Testimony of Jeff England
Chief Financial Officer
Silver Star Communications

before the
Senate Committee on Commerce, Science and Transportation

"Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework"

February 4, 2015

Silver Star Communications, located in Freedom, WY, has been using the NIST Cyber Security Framework since it was originally released in draft form. Our initial intent was to review the framework and provide comment and feedback to NIST regarding its value to us as a rural telephone and Internet service provider. Our initial impressions were positive and some of our comments, including the incorporation of a gap analysis, were included in the official released version of the framework.

We have found that the framework has created an environment that encourages discussion, both internal and external, regarding its application in our organization. But above all, the greatest benefit from the framework has been the ability to use and adapt it within our organization such that it has become a meaningful management tool for improved cyber security practices.

The framework helped provide us with a disciplined approach to reviewing cyber security practices within our organization. In the course of completing a self assessment, there were many processes and procedures identified that we had not previously considered. The focus on current state relative to desired state in the context of acceptable risk provided meaningful focus and direction to IT staff and management. Additionally, since the framework allowed for organizational specific adaptation, we developed an internal reporting mechanism that provided executive visibility into our progress on highest priorities.

The voluntary nature of the framework has been the key to success for use within our organization.

We believe cyber security to be a competitive advantage whereby we differentiate ourselves from our competitors and make ourselves more attractive to our suppliers and those we serve. Because of this, we are self driven toward improvement and have begun sharing our cyber security practices with those we serve more openly. Curious as to whether or not our suppliers have used the framework, we began asking them to share with us their cyber security practices. These conversations have been extremely valuable in helping us identify customers and suppliers who share similar cyber security risk tolerances to our own and has become an important part of our vendor selection process.

We also believe that a regulatory mandate requiring the use of the framework creates a minimum standard environment. We believe this to be problematic because minimum standards are more likely to be treated as a checklist that can be delegated without having the necessary interdepartmental conversations regarding exposure and acceptable risk tolerance. There is also risk that minimum standards would put perpetrators on alert as to where they should focus their attentions for exploitation potentially placing organizations at additional cyber security risk than before.

Finally, we believe that a regulated approach to cyber security may, at least in part, misplace government attention away from the root problem. Cyber attackers are criminals and state sponsored cyber attacks are acts of war. Government action regarding cyber security should place primary emphasis on tracking down and bringing cyber criminals to justice.