Morgan Wright, Principal - Morgan Wright, LLC

Testimony of Morgan Wright, Principal, Morgan Wright, LLC, Before the House Committee on Science, Space, and Technology, Subcommittee on Research and Technology and Subcommittee on Oversight

February 12, 2015

Chairwoman Comstock, Chairman Loudermilk, and members of the Committee:

Thank you for inviting me to testify before you today. I'm Morgan Wright, Principal of Morgan Wright, LLC. I provide advisory and consulting services to the private sector in the areas of cybersecurity, advanced technology introduction, market development, strategic planning and identity theft solutions. In addition, I am also a Senior Fellow for the Center for Digital Government. The Center for Digital Government is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge, and opportunities to help them effectively incorporate new technologies in the 21st century.

I am providing this written testimony pursuant to your invitation to testify. My testimony is in response to the three questions posed by the committee:

1. Why would HealthCare.gov need to embed data mining firms within the website's infrastructure and is it reasonable for there to have been 50 companies connected at one time?
2. What are the cybersecurity implications of the high number of third party connections to HealthCare.gov, and what are the vulnerabilities associated with these types of connections?
3. What guidance does the National Institute of Standards and Technology provide federal agencies relative to cybersecurity practices, and how would they be applicable in this context?

1. Why would HealthCare.gov need to embed data mining firms within the website's infrastructure and is it reasonable for there to have been 50 companies connected at one time?

According to Gartner, data mining[1] is defined as *"The process of discovering meaningful correlations, patterns and trends by sifting through large amounts of data stored in repositories. Data mining employs pattern recognition technologies, as well as statistical and mathematical techniques."*

Investopedia defines data mining[2] as *"A process used by companies to turn raw data into useful information. By using software to look for patterns in large batches of data, businesses can learn more about their customers and develop more effective marketing strategies as well as increase sales and decrease costs. Data mining depends on effective data collection and warehousing as well as computer processing."*

A reasonable user of the site would be led to believe that there are third-party applications to measure web site statistics, in addition to the obvious social media providers. Since a user coming to the site, either directly or from a referral (like a search engine or link from another site), is not required to enter any personally identifiable information (PII), it is reasonable to assume that their PII later entered on the site would not be passed to anyone other than HealthCare.gov.

The original press reports by AP[3] indicated that 50 separate third party applications were collecting data from consumers without their knowledge. According to the story Medicare spokesman Aaron Albright said outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes." The use of the term 'vendor' would imply some form of written agreement as to specific prohibitions on use of the data.

[1] http://www.gartner.com/it-glossary/data-mining

[2] http://www.investopedia.com/terms/d/datamining.asp

[3] http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html

After the initial report, Cooper Quintin of the Electronic Frontier Foundation published a follow-up article examining the current state.[4] In it, he wrote "*EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled Do Not Track.*" I reviewed the same data on Feb. 10th and observed at least 12 third party sources.

Troubling questions arise as to this practice of allowing numerous companies to access the data, including:

- Does CMS have a standard agreement third parties are required to execute before being allowed access to HealthCare.gov? If so, where are these agreements?
- Does CMS have a list of all companies with third party access? If so, how long has each company been operating on HealthCare.gov?
- If written agreements exist, does CMS verify what data is being collected and that the data is being used only for the specific purpose for which it was collected?
- Does legal counsel review these agreements? What are the specific privacy provisions in each agreement?
- Is data ever sold to third parties? Does CMS charge for access?

The ability to identify a consumer based on their online activity, regardless of the perceived level of anonymity indicated by a privacy policy, was demonstrated by a recent article on a study by MIT scientists and published in the journal Science[5]. The study found that "*Scientists showed they can identify you with more than 90 percent accuracy by looking at just four purchases, three if the price is included -- and this is after companies 'anonymized' the transaction records.*"

A consumer visiting HealthCare.gov, providing only minimum information like browser, IP address and operating system could have their 'anonymous' data harvested by numerous data brokers, and would be able to match your previous browsing history on other sites and make correlations. While some level of measurement on HealthCare.gov

[4] https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-data

[5] http://www.thonline.com/news/business/article_906ceef0-f32f-521f-af2b-06dc8fab74e0.html

is needed (and it makes no business sense not to have any measurement), the use of 50 companies to perform data mining is digital overkill and puts the PII of consumers at significant risk.

2. What are the cybersecurity implications of the high number of third party connections to HealthCare.gov, and what are the vulnerabilities associated with these types of connections?

The security of HealthCare.gov has been a primary point of weakness since before the site launched Oct. 1, 2013. In my previous testimony before the House Science, Space and Technology Committee on November 18, 2013, I highlighted several major issues prior to and after launch. Primary among them was the "…lack of, and inability to conduct, an end-to-end security test on the production system. The number of contractors and absence of an apparent overall security lead indicates no one was in possession of a comprehensive, top-down view of the full security posture."

The fact that numerous security flaws, flaws that are the most basic type (unencrypted PII, SQL injection attacks, etc.) are left to be discovered by outside third parties makes it appear HealthCare.gov is crowdsourcing the security and privacy of the site.

