Statement of Joshua Corman

For the House Energy and Commerce Committee's Subcommittee on Health
"Examining Cybersecurity Responsibilities at HHS"

May 25, 2016

Opening:
Chairman Pitts, Ranking Member Green, and distinguished Members of the Subcommittee on Health, thank you for the opportunity to testify today.

My name is Joshua Corman. I am the Director for the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security at the Atlantic Council – a non-partisan, international policy think tank. I am also a Founder of I am The Cavalry (dot org) – a grass roots, cyber safety volunteer focused on public safety and human life in the internet of things. Additionally, I am an adjunct faculty for CISO Certificate Program at Carnegie Mellon University's Heinz College where I've worked with dozens of CISOs at a time. Lastly, I am currently serving on the HHS Cybersecurity Task Force – initiated by Congress in the Cybersecurity Act of 2015.

Over the past 15 years, I've been a staunch advocate for the role of CISO (Chief Information Security Officer) – an increasingly difficult role. A significant portion of my research and career has been focused on the vanguard of emerging threats, and challenges affecting cybersecurity as well as identifying, advancing, and originating new and more effective responses to these growing challenges. As such, I've worked deeply with many of the Fortune 50, 100, and 1000 – on emerging issues such as the rise of cybercrime, the rise of nation state espionage, the rise of Anonymous & hacktivism, and the growing exposures to cyber safety and national security as we become increasingly dependent on the Internet of Things.

I say all of this, because I've had a front row seat to the evolution of the role of a CISO (and related titles and duties: ISO, CSO, CRO, Risk Management, Director, etc.). While there is no "one true path" to success, there are a number of factors which contribute to the overall success of a Cyber Security program. What I hope to do here today is to frame a few of those factors for the Subcommittee, to explore some of the costs/benefits of alternative reporting structures to the CIO, to speak to the value of experimentation in this evolving space, and then to answer any questions that you may have as you consider your choices.

Cybersecurity context in 2016:
It is worth noting that Cybersecurity is a relatively nascent field – and is having a very difficult time rising to meet the challenges. High profile failures in the private

sector and in governments are becoming quite clear. About 100 of the Fortune 100 have lost intellectual or trade secrets to foreign industrial and nation state adversaries. Most Merchants have had a breach of credit cards – despite being compliant with "best practices" and industry compliance regulations like PCI DSS (Payment Card Industry Data Security Standard). Breaches are getting bigger like Target and Ashely Madison. Breaches are hitting Federal Agencies like the Pentagon and OPM. Breaches are getting dangerous as we connect everything in the Internet of Things – such as the denial of patient care at Hollywood Presbyterian Hospital in California due to Ransomware. The Internet of Things is where bits & bytes now meet flesh & blood. In fact, the problem statement which caused me to form "I am The Cavalry" was:

"Our dependence on connected technology is growing faster than our ability to secure it – in areas affecting public safety and human life."

As society (and the government) increasingly depends upon IT, the importance of effective cybersecurity must also rise in kind. In the case of HHS, the consequences of failure may bleed into public safety and human life. We must be at our best.

It is hard to argue that we're (collectively) doing a very good job. A situation like this merits experimentation, innovation, and even a grand challenge – to ensure we can enjoy the promise of connected technologies (versus the perils of getting them wrong). It seems prudent to look at what the best are doing and to do controlled experimentation.

Factors which enable an effective CISO and Cybersecurity program:
Some of the factors contributing to the success of a cyber security program include:

1) The individual CISO's qualifications and experience
2) The reporting structure (e.g. to the CIO or others) <- *in focus today*
3) The relationships the CISO maintains across key executive stakeholders
4) CEO and Board level visibility and prioritization
5) The application of Risk Management principle versus blind, minimum compliance to standards and "best practices".

6) The ability of the CISO to both influence IT and business choices in advance – versus react to/inherit the downstream consequences of indefensible choices

Migration away from reporting to the CIO:
Regarding the #2 "Reporting structure", it is important to note there is not "one path to success". While CISOs can be successful reporting to various different executives, there has been a migration *away* from the more historical relationship under the CIO and *toward* other formats such as to the General Counsel, CFO, CEO, and the Board of Directors, etc. - including dotted lines and the like. In general, the belief is that a CISO reporting to a CIO is a structural conflict of interest – as there can be tensions between their missions, their performance objectives, and their budgets.

Availability and Uptime: The CIO is (in part) measured on the availability of IT services. In contrast, the CISO may need to temporarily interrupt said service in order to test for exploitable weaknesses – or to patch and update vulnerable systems to avoid successful exploitation.

Deployment of Services: The CIO may be held to deploy new services within an acceptable, projected time frame. A lack of acceptable security and/or compliance readiness may merit delays to the launch of said services. Worse, even the assessment of security and/or compliance can be skipped or compressed – affecting the overall outcome.

