Written Statement of Brigadier General (ret) Gregory J. Touhill
U.S. House of Representatives
Committee on Science, Space, & Technology
Hearing on "Ransomware and whether or to what extent the May 11th Executive Order, NIST Framework, or Private Sector Could Assist in Preventing Future Attacks."
Washington, DC
June 15, 2017

Good morning, Chairman Smith, Ranking Member Johnson, and Members of the committee. Thank you for the opportunity to appear here today to discuss cyber risk management.

I am retired Air Force Brigadier General Greg Touhill. I currently serve on the faculty of the Carnegie Mellon University's Heinz College, where I instruct on Cybersecurity and Risk Management. I appear today at the invitation of the committee and am testifying on my own behalf.

Prior to my current appointment, I served as the United States Chief Information Security Officer in the Executive Office of the President and, before that, in the U.S. Department of Homeland Security, where I served as the Deputy Assistant Secretary for Cybersecurity and Communications. During that period I also served as the Director of the National Cybersecurity and Communications Integration Center (NCCIC), commonly referred to by its acronym, "N-KICK".

During my Air Force career, I served as one of the Air Force's first cyberspace operations officers and was the 81st Training Wing commander where my team and I created the Air Force's cyberspace operations training programs for officers and enlisted personnel. I maintain both the Certified Information Systems Security Professional and Certified Information Security Manager professional certifications.

Cybersecurity is a risk management issue. Many people mistakenly view it solely as a technology problem. Cybersecurity is a multi-disciplinary risk management issue and is an essential part of an enterprise risk management program.

The recent Wannacry ransomware attack highlights the risk exposure many entities in both public and private sector accept when they do not implement best practices. Last month we saw many entities around the world fall victim to the consequences of Wannacry because they did not practice widely recognized best practices, such as keeping their hardware, software and network security procedures up-to-date in today's ever-evolving threat environment.

While Wannacry had severe impacts to many organizations around the world, it could have been much, much worse.

Wannacry did not incorporate what we call a classic “zero day” attack, where there is no advance warning. In fact, had the victim organizations updated their systems upon the initial warnings from entities like the US Cyber Emergency Readiness Team (USCERT), the FBI’s Infragard program, Carnegie-Mellon’s C-CERT, and private organizations such as the ISC2, ISACA, and the Center for Internet Security, I believe it is likely for the vast majority of victims that the attack could have been averted.

Systems using unpatched versions of the Windows 95 operating system have been highlighted as exemplar victims of the Wannacry attack. Microsoft who, after a long and very public notification process, discontinued support to the Windows 95 operating system in 2014, about 19 years after its initial release. However, in light of the warnings and their own research, in March of this year Microsoft issued a rare emergency patch to Windows 95, nearly three years after they had discontinued support of the software. Despite these extraordinary actions, many organizations still did not heed the warnings and properly patch and configure their systems. As a result, they fell victim to Wannacry.

The lesson here is that in today’s highly-connected Internet-enabled world, our national prosperity and national security require us to ensure that we adhere to best practices to better manage our enterprise risk. One of those best practices is to keep our systems, both hardware and software, properly maintained and configured. In my view, this is a matter of due care and due diligence.

Regrettably, despite numerous warnings about aging hardware and software systems, both public and private sector organizations continue to accept significant risk by operating technically antique systems and unsupported software vulnerable to exploitation by hackers and other criminal groups.

The risk continues to grow as all aspects of our society, including our critical infrastructure, national economy, and even societal institutions, are reliant on a safe and secure Internet that is always on-line and available.

We got lucky with Wannacry. While warnings to update systems helped many harden their systems, many failed to do so and fell victim to the Wannacry ransomware. Fortunately, a cyber researcher discovered the Wannacry code contained an instruction that told the program to cease functioning if it made contact with a designated web site. Such sites are often used to provide command and control to the malicious software. The instruction found by the researcher is a rudimentary “kill switch” type of command that often is used by programmers to create a means of stopping a program or process.[i] The researcher found that the domain had not yet been registered and, for less than $11USD, created the domain. Once the domain was created, Wannacry-infected devices made contact with the domain, received a response that the domain was active, and the Wannacry program terminated on the infected devices per its instructions. Most programs are not written like Wannacry and aren't so easy to stop. We were lucky.