In September of 2014, the United States Government Accountability Office (GAO) issued a report entitled "HEALTHCARE.GOV – Actions Needed to Address Weaknesses in Information Security and Privacy Controls". (GAO report, GAO-14-730[6]) The highlights clearly state that " *While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain both in the processes used for managing information security and privacy as well as the technical implementation of IT security controls".*[7]

[6] http://www.gao.gov/products/GAO-14-730

[7] http://www.gao.gov/assets/670/665841.pdf

There are several key findings worth noting and expounding upon. In this section, I will outline those findings and provide a high-level observation of the cybersecurity implications for each. It must be noted that privacy and security are intertwined – you cannot have one without the other. Policies are only as effective as the implementation, enforcement, management, audit and revision of them.

Information Security and Privacy Weaknesses Place Healthcare.gov Data at Risk (Page 35)

"*However, CMS has not fully addressed security and privacy management weaknesses, including having incomplete security plans and privacy documentation, conducting incomplete security tests…"*.

In my original testimony, this was a key area I highlighted that was critical and needed immediate resolution to. It is a known maxim that you cannot manage what you cannot measure. CMS is unable to measure the security of HealthCare.gov because it has never successfully completed comprehensive security testing of the entire site. Adding third-party applications without proper due diligence and compliance speaks to the continued lack of oversight and management of the security of the site. Willfully or unintentionally ignoring established governance mechanisms and security controls in order to add up to 50 third-party applications is incomprehensible.

CMS Has Not Fully Implemented Security and Privacy Management Controls Associated With Healthcare.gov (Page 42)

"Though CMS developed and documented security policies and procedures, it did not fully implement actions required by NIST ***before*** *(emphasis added) Healthcare.gov began collecting and maintaining PII from individual applicants."*

The failure to follow published, documented and widely available security guidance from NIST, even when compliance was mandatory, only increases the likelihood of a preventable security incident. Because privacy controls were not fully implemented, it is difficult to understand how CMS and HealthCare.gov could truly understand the scope and magnitude of any Personally Identifiable Information (PII) being collected and used by third party applications – **especially applications that are data mining products.** And, because security controls were also not fully implemented, it is just as difficult to understand how CMS prevented unauthorized access to, or use of, this PII.

CMS did not document key controls in system security plans (Page 42-43)

"Without complete system security plans, it will be difficult for agency officials to make a fully informed judgment regarding the risks involved in operating those systems, increasing the risk that the confidentiality, integrity, or availability of the system could be compromised."

This finding was written months before the existence of the 50 embedded third party applications that spawned the current hearing before the Committee. If an authorized security decision maker cannot be fully informed in order to understand the current risk, it is inconceivable to think sufficient information exists to enable 50 third party applications to operate on HealthCare.gov and to **fully understand** the associated risks.

CMS did not fully assess privacy risks in PIAs (Page 43)

"CMS privacy documentation was also incomplete. OMB requires agencies to assess privacy risks as part of the process of developing a privacy impact assessment (PIA)… However, in completing these PIAs, CMS did not assess the risks associated with the handling of PII or identify mitigating controls to address such risks."

Given the amount of time the system has been under development, and the amount of money spent, the one area CMS should have exceled at is privacy. The failure to fully understand and document the privacy impacts only means future decisions will also be based on incomplete information, as in the case of the third party applications.

CMS did not conduct complete security testing (Page 46)

"NIST and CMS guidance make clear that the security of complex systems such as the FFM and interconnected systems needs to be tested in a comprehensive fashion that takes into consideration how the systems are interconnected and how security controls are managed across all interconnected systems…"

(Page 49) "Without comprehensive testing, CMS does not have reasonable assurance that its security controls for the FFM are working as intended, increasing the risk that attackers could compromise the confidentiality, integrity or availability of the system."

Unless, and until, CMS is able to conduct a complete security test, it will forever be unable to make a qualified risk decision relating to privacy and security. This means avoidable risks will become unavoidable, and preventable incidents will become unpreventable.

A primary source of this risk was the apparent unabated installation of third party applications that collected numerous types of data from consumers visiting HealthCare.gov – data they were unaware of that was being collected and not informed of prior to. It cannot be underscored heavily enough that a fundamental task CMS should do, without further delay, is the complete end-to-end security testing of HealthCare.gov.

Control Weaknesses Continue to Threaten Information and Systems Supporting Healthcare.gov (Page 50)

(Page 51) "CMS did not effectively implement or securely configure key security tools and devices on the systems supporting HealthCare.gov to sufficiently protect the users and information on the system from threats to confidentiality, integrity and availability."

"CMS did not restrict systems supporting the FFM from accessing the Internet... Allowing these systems to access the Internet may allow for unauthorized users to access data from the FFM network, increasing the risk that an attacker with access to the FFM could send data to an outside system, or that malware could communicate with a command and control server."

The key word in the finding is "continue". Consumers using HealthCare.gov are exposed to ongoing risk that their PII will be compromised, or used inappropriately by third party applications. Most troubling is the finding that these systems had access to the Internet. The unmanaged access to outside connectivity is very disconcerting. The documented activities of Unit 61398 of the Chinese PLA, and the indictment of four of their members, relied upon this exact recipe for their activities.

