Under the current model, the most prevalent way to deliver secure data is over the Internet through "Secure Public Websites" with user names and passwords. Some sites go further by using two-factor authentication, such as tokens with number codes that rotate on a timer. These token solutions are only a slight improvement over user name and password security systems. While they provide access to a group, they do not provide the ability to identify the individual gaining access. Any member of the group can gain access using another member's credentials, thus defeating the purpose of the system. Both of these methods also have the same weakness: browser-based, publicly available access methodology and reflect a larger problem with current cybersecurity infrastructure. Current solutions simply build upon underlying architectures that are outdated and overly-complex because of layers and layers of updates that are simply put on top of weak foundations. The Information and Internet Innovation Sector's (I3S) reliance on layering inherently places it at risk, as hackers are increasingly able to exploit these weaknesses. Instead, the government should undergo a paradigm shift in cybersecurity by researching potential uses of existing capabilities packaged in unique ways to improve security, reduce costs, and improve the efficiency of corrections once a breach is detected.

The inherent paradox in current data exchange on the Internet is that the private sector and government want to make their sites as available as possible to authorized users, yet this availability is the principle obstacle to properly securing data. To truly create a secure data exchange methodology to protect consumers, the nation must abandon the "welcome mat" approach of browser-based access and evolve to a virtual security application that is not available in a browser and that only exists during a user's session. Furthermore, the application must incorporate the tracking and reporting of logon activity and transmission of data by users to prevent anonymous action and foster an environment of absolute individual-level accountability. This type of model would create a true one-to-one relationship between cleared individuals and secure data.

This type of virtual software application could drastically improve the cost and efficiency of cybersecurity (and subsequent security corrections) in I3S systems as compared to current methodologies. The March cyber-attack against RSA Security, Inc. possibly compromised the legacy code used by their SecurID system, forcing them to replace one-third of all customers' deployed tokens. Not only has this cost $66 million in damages to date, but RSA has estimated replacing tokens will take roughly two months. Adding to this manufacturing bottleneck is the fact that all RSA tokens expire after three years and must be replaced. In comparison, research into virtual systems that do not require legacy code to operate could ensure any upgrades or patches would be deployed automatically upon access of the application. In the case of a security breach, a solution could be deployed efficiently, quickly, and at a far smaller cost.

In addition to new tools, Vir-Sec strongly believes that the government must consider new ways of looking at old problems - exploring innovative uses for current technologies to meet the modern threat environment. We further believe that research into virtual software applications will improve security for the I3S without sacrificing efficiency or increasing system complexity.