CYBER
SECUREAMERICA
COALITION

Companies focused on
cyber security and
public policy

Dear Sir or Madam:

RE: Report to the President on Federal IT Modernization

On behalf of the Cyber Secure America Coalition, thank you for the opportunity to provide public comment on the Report to the President on Federal IT Modernization. Transforming the federal government's IT infrastructure to a secure cloud based system where possible is a positive and important step to towards cost savings, greater efficiency and better security among federal IT systems. Secure IT systems are a critical building block to trusted interactions in government, with suppliers in the private sector, and with its citizens. We applaud the Administration's efforts in this important area. The Cyber Secure America Coalition (www.cybersecureamerica.com) is comprised of leading cyber security companies with a focus on helping governments, enterprises and consumers be more secure in their online interactions. We support the strong focus on cyber security in the Report to the President on IT Modernization.

We further believe that the Report's recommendation to move towards a risk based approach is correct and can help improve security in cases where resources are scarce and protection needs to be prioritized. Placing more security at the data level, including device authentication, and secure cloud back-up is a smart focus. We agree that emphasizing the use of encryption for data at rest and in motion is necessary and contributes to the notion of defense in depth. Providing more visibility throughout the network to security risks, through security logs at the application level, and enhanced information sharing provides tools to enable IT security professionals the ability to see potential risks and take actions to mitigate them.

Cloud Migration

Migration to the cloud, through the Cloud First initiative is a positive step and we support this effort. While moving to the cloud will improve efficiency, it is important that data security remains in the forefront. This means having enough trained cyber security professionals in government to monitor networks and manage overall security operations is crucial to the success of government IT modernization. The report discusses the idea of prioritizing low risk data first as a way to begin migration of data. We think this is a reasonable approach, we also believe that data and cloud centric solutions will be more secure. However, focusing on low risk data, should not prohibit the migration of broader amounts of government data and systems to the cloud. Security of more sensitive data can be achieved through appropriate data protection, encryption, and key management approaches already widely adopted in the private sector.

We further support efforts to improve situational awareness, and support improving information sharing efforts within the government but also with the critical infrastructure and private sector. This will help in ensuring accurate, timely and relevant data is available to ensure appropriate responses to threats. This is an important key to better security management.

Finally, we agree with the report's recommendation to bring cloud to the government rather than bringing government to the cloud. Commercial solutions exist, are secure and cost effective. This is a better more efficient approach to IT modernization.

Improving the Acquisition Process

As part of this modernization effort, it is also important to improve the acquisition process. The FedRAMP process continues to be a challenge especially for small to medium businesses trying to break into the federal marketplace. The current process hinders innovation and can restrict government access to the newest and most advanced IT solutions. Government must look to streamline the FedRAMP approval process and also the guidance to agencies. Currently commercial enterprises must commit significant resources, often millions of dollars to engage in the FedRAMP process; a huge burden for the small businesses which often create the most innovative technology solutions. The sheer number of controls as part of FedRAMP is daunting and requires a significant investment. In many cases this means a full-time employee dedicated to FedRAMP, which can is big investment for a small business. The predicated return on investment is often difficult to justify for these small firms. This barrier to entry means government loses and sometimes can not access the best and most innovative products. And when a small company does invest, they may be knocked out of specific acquisition opportunities to companies that have not gone through the FedRAMP process. We strongly encourage the Administration to look at ways to streamline the FedRAMP process and to look at ways to provide relief and assistance to small and medium enterprises as part of the acquisition process. This could include pilot programs, technical support from agencies, or innovation grants.

Email Security

A major component of migration to the cloud is moving to cloud based email security. We wholly support the Administration's efforts in this area of IT modernization. Moving to the cloud for email brings economies of scale, will improve efficiency and provide well documented security advantages. First we support the idea of shared services for cloud email services. We would recommend, however, that this is managed by GSA. They have experience in procurement and we believe the best place to create a marketplace for cloud based email services. GSA should be the place for approving solutions that can be made available for purchase, however, there should also be flexibility in the purchasing process offering choice from a range of solutions.

As mentioned earlier, while it is fine for agencies to take their time with cloud migration, government should not limit itself to low risk data. Sensitive and even classified data can be more secure in the cloud. There are many ways to ensure adequate protection of data. For example: encryption key management separated from the commercial cloud provider, enables further migration of sensitive data that stays within government control. This should be explored as an option for multiple levels of sensitive data.

Separately, government should look at modernizing email data protection to meet the collaboration and ease-of-use requirements of the modern agency. We support moving off of legacy encryption solutions like – S/MIME- that are not adaptable to modern technologies, like mobile and do not support government communications with a wide variety of private sector organizations or other constituents. They are not portable, slow up and break work flow, reducing efficiency and collaboration.

Handling Sensitive Data

Finally, we believe that as part of the Administration's IT modernization efforts, we would encourage that government look at harmonizing rules related to handling of ITAR and EAR data. Specifically, we agree with the Commerce department position that unclassified technical data should be allowed to be stored in Cloud services and shared electronically if it is encrypted "end-to-end" and that the encryption keys are stored and managed in the United States. The State Department is continuing to deliberate on its position, and bringing a consistent approach for handling of ITAR will unlock significant efficiencies in the defense industrial base and Department of Defense.

Conclusion

Thank you again for the opportunity to provide our thoughts on the Report to the President on Federal IT Modernization. We strongly support many of the key recommendations in this report, including moving to a secure cloud with a focus on protecting the data at all levels of sensitivity through the use of end-to-end encryption, access control and effective encryption key management. Improvements to the acquisition process, including support for small business and innovative technologies will further improve government IT services and it will improve security. We look forward to the final report and stand ready to work with the Administration to achieve its goals of modernizing the federal IT infrastructure.

Regards,

Phil Bond

Executive Director