Statement for the Record
Ronald Nielson
Parsons Corporation

Mr. Chairman, Senator Nelson, distinguished members of the Subcommittee, thank you for the opportunity to testify today as a subject matter expert concerning the Department of Defense's cybersecurity acquisition processes and practices from the private sector's perspective. To that end, I have been asked to discuss the challenges and to provide some recommendations regarding what lessons can be learned from the SharkSeer program.

Our Nation's cybersecurity prowess is best measured as an integration of people, processes and technologies. Our ability to succeed in this critical mission area requires all three to function in unison across government and industry. I have been very fortunate to assist the Department's cyber operations for many years.

My military career began as a Signals Intelligence Voice Intercept Operator that grew into working in the cyber mission area since the late 1990s. After retiring from the US Army in 2002, I consulted in the private sector before returning to federal service in 2006 when I was assigned to develop and deploy government-off-the-shelf (GOTS) tools. Today, I support the DoD through my position as the Chief Technology Officer of Parsons Cybersecurity and Intelligence Division. My job, both in government and now at Parsons is the same, to develop system requirements into technology solutions that support operational needs. In both cases, I have been fortunate to lead a dynamic team charged with improving DoD cybersecurity capabilities through a constantly evolving mission delivery culture tuned to the ever-changing threat environment.

Time is a defender's worst enemy so in late 2011, I was challenged to create SharkSeer to help overcome this vulnerability. At the time, cyber protective systems relied primarily upon signature-based methods to detect malicious events. "Signature" detection required a defender to "know" or to have previously "seen" the malware to be isolated and inoculated – the technology was reactive and therefore provided an adversary operational leverage. SharkSeer enabled our systems to keep pace with any adversary's unique tradecraft. Today, we can detect and correct an adversary's constantly evolving malware attacks so that DOD's operations can continue uninterrupted. The same is needed for industry.

My mission was driven by General Keith Alexander. He defined my mission via a problem statement rather than through the normal source selection approach. The General enabled my team to explore capabilities if I remained focused on "solutioning" the problem. "Solutioning" meant the freedom to innovate by "failing fast." An 80% solution that could be evolved was better than a 100% solution someday in the future. Accelerated detection is at the heart of SharkSeer.

The innovation phase focused on discovering technologies that had the potential to keep pace with the evolving threat regardless of origin. I could investigate without the time-consuming request for information process. After several months of investigation, I selected capabilities to test in our laboratory environment. These capabilities ultimately became components of the SharkSeer mission system. The tools developed through collaboration between the DoD and the private sector delivered an evolvable integrated capability that kept pace with the threats. The federal government's willingness to allow incorporation of the jointly developed technology into their commercial products was key to industry participation and the program's ultimate success.

The Demonstration Phase provided valuable lessons. This phase had to answer the question, can SharkSeer perform as demonstrated in the laboratory? In this phase, the development team left the laboratory to test/demonstrate mission value to a field operator. A key success criterion was failing fast and adaptation to changing mission problems. Field test results convinced NSA, US Cyber Command, and Pentagon leadership, as well as the Armed Services and Intelligence Committees in both the House of Representatives and Senate to support the program. SharkSeer is now operational and performing as designed to protect against continuously evolving cyber-attacks.

From the "Innovate" phase to Full Operational Capability the program advanced at a rapid pace. All the people, processes, and technologies came together in less than four years. The SharkSeer program survived and became operational because (1) it "innovated" to fill a pressing need; (2) it "demonstrated" that it worked, which led operators to support it; and (3) it was rapidly deployed because of stakeholder involvement.

This program began at NSA; it was NSA's leadership that ultimately allowed it to succeed. It is now operational at every DoD Internet Access Point and every day it is detecting and eliminating a huge numbers of threats. Industry also benefits from its participation in the program as the threats are the same.

The many challenges faced during SharkSeer development, testing and deployment were accompanied by many successes realized during my time leading the program team. It was not easy nor smooth sailing. The DoD has many proud cultures for developing solutions to hard problems, but such an environment needs to be agile and evolvable so that innovative solutions can be employed. Adopting a culture of incorporating commercial capabilities is a dramatic shift from traditional methods and greatly expands the solution set from which both industry and government can select.

As may be expected, the federal government led the way in cyber for many years because technology in this critical field of expertise had a limited path towards commercial viability. Today however that equation has changed as America's industry is under attack. Thus, there is now a viable government and commercial need for collaborative solutions so that both may benefit. Where appropriate, SharkSeer can serve a model for a public private cybersecurity partnership that benefits both the national security and industrial communities.

You have my personal commitment and that of my company to the success of that partnership. Thank you for your support of this critical mission area. I look forward to answering your questions.