TESTIMONY of

Colonel Gent Welsh
Commander, 194th Wing, Washington Air National Guard

BEFORE THE

Senate Committee on Energy and Natural Resources
U.S Senate

April 4, 2017

TESTIMONY BY

COLONEL GENT WELSH
COMMANDER, 194th Wing, WASHINGTON AIR NATIONAL GUARD

Madam Chair Murkowski, Ranking Member Cantwell and members of the Committee, my name is Colonel Gent Welsh. I'm the Commander of the 194th Wing for the Washington Air National Guard. Thank you for the honor to participate in such a crucial conversation.

Please note that I appear before the Committee today in a National Guard, Title-32 status. Although I have served as an Air National Guard officer for more than 23 years, my testimony has not been reviewed or approved by anyone in the United States Air Force or the Department of Defense.

I don't need to convince you that our nation currently faces sobering threats in the cyber realm. You've heard the alarming statistics on the number of daily attacks on our critical infrastructure to include the energy and financial sectors, our military, and other entities across the public and private spectrum. We know that as a nation, we desperately need more cyber warriors, more cyber collaboration and more cyber training. We know that the consequences of inaction will bring disaster. And we know it's not a question of 'if,' but 'when.'

Media reports concerning our national vulnerability to a significant cyber-attack often refer to a "Cyber 9/11." The media didn't invent that rhetoric – it's been discussed in the halls of Congress, as well. In early 2012, Senator Joe Lieberman rose to the Senate floor to declare "Mr. President, I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens. Would-be enemies probe the weaknesses in our most critical national assets – waiting until the time is right to cripple our economy or attack a city's electric grid with the touch of a key. The system is blinking red. Yet, we fail to connect the dots – again."

According to the *National Security Strategy* of May, 2010, "Cybersecurity threats truly represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale."

Madam Chair and members of the committee, the front lines of the next conflict are not overseas in some country most folks can't find on a map. They are right here, right now at the doorstep of every owner and operator of our nation's critical infrastructure.

And the Washington National Guard, under the leadership of Major General Bret Daugherty, the Adjutant General (TAG), is doing everything possible to address this growing threat.

For the past five years, we've been tirelessly working on efforts to better secure critical infrastructure in our state from the consequences of a devastating cyber attack. In Washington

state, our Adjutant General is also the Governor's Homeland Security Advisor and the overall head of Emergency Management efforts. These positions give him incredible "convening authority" to pull people together and enable serious conversations and planning efforts concerning a significant cyber attack. In our state, through these convening authorities, and with the help of Sen. Cantwell and members of our House delegation like Representatives Kilmer and Heck, we're able to get industry, state and local governments, owners and operators of critical infrastructure, the National Guard, and the educational services sector all together regularly in a room to make steady progress on mitigation, preparation, response and recovery efforts in cyber. These four phases may sound familiar to you because they are the four phases of Emergency Management as outlined in the National Response Framework. It's important to highlight that our state treats cyber threats like any other threat we plan and prepare for.

It takes more than simply acknowledging that someday we might see a significant cyber event that hits us like 9/11 did. If you haven't already, I'd highly recommend you download and read through the Executive Summary of the 9/11 Commission Report. It's both a fascinating and tragic read at the same time.

At its core, it acknowledges that we knew there was a problem. We were aware that Al Qaeda had interest in commercial aviation, and we weren't able to do anything about it until it was too late. The 9/11 Commission Report also highlighted four failures.

The first was imagination. I'm sure you've heard, "Failure of Imagination."

But did you realize that there were three other failures? They include policy, capabilities, and management.

If you take that same 9/11 Commission Report and replace the word 'airplane' with 'cyber,' it's scary and striking at the same time. Doing so makes it crystal clear that we face the same four failures – imagination, policy, capabilities and management – in our cyber preparation just as we did prior to 9/11.

As I mentioned, we're addressing these failures as quickly as we can in Washington state. And we appreciate your help – the fact that you're here and we're talking about this topic addresses the failure of imagination.

While it's recognized at the national level that a significant cyber attack could occur domestically in the future, the true failure of imagination lies within the unaddressed gap that exists between the rhetoric surrounding the nature of the cyber threat and our actual resource capacity to respond and recover from an attack. Federal efforts have principally emphasized efforts to prevent cyber attacks, rather than anticipate response considerations. Since 2000, federal government strategies have consistently emphasized the importance of information sharing, partnerships, analysis and warning capabilities, and coordinating efforts in cyberspace among relevant entities to minimize the impact of incidents. While these information sharing and coordinating mechanisms are vitally important, they have done little to anticipate and develop actual response capacity that would be needed post-attack. In remarks before Congress in October 2013, Charley English, the director of the Georgia Emergency Management Agency,

stated, “while the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations.”

I’d like to also address the policy, capabilities and management failure pieces from a cyber perspective.

The US Department of Homeland Security designates 16 different sectors as critical infrastructure. Some of these are obvious – like the power and water sectors. Others are things you might not immediately think of, like dams (and we have a lot of those), healthcare and public health, agriculture and food, and critical manufacturing. In Washington state alone, we have operations in every one of these sectors. Before 9/11, the federal government had never fully put these sectors together and hadn’t put policies and actions in place to better secure these sectors. Why? Likely because more than 85 percent of our national critical infrastructure is owned by the private sector.