The introduction of third party applications, combined with lack of security oversight and controls, raises the specter of current undetected state-sponsored penetration of HealthCare.gov. Significant data breaches have been accomplished against far more secure systems.

3. What guidance does the National Institute of Standards and Technology provide federal agencies relative to cybersecurity practices, and how would they be applicable in this context?

Throughout the GAO report, numerous references to NIST publications are documented. As NIST continues its leadership role, it has spearheaded the development of The Framework for Improving Critical Infrastructure Cybersecurity[8] (The Framework). This was authorized by on February 12, 2014, via Executive Order 13636.

In addition, NIST has also developed the *Risk Management Framework*[9] that has marshaled all of the Federal Information Security Management Act (FISMA) standards

[8] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[9] http://csrc.nist.gov/groups/SMA/fisma/framework.html

and guidance in order to generate the proper awareness and development of comprehensive security programs.

The Framework

A review of The Framework provides valuable approaches for CMS to utilize in securing HealthCare.gov. Through the Executive Order, the issues of security and privacy were specifically addressed. The Order states *"It is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."*

The aspect of privacy is so fundamental to The Framework, it is mentioned over 30 times in the document. The other aspect that makes The Framework a model approach is the voluntary collaboration between the public and private sector in developing the document. While it is voluntary, the benefit of the collective insight and experience across multiple sectors and domains is impressive.

The Framework is a collection of 97 controls and 5 discrete functions. The functions contain relevant categories and subcategories for each function, along with a set of informative references for each subcategory. The advantage of The Framework over FISMA is that The Framework is a living document – constantly updating and evolving based on the collective contributions of all.

One of the foundational documents of The Framework is NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013 (includes updates as of Jan. 15, 2014)[10]. SP 800-53 Revision 4 is a furtherance of the statutory responsibilities of NIST under FISMA.

[10] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

A key section of SP 800-53 Revision 4 is Appendix J – *Privacy Control Catalog*. It is a relatively new section intended to "address the privacy needs of federal agencies". According to the document, the Privacy Appendix addresses some of the key issues, such as:

- Provides a structured set of privacy controls, based on best practices…
- Establishes a linkage and relationship between privacy and security controls…
- Demonstrates the applicability of the NIST Risk Management Framework…
- Promotes closer cooperation between privacy and security officials…

Under Appendix J, there is a set of controls that belong to the 'Accountability, Audit and Risk Management' family. I believe control 'AR-3 Privacy Requirements For Contractors And Service Providers' would be applicable to the use of third party applications. And, if followed, would not have allowed for the proliferation of unmanaged data collection. In part, the control says:

a. *Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and*
b. *Includes privacy requirements in contracts and other acquisition-related documents.*

Supplemental Guidance*: Contractors and service providers include,* ***but are not limited to*** *(emphasis added), information providers, information processors, and other organizations providing information system development, information technology services, and* ***other outsourced applications*** *(emphasis added). Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.*

The foregoing is in addition to the security controls in Appendix F (*Security Control Catalog)* and G (*Information Security Programs).* The application of this one control could have mitigated the unnecessary exposure of PII by HealthCare.gov.

Morgan Wright, Principal - Morgan Wright, LLC

Morgan Wright's professional career includes over 17 years of service in state and local law enforcement as a city officer, state trooper and detective. He provided in-service training to the FBI Computer Analysis Response Team (CART) Team on the investigation of computer intrusions. Morgan was also an instructor for the US State Department, Diplomatic Security Service, Antiterrorism Assistance Program. He delivered briefings on cyberterrorism in Pakistan and Turkey.

Over the last 15 years, Morgan has held positions in companies who specialized in systems integration, defense, intelligence, justice, consulting, network and information security, advanced technology and broadband communications. His subject matter expertise was used for several programs, including Technology Exploration Development, Counterintelligence Field Activity; Consolidation of The Terrorist Watch Lists, and; Concept of Operations – Law Enforcement Information Sharing Program (LEISP), Department of Justice (now called OneDOJ).

Morgan's technology leadership includes Global Industry Solutions Manager at Cisco for Public Safety and Homeland Security. He later become the Vice President of Global Public Safety, End-To-End LTE, at Alcatel-Lucent, delivering the first deployment of a secure, public safety broadband network, now the mission of FirstNet.

In 2012 Morgan served as the Senior Law Enforcement Advisor at the Republican National Convention, deploying a secure, private broadband network. He currently is the Principal at Morgan Wright, LLC providing advisory and consulting services to the private sector in the areas of cybersecurity and identity theft solutions. He is also a Senior Fellow for the Center for Digital Government, a national research and advisory institute on information technology policies and best practices in state and local government.

Morgan is the author of two chapters in the 4th Edition Computer Security Handbook, and holds bachelor's degrees in Computer Information Systems and Human Resource Management. He is a 2011 graduate of the Executive Leadership and Management Program, Mendoza College of Business, University of Notre Dame.