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 Homeland Security

November 13th, 2013

Table of Contents

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 Homeland Security U.S. House of Representatives

"Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?"

November 13, 2013

Waylon W Krush

Testimony

"Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?"

November 13, 2013

Chairman McCaul, Ranking Member Thompson, and members of the committee; thank you for this opportunity to testify today 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 both federal and commercial clients.

I am also a founding member of the Warrior to Cyber Warrior program. Warrior to Cyber Warrior provides, at no-cost, a 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 the recent events surrounding the Healthcare.gov website and related 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 was recently asked by the press if I would, as a cyber security professional, trust my own personal data to HealthCare.gov. I said yes, that I would. I stand by that statement.

This is not because I believe that HealthCare.gov is 100% secure. There is no IT system, Federal or otherwise, that can make this claim. Instead my confidence in HealthCare.gov is based on my hands-on experience with the rigorous processes the federal government has instituted to effectively manage - not eliminate, but manage - cyber security risk.

Now I realize it is a bit odd for a cyber security professional to come before Congress and preach confidence in our government's security posture. We cyber security folks are usually better known for pedaling cyber doom and gloom. However, the truth is, there is plenty of cause for confidence, particularly when it comes to federal cyber security.

To explain why I feel this way, I would like to focus my testimony today on the Risk Management Framework and how it relates to some of the concerns recently brought up in the ongoing media coverage of Healthcare.gov.

Now, I have been given just five minutes to very briefly describe the extensive cyber security processes and regulations that provide the foundation for US Government system security. To put this task in context, a few years ago a colleague and I wrote a book entitled the The Definitive Guide to the C&A Transformation. In this book we did our best to scope down thousands upon thousands of pages of federal cyber security and privacy regulations into just 600 pages of easy reading.

The easy reading part is a joke, but the level of depth and rigor in the process is not. Here today, I will try to distill these processes even further, into just five minutes of testimony. During these five minutes I will do my best to inform everyone on how the six step federal Risk Management Framework (RMF) supports the Federal Information Security Management Act (FISMA).

This, in turn, should provide a baseline for understanding the security processes governing healthcare.gov, and in reality any government IT system. I also hope that my testimony will help folks interpret the now famous "decision memo" - originally intended for Marilyn Tavenner - that describes some of the known security risks faced by HealthCare.gov.

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.

In conclusion,

I hate to tell everyone this, but at this point and time there is no cyber security silver bullet. If there were, I would be selling them – lots of them. A secure system requires the right people, process, and technology to work together, harder, smarter, and faster than the adversary.

2. Summary of Testimony to the US House of Representatives

On Wednesday November 13th, 2013, Mr. Waylon Krush will appear before the Homeland Security Committee of the United States House of Representatives 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.

1.1. Summary of Mr. Krush's Testimony

- 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. Note that this is not called the "No Risk Framework," but rather provides detailed guidance to security professionals on the proactive and effective management of risk to federal IT infrastructure.
- An understanding of the Federal Risk Management Framework gives us the tools to properly interpret the "Tavenner Memo" and understand Healthcare.gov's security posture.
- **Mr. Krush has publicly stated** that he would entrust his personal data to Healthcare.gov. He stands by this statement.
- There is no such thing as a 100% secure system. Cyber security professionals seek instead to manage risk.

1.2. Mr. Krush's Qualifications

- **Mr. Krush is the CEO of Lunarline**, a *Service Disabled Veteran Owned Small Business* that provides cyber security 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 nonprofit organization **Warrior to Cyber Warrior**. Warrior to Cyber Warrior provides, at no-cost, a six month cyber security boot camp for returning Veterans to equip them for the challenges of the civilian cyber world.
- **A Veteran of the US Army**, Mr. Krush is a recipient of the Knowlton Award – **one of the highest honors in the field of Intelligence**. For his outstanding contributions to US National Security, he was also recognized as the **718th Military Intelligence Soldier of the Year**, the NSA Professional of the Quarter, won the Voice of America Award and is a two time winner of the American Legion Award.
- As founder of Lunarline, Mr. Krush has developed a reputation for **cyber security thought leadership**. He has appeared as a cyber security expert on CNBC, NPR, Fox Business 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".