That can make securing our critical infrastructure sometimes difficult and requires a very high level of trust and cooperation with the private sector. That trust isn’t always easy to build – especially when you’re dealing with cyber. There is an on-going national debate on how the government can work better together with the private sector. And in Washington state, we like to think we’ve developed the mold. In our state, the Washington Military Department has become a key player in the cyber discussion relating to securing critical infrastructure in this state. And by doing so – we’re able to address some of the failures I mentioned earlier. We’re fortunate that state law provides us with the policy and authorities. We have the capabilities through the more than 600 cyber professionals that work in the Washington National Guard. And we have the outreach mechanisms to touch not only the private sector but also the ability to leverage existing emergency management relationships and evangelize on cyber all the way down into our local governments.

This has helped Washington state secure the cooperation and support of the private sector. We have numerous private and semi-privately owned organizations that we now consider strong partners – to include Pacific Northwest National Laboratory and Idaho National Laboratory. We’re also working closely with several utility companies. These partners are making instrumental contributions to our efforts to enhance national security.

The cooperation and support of the private sector is necessary to be successful at any level in cyber security as it relates to critical infrastructure. The private sector will need help when something bad finally happens, whether that’s a conduit for information sharing or assistance in requesting federal resources. A major cyber event won’t just have digital consequences. Consequences will manifest themselves in the physical space very quickly and create a complex issue to manage.

With all of that said, to get true cooperation with the private sector, government must be able to offer something tangible and something of value. When we look at cyber, we have to have something the private sector needs in exchange for meaningful and purposeful cooperation and outreach. That’s why the discussion before about policy, authorities and capabilities matters. If government has clear policies and plans for either resources or outside assistance, that makes the

decision to work with government easier. This process is no different than how we work with the private sector during any other emergency or disaster.

An additional tangible resource we've been able to assist the private sector with is security clearances. The Adjutant General, in his role as Homeland Security Advisor, is able to sponsor folks for clearances based on their potential requirement to have access to classified information. This is a huge benefit to industry and is a confidence building mechanism in terms of public-private information sharing partnerships. In terms of threats, we'd love to know what industry is looking at, and they certainly want to know what we're looking at.

While we've only been at this for five years, they've been incredibly busy. In 2012, we formed an Integrated Project Team within state government to develop the first ever significant cyber incident response plan for the state. This plan goes beyond state agencies to include the whole state. After building the plan, we began a significant process to exercise it, not only at the local level but nationally. Our efforts in this area have truly led the nation and positioned Washington in many ways as the national thought leader in cyber security. From 2014 to now, we have continued to work with our state critical infrastructure sectors to refine our statewide plan, and have involved the private sector both in our planning process and exercises. We know we still have a lot of work to do, both in integrating all 16 sectors of critical infrastructure into the process and in developing the right mechanisms within government to address emerging cyber threats. We did a lot of work after 9/11 in the physical security space across all 16 sectors and now we're attempting to do that in cyber.

Here's where I get to brag a little more about our folks. We have more than 600 cyber professionals in the Washington Military Department between the Air and Army Guard, and our State Guard. After news spread about the assessment our folks accomplished at Snohomish County Public Utilities District back in 2015, we have had a steady stream of visitors who want to learn more about Washington state's secret sauce in how cyber cooperation works. What makes this success possible is what we call the power of the Citizen Airman and Citizen Soldier. Remember our typical Soldier and Airman drills one weekend a month and two weeks a year. Outside of that obligation, they have full time jobs. Our cyber folks' day jobs are out there in these very same industries, many working in sectors of critical infrastructure. They bring in a remarkable understanding of the private sector's needs as well as their capability shortfalls. They also bring credibility in dealing with these organizations. Our folks are not full time career government employees doing industry outreach. These are truly folks that understand government and understand private industry because they work in it every day and are able to bridge gaps. What a combination! Just last year, we hosted a visit from former Secretary of Defense Carter where he highlighted our efforts working with critical infrastructure as a national model.

Looking forward, securing Washington's cyber critical infrastructure is General Daugherty's top priority in cyber. We've developed a five year strategic plan that guides this agency in all of our cyber interactions. We are continuing our meaningful outreach work with actual sectors of critical infrastructure. We're working resource typing. That means working with DHS and FEMA on developing specifications for actual cyber response teams that can be deployed to help industry, the same way we resource type any other response asset. I'm not sure it would surprise

this committee, but as of today, there is not a single cyber resource type within DHS or FEMA that allows a state to request cyber response assistance from the federal government or even state to state using existing emergency management processes.

We're also working with our Congressional delegation to bring a cyber schoolhouse to Washington state that allows us to train members of the critical infrastructure sectors alongside our national guard members. Sharing information and best practices among those tasked to defend this nation with the private sector is how we'll be more resilient to a significant cyber attack in the future. Cyber resilience requires a disciplined and team engagement.

And finally, we continue to bring in cyber force structure to the Washington National Guard. Our past efforts are bearing fruit in that Washington is viewed as a place to invest additional resources at the national level.

We believe our work is a model for other government organizations and have four key recommendations for the federal government to consider to supplement and support our work:

- Develop federal governance and policy that sets forth a clear process to provide critical resources both before and following a cyber event that help harden our critical networks, and respond/recover from the follow-on consequences of a cyber attack;
- Don't treat cyber differently and use existing emergency management processes to respond/recover from a significant cyber attack. Encourage each state to identify a key official to lead cyber efforts and provide that individual with convening authority or the ability to pull various sector leads together to develop meaningful solutions and strategies;
- Ensure joint research efforts between the states and federal government continue. Washington state is seeing tremendous success through our partnerships with PNNL and INL; and
- Provide for a Cyber Schoolhouse that allows for the sharing of knowledge and expertise among National Guard and civilian critical infrastructure partners, with the ultimate goal of developing a Center of Excellence for those defending this nation.

Thank you again for the opportunity to appear here today and share some of our efforts out in the "other" Washington!