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

November 19, 2013

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

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

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

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

It has been widely reported that Healthcare.gov has over 500 million lines of computer code. The number of daily unique visitors to the website since October 1, 2013 has trended down, reported to be no more than 500,000[1]. Many visits resulted in a website that was not functional. In contrast, Facebook is reported to have less than 20 million lines of code with 727 million daily active users in September 2013. This is based on 1.2 billion monthly active users.[2]

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

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

[2] http://newsroom.fb.com/Key-Facts

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

During my written testimony I will cover four major topics:

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

End-To-End Security Testing

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

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

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

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

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

The GAO recently released a report on the changes to FISMA[5] and the result of reviews of government agencies subject to FISMA. GAO noted a significant increase in security incidents (from 42,854 in 2011 to 48,562 in 2012), with security management weakness as the top deficiency in general control areas. The common recommendations from this report should have formed the basis of a starting point to ensure the most likely vulnerabilities were addressed, including protecting user names and passwords.

The lack of end-to-end testing was also documented in questioning by Rep. Mike Rogers of Secretary Kathleen Sebelius[6] on October 30, 2013. Based on the testimony of Secretary Sebelius as to the process of applying almost daily hot fixes and patches, it would be highly unlikely that the required remediation can occur anytime soon. This information was documented in a memo[7] from Tony Trenkle dated September 3, 2013. While the memo issues an Authorization To Operate (ATO), it does outline significant security issues on Page 2 of the Authorization Decision attachment. The 'Finding' column indicates the Federal Facilitated Marketplace (FFM) has an open high finding. Because the document is redacted, the only text readable under 'Finding Description' column says, "…the threat and risk potential is limitless." It gives until May 31, 2014 – eight months after the launch of Healthcare.gov – to fix the issue.

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

[5] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-02/ispab_feb2013_gaos-view-of-fisma_alawrence.pdf

[6] http://www.youtube.com/watch?v=y2-SeXEoaBU

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

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

User Account Creation and Registration

The second major issue was the decision to require users to create an account and register before being able to view available plans. This required consumers to provide PII before making a buying decision and is the polar opposite of how consumers buy in the private sector[8]. The lack of effective security controls, combined with the requirement to provide PII up front, has created the conditions for massive fraud and hacking.

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

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

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

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

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

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

Cybersquatting and Domain Name Confusion

A third major issue is the registration of similar, misspelled or deceptive domain names, also known as cybersquatting. A recent article from the Washington Examiner[9] quoted a cybersecurity expert who had identified 221 websites that appeared to exploit Healthcare.gov, and another 499 that also exploited the websites of state exchanges.

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

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

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

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

In addition, the current Healthcare.gov site contains no information that is readily available or easily discoverable by consumers that educates and informs them about how to make sure they are engaging with an authenticated site and service. For example, financial institutions have gone to great lengths to educate their customers about how to spot phishing[10] emails and prevent fraud. No such education material is present on Healthcare.gov.

The Insider Threat

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

During testimony on November 6th, 2013, Secretary Sebelius admitted that convicted felons could be hired as 'Navigators' and that no federal policy existed to require background checks. Currently, positions of public trust for the federal government require the completion of Standard Form 85P[11] (SF85P). At a minimum, the completion of the SF85P would identify those individuals who should be disqualified from accessing PII or sensitive information systems.

[10] http://www.consumer.ftc.gov/articles/0003-phishing

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

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

Professional Background and Experience

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

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

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

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

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

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

That same day, February 7th, the largest computer event ever known at that time – a full blown Distributed Denial of Service attacks (DDoS) - was in full force taking down Yahoo, CNN, eBay, Dell and Amazon. As a result, our company was asked to testify before a Subcommittee of The Committee on Appropriations, United States Senate[12].

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

Again, our company was asked to testify[13] about this event, this time before the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform, House of Representatives. The ILOVEYOU virus

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

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

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

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

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

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

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

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

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

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

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