I believe Wannacry was a slow-pitch softball while the next attack is likely to be a blazing fastball. This time we anticipated an attack and issued warnings with valuable practical advice to mitigate it. The creators of Wannacry overtly placed a "kill switch" instruction set in the program's code. A researcher discovered and implemented that "kill switch" quickly to interrupt the attack. Next time I do not believe we will be so lucky.

We need to step up our game and take immediate actions across both the public and private sectors to better manage our cyber risk before the really fast pitches come flying into our networks.

I believe that stepping up our game includes building upon public-private sector partnerships and information sharing.

While I served as the Director of the National Cybersecurity and Communications Integration Center (NCCIC), I referred to our mission as being the lead for what I called the "National Cyber Neighborhood Watch". I believe that the "See Something, Say Something" concept applies to the cyber domain as it does to physical domains. Like our physical neighborhoods, when we see a problem, we need to point it out and share threat information and best practices to mitigate those threats with our neighbors. When we do so, we have a safer, more secure, and better Internet that promotes our national prosperity, our national security, and the values our society cherishes.

Sharing information about cyber threats, indicators of compromise, and best practices are essential parts of being responsible members of the "Cyber Neighborhood". I believe the US government is a leader in fostering public and private sector partnerships yet more work needs to be done to improve these partnerships so that all parties are satisfied with the relationships.

For example, I believe we need to relook at how we classify information. I found during my public sector career that well-intentioned government entities over-classify information. That stifles the timely sharing of information in an environment that already moves at light speed. Regrettably, some elements of the government hoard information that would be invaluable to America's critical infrastructure and other elements of the government. They do so under the guise of "protecting sources and methods." I found the bulk of classified indicators of compromise that came to my team in the NCCIC could be found on the Internet within days of our receiving it. I believe we ought to relook how we classify information and, instead of making the highest classification the default setting for data collection and dissemination, we ought to flip the default to a shareable setting. Classification at the highest level should not be the default setting; it should be the result of a deliberate determination by appropriate authorities that the information indeed is sensitive.

Sharing of information goes both ways. I thank the Congress for the creation of the Cybersecurity Information Sharing Act of 2015, which specified that private sector entities would not be penalized for sharing with the federal government and incorporated privacy provisions. This legislation was extremely helpful in providing "top cover" for programs such as the creation and fielding of the Automated Indicator Sharing (AIS) system developed by DHS. This system shares information about cyber threats between subscribers at machine speeds, reducing risk exposure to known threats. At the time of my departure from public service, over 3000 partners in the private sector had direct and indirect access to this capability. In essence, this technology took the time to share information from months to milliseconds.

While AIS is a welcome technology to improve public-private partnerships, it should not be viewed as the only means of sharing information. I view human relationships as critical. For example, while I was at DHS I engaged in monthly meetings with industry groups such as the Information Technology Sector Coordinating Council. I believe we need to encourage and remove impediments to direct engagement with industry leaders that will improve sharing of best practice information from experts in the private sector while providing those we serve with an open and transparent government. Teamwork is essential and the worst time to exchange business cards is during a crisis.

In all my many engagements as the US CISO, DHS Deputy Assistant Secretary, and NCCIC Director, I have been a huge proponent of incorporating the Framework for Improving Critical Infrastructure Cybersecurity into enterprise risk management programs in both the public and private sectors. I still am.

A framework is a basic structure underlying a system or methodology for solving a problem. For cyber risk management, our National Cybersecurity Risk Framework promotes a best practices-based methodology focused on:

1. **Identify**ing your assets and the threats against them
2. **Protect**ing against those threats based on your risk appetite
3. Being able to **Detect** when you are under attack or exceeding tolerable risk levels
4. Being able to **Respond** appropriately
5. Building in resiliency so that you can **Recover** when your bad day occurs

This core risk framework is not just a great one for Cybersecurity. I submit it is a great framework for risk management in general.

Most people refer to it as the NIST Cybersecurity Risk Framework. I prefer to refer to it as the National Cybersecurity Risk Framework because, while the NIST led the team that created it, it truly was a crowd-sourced document that incorporates best practices from numerous organizations and citizens, including me. It wasn't developed just by NIST. It was developed through the open call for best practices that NIST so brilliantly led.

As such, I suggest we formally name it the National Cybersecurity Risk Framework to reinforce that it is a best practice framework applicable to all of us, regardless of whether we are in the public sector, the private sector, in academia, or even at home. Our core National Cybersecurity Risk Framework is the best one I've seen and we ought to widely adopt it to better help manage our risk posture.

