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

1. FULL TESTIMONY OF MR. WAYLON KRUSH 1

2. SUMMARY OF TESTIMONY TO THE US HOUSE OF REPRESENTATIVES 4

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 "Tavenner 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.