APPENDIX B

Appendix B:

The following is an overview of the roles of various government agencies in relation to cybersecurity:

- The White House's Cybersecurity Coordinator – responsible for setting a national agenda and for coordinating Executive Branch cybersecurity activities.

- Director of the Office of Management and Budget (OMB) – responsible for overseeing federal agency information security policies and practices under the Federal Information Security Management Act of 2002.

- Department of Homeland Security (DHS) – serves as the focal point for security of cyberspace. DHS provides consolidated intrusion detection, incident analysis and cyber response capabilities to protect federal agencies' external access points, including access to the Internet. DHS has the lead in securing federal civilian systems and works with public and private stakeholders to protect CIKR.

- Department of Defense ("DOD") – defends military and national security systems.

- Federal Bureau of Investigation ("FBI") – tracks and prosecutes cyber crimes.

- United States Secret Service ("USSS") – tracks and prosecutes cyber crimes.

- National Science and Technology Council (Committee on Technology) – serves as the coordinating organization over the Network and Information technology Research and Development (NITRD) program. NITRD is the primary mechanism by which the U.S. coordinates its unclassified networking and IT research, and developing investments, which includes cybersecurity research and development.

- DOC – National Institute of Standards and Technology (NIST) – develops standards and guides for securing non-national security federal information systems. NIST identifies methods and metrics for assessing the effectiveness of security requirements, evaluates private sector security policies for potential federal use, and provides general cybersecurity technical support and assistance to the private sector and federal agencies. NIST is also a primary contributor to NITRD and is also responsible for the National Software Reference Library, National Vulnerability Database, and the Security Content Automation Protocol.

- DOC – NTIA – principle advisor to the President on telecommunications and information policies and works closely with other government entities on broadband deployment, securing the Internet namespace and other issues. The Internet Policy Task Force is reviewing Internet safety and recommendations for public policies and private sector norms to improve the cybersecurity posture of private sector infrastructure operators, software and service providers and users of CIKR and their customers. [1]

[1] *See* NOI at 44217-44218.