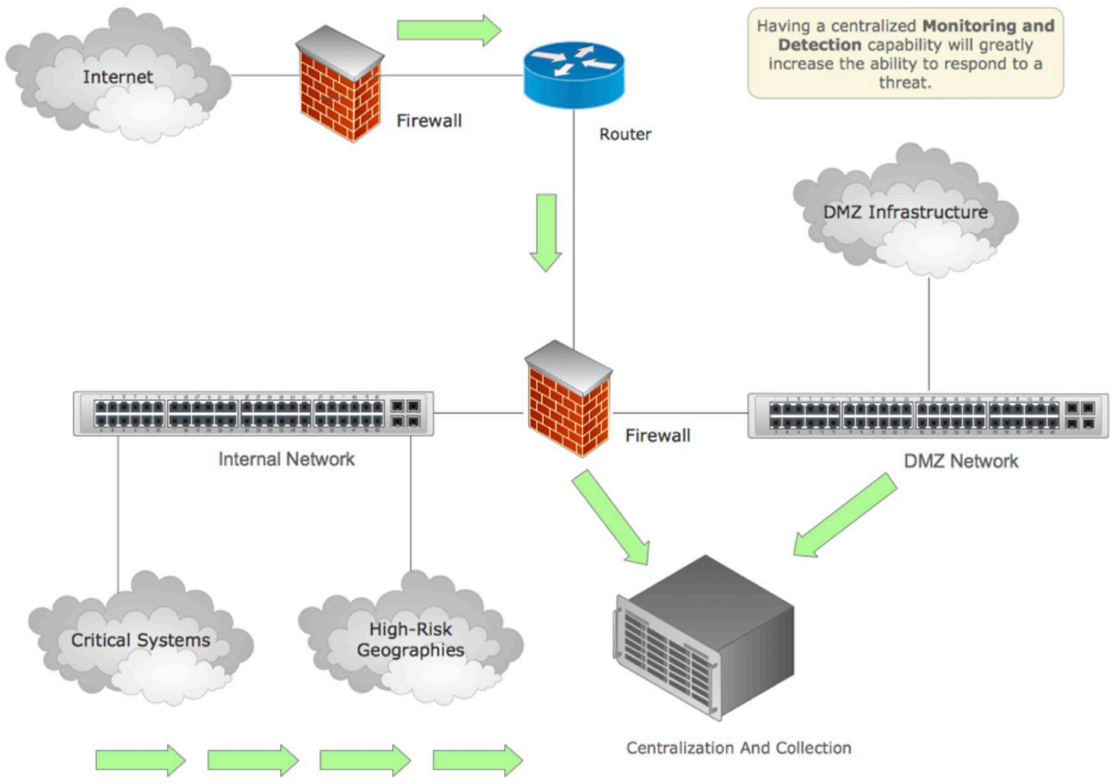
3.0 Monitoring and Detection Capabilities

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.


Internet
Firewall
Router
Having a centralized **Monitoring and Detection** capability will greatly increase the ability to respond to a threat.
DMZ Infrastructure
Internal Network
Firewall
DMZ Network
Critical Systems
High-Risk Geographies
Centralization And Collection

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]?," Fryrer 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-bourne 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.