Responses to Written Questions Submitted by Honorable Jerry Moran to Donna Dodson

Question 1. Your testimony described the utility of the National Vulnerability Database (NVD), which is administered by NIST as a repository of reported vulnerabilities found in different types of systems. According to a report produced by the cyber security firm Recorded Future, DHS's US Computer Emergency Readiness Team (US-CERT) takes up to 33 days on average after the public disclosure of a software vulnerability to complete the cataloguing process and create a new entry in the database, while China's version takes on average 13 days. Are you able to describe what procedural differences might account for this longer process?

Response. That report is not entirely correct. New vulnerabilities are posted to the National Vulnerabilities Database (NVD) as soon as the National Institute of Standards and Technology (NIST) receives them. NIST subsequently updates the entries with severity metrics, the complete range of affected platforms, remediation recommendations, and links the information to vendor alerts. Both the number of vulnerabilities in the NVD and use of the NVD continues to grow. Since January 2017, each month we have seen an average of 10 percent growth in the amount of data downloaded from the NVD. NIST is working aggressively to ensure that it can continue to provide this important information in a timely fashion.

Question 2. Your testimony also mentioned the expanded areas of focus like the Internet of Things that the database is expected to cover. How will the wider range of technologies included impact NIST's efforts to maintain the database, especially as database use continues to grow?

Response. With more and more products connecting to the Internet, NIST expects the number of entries into the NVD to continue to increase. Part of our strategic planning is to ensure the continued usefulness of the NVD data by extending our ability to receive, assign metrics, and publish information that covers these new technologies. Our plans include using machine learning, natural language processing, and artificial language technologies; leveraging vendor self-scoring capabilities that are NIST verified; training and hiring new vulnerability analysts; and extending the used standards to cover new technologies. We are projecting our future needs for maintaining the NVD based on, not only a historical view, but the projected growth of technologies like the Internet of Things.

Question 3. As it relates to identifying cybersecurity vulnerabilities within our federal agencies, modernizing the federal government's IT systems needs to remain a top-priority. According to the GAO's High Risk Series report, the federal government annually spends over $80 billion on information technology (IT), but more than 75 percent of this spending is for "legacy IT." The Modernizing Government Technology (MGT) Act was signed into law last year in an effort to bolster agencies' capabilities to defend themselves from cyber threats at home and abroad by replacing outdated and vulnerable systems. Could you please describe the threat that "legacy IT" specifically poses to federal agencies' cyber infrastructure?

Response. Legacy information technology poses risks to an organization's infrastructure for several reasons. Often legacy software and hardware are more susceptible to malware. Sometimes there are no patches, updates or technical support for legacy software and hardware for remediation when a vulnerability is discovered. NIST continues to provide guidance to agencies managing risk across their organization to assist with the challenges of "legacy IT" while encouraging organizations to update software and hardware and maintain a rigorous program to patch these products.

Question 4. My subcommittee has held hearings on private and public sectors' use of "bug bounty programs" to incentivize the expertise of outside cybersecurity researchers to identify cyber vulnerabilities in a timely fashion. Can these types of arrangements be used to in supply chain cybersecurity disclosures? If not, why?

Response. Yes, bug bounty programs may provide an additional and valuable capability for organizations to identify vulnerabilities in their supply chains. However, these types of programs frequently require organizational, technical, and legal infrastructures, as well as a skilled and knowledgeable workforce, to help them achieve the desired outcome in a manner that protects the organization. NIST generally encourages research into tools and processes that support greater visibility and understanding of cyber supply chain risks. NIST also encourages organizations to share incident handling activities related to supply chain incidents with supply chain partners.

Question 5. Your testimony covered the stakeholder engagement following the development of the Cybersecurity Framework. As outside comments and feedback from workshops continue to shape the Framework (including the expansion to supply chain guidance), what do you see as the next step to effectively promoting coordinated vulnerability disclosure among private and public stakeholders?

Response. With subject matter such as supply chain risk management (SCRM) and coordinated vulnerability disclosure (CVD) incorporated into the Cybersecurity Framework, NIST will advocate of the adoption of the Cybersecurity Framework both nationally and internationally which will help increase awareness and understanding of CVD. This awareness and understanding will naturally help organizations implement more detailed guidance such as NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations. Further, basic dialogues about CVD can be enriched through International Organization for Standardization (ISO) and Forum of Incident Response and Security Teams (FIRST) guidance.

Question 6. As NIST's Supply Chain Risk Management Program continues to work with private and public stakeholders to identify best practices and standards related to the supply chain ecosystem, could you please describe how interoperability of technologies is accounted for in these considerations? Are you able to give specific supply chain examples where interoperability has a pronounced role?

Response. An interoperable supply chain platform (automated digital processes that help buyers and suppliers integrate and optimize their order and delivery processes) is essential to most organizations' supply chain infrastructure. Since supply chain platforms are often a system-of-systems that involve order management, returns management, sourcing, finance, inventory visibility, transportation management, and warehouse management—all of which may involve various physical and digital technologies—it is necessary that each of these sub-systems interoperates for an organization's supply chain infrastructure to function seamlessly. NIST has case studies available that discuss supply chain platforms and interoperability, for example, NIST's case studies on Exostar and Smart Manufacturing are available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/Best-Practices.