I am pleased to see the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure issued by the president on May 11th acknowledges that cybersecurity is a risk management issue. I further am pleased that it directs agency heads to use the framework to manage the agency's cybersecurity risk. Moreover, I am delighted that the order calls for a more modern, secure and resilient architecture. The companion OMB Memorandum 17-25, issued on May 19th, gives solid guidance for measuring progress toward meeting goals specified in Section One of the Executive Order. Both of these documents build upon the substantive work accomplished in both the Bush and Obama administrations to improve our cybersecurity risk posture and set the stage for even greater improvements.

While the executive order and the OMB memorandum are positive measures taken by the executive branch, there are opportunities the Congress can act upon to further enhance our cybersecurity posture. For example, despite the position being recognized as a best practice in the private sector for over 20 years, the Congress has yet to formally recognize the Federal Chief Information Security Officer position nor give it the specific authorities it needs. While I served in the position, I leveraged the experiences of my long career in public service, personal relationships and delegated authorities in order to perform my duties successfully, but it could have been a lot easier with help from the Congress. I recommend the Congress formally specify the Federal Chief Information Officer position in the next version of the Federal Information Security Management Act or comparable legislation and grant specified authorities to better manage our cybersecurity risk.

I am pleased this committee recognizes the importance of cyber risk management and implementation of the cybersecurity risk framework to better manage and reduce our cyber risk exposure. I have read the proposed HR 1224 bill and applaud your intent to improve the federal government's cybersecurity posture. I believe Section 20A to direct implementation of the framework and creation of the Federal Working Group to develop meaningful metrics and public reporting is hugely important and exercises the oversight appropriate in this risk environment.

I do not believe Section 20B, as currently written hits the right target. I am pleased that the committee wisely recognizes the importance of audits and what I call, “following through”. However, I submit the following recommendations for your consideration and our potential discussion today:

1. National Security Systems should not be exempt. Based on my experience as a cyber operator in both the .mil and .gov domains, I believe the risk framework applies equally to all systems, especially to national security systems. I would not exempt them from the provisions of this act.
2. NIST should not lead cyber preparedness audits. Preparedness is a measure of operational readiness. The NIST mission and culture is deliberately not aligned with operations nor auditing. NIST cyber experts do not have the culture, expertise, manpower, or resources to conduct or orchestrate effective auditing. Moreover, NIST is widely viewed as “an honest broker” in developing standards and promoting new technologies. Assigning NIST duties to oversee audits or compliance activities changes their writ and perceptions about NIST’s current and future roles. One of my senior colleagues in government service believes such action will have what he calls, “a chilling effect” on many of the relationships NIST has within government and industry. Additionally, many of my colleagues in the public, private, and academic communities have commented that their current relationships with NIST are “learning” relationships based on a common quest to identify and incorporate best practices. Assigning NIST duties to lead auditing or compliance activities changes those relationship and not in a good way. I have had numerous senior colleagues confess to me it likely will inhibit or stifle the free exchange of information from public and private entities to NIST. I recommend that the Congress not assign auditing and compliance activities to NIST and consider alternative actions.
3. I recommend the Congress direct the existing Inspectors Generals and Auditing functions, as choreographed through the Council of the Inspectors General on Integrity and Efficiency (CIGIE), to implement the actions of section 20B. This community has the culture, expertise, and organizational function to execute the tasks specified in Section 20B of the proposed legislation. The CIGIE and its members already have been incorporating the National Cybersecurity Risk Framework as part of their assessment criteria in many of their inspections and audits. In 2016 during my tenure as the U.S. Chief Information

Security Officer, I had discussions with the CIGIE and its cyber committee leadership to synchronize the efforts of OMB and the CIGIE to assess the cybersecurity risk of the executive branch departments and agencies. With the new executive order and companion OMB Memorandum 17-25, the stage is already set to follow-through on these efforts. I strongly urge the Congress to support these efforts by editing the proposed Section 20B to assign the proposed auditing and compliance actions from the NIST to the existing Inspectors Generals and auditing functions.

Again, I thank you for inviting me to discuss cyber risk management with you today. I look forward to addressing any questions you may have.

[i] Many researchers, academics, and practioners cite the 1988 Morris Worm incident as a reason why programmers should install a "kill switch" in the event that their program goes "out of control." See the following for more information on the Morris worm: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-Internet-to-its-knees/?utm_term=.e38dbbf0a2c0