Cost Reductions: The CIO may wish to use lower cost alternatives for IT (Information Technology), and if they fail to properly factor the ability to meet security and/or compliance requirements, they may see the CISO as an obstructionist and/or a budget risk.

Zero Sum Budgets: The CIO has a dedicated budget, and they tend to prioritize more IT staff and more IT purchases than over more security staff or security reduction. It is not uncommon for a CIO to state: "We will only approve compliance mandatory security spending and not one penny more." First, compliance is no proxy for security or resilience against attackers. Second, compliance regimes can't possibly inform the agency specific or business specific risks and objectives – which require broader Risk Management practices. More

importantly, this approach has the mistake of focusing only on regulated data – and often misses less replaceable asset types such as intellectual property, trade secrets, sensitive organizational data, and even cyber physical systems damage and safety implications (depending upon the industry/use case).

NOTE: This should not suggest that Cybersecurity should be expense. On the contrary, intelligent selection of more defensible IT , smarter security by design architectural choices, complexity reduction, operational excellence, and situational awareness can both improve cybersecurity and reduce costs and wastes in the agency or business.

IT tunnel vision: While historically, CISO mostly focused on IT risk, the modern CISO must factor for other types of risks, mission/business objectives, and the like. An effective and comprehensive Risk program must span multiple disciplines

Alternative Reporting Structures for the CISO:
Each reporting structure comes with trade-offs and advantages/disadvantages. I've often joked that after 2 years under each – in rotation – you just might achieve a full security program.

There have been dozens of articles and studies recently showing evidence of the gains organizations get from reporting structures (other than CIO). This article highlights "Seven reasons the CISO should report to the CEO and not the CIO" http://www.cio.co.uk/it-security/seven-reasons-ciso-should-report-ceo-not-cio-3634350/

It highlights two oft quoted metrics from a PWC Study, namely:

- Organizations where the CISOs report to CIOs have 14% more downtime due to security incidents, according to a study by PwC.
- Organizations where the CISO reports to the CIO have financial losses that are 46% higher, according to the same PwC research.

For these or others, I can provide anecdotes and examples – as merited. Here are a few simple examples:

General Counsel: CISOs who previously could not find support for anything but regulated data and/or compliance minimums, find that reporting to the General Counsel affords them more attention to trade secrets, intellectual property, sensitive organizational data, and anything deemed "material". This also elevates risks closer to board level attention.

CEO: With a direct line to the CEO, it is often easier to truly align the program to business priorities and objectives. Also the CEO is better poised to explicitly resolve tensions between competing priorities or trade-offs. It doesn't hurt to drive a culture of security when the top executive is making it a priority – all the way at the top. The odds of informing lower risk business and IT moves before they are made go up (versus reacting to less tenable or defensible choices after they are too late to materially improve).

CFO: Given the scrutiny and legal consequences introduced upon CFOs of publically traded firms via, for example, Sarbanes-Oxley, working for a CFO often affords you the permission and rigor of using audit functions and the internal gravitas they convey. This is useful for streamlining the more established aspects of a cybersecurity. In theory, this will liberate the CISO to do better on emerging and less established parts of their programs. However, I have seen a CFO reporting structure create a tunnel vision on the easy-to-audit-only bits.

The value of experimentation:
IT is in a constant state of flux and improvement. It is one of the fastest moving parts of the global economy. At the vanguard of this innovation is a movement called DevOps - short for the union and aligned incentives of software Development (Dev) and IT Operations (Ops). In fact, DevOps is being further extended by some (including me) into Rugged DevOps - a further Union with the Rugged Software Manifesto and adopters.

Core to their philosophy and success is a spirit of continuous experimentation and improvement. Fail Fast, Iterate. An advantage of controlled experimentation is one can "fail small" with little downside risk, and uncover very large upsides which can be later replicated and scaled. An HHS reporting structure change, if successful, could reveal a pattern worth repeating in other agencies. Einstein is quoted saying that insanity is doing the same thing over and over but expecting different results. The modern Lean and DevOps cultures have fully integrated this

mindset and continue to shatter expectations of what was previously thought possible. Combined with the private sector trends toward more effective CISO reporting structure models, a controlled experiment in HHS may carry little downside - especially if objectives/measurements are established early and tracked.

Members may have heard about experiments within the federal government like the GSA program known as 18F – which is bringing modern DevOps principles into Federal IT. One of their early projects with DHS USCIS (US Citizenship and Immigration Services). The USCIS CIO Mark Schwartz is enjoying tremendous results at a more nimble, responsive, and less wasteful approach to IT. Part of the hope of such experiments is to fail small – and also to find new and more effective patterns which can later be applied to more parts of government.

Lastly, in the context of a DevOps culture, there is an increased “flattening” of organizational relationships which may diminish the importance of exactly where the CISO reports, but in a more hierarchical and traditional context, the negative effects of being underneath a CIO may be more pronounced.