Responses to Written Questions Submitted by Honorable Jerry Moran to Joyce Kim

Question. 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. In short, yes. As you correctly point out, bug bounty programs serve a valuable purpose in that they incentivize researchers to identify and responsibly notify affected companies of potential vulnerabilities in products so the companies can address the problem. Often the existence of a bug being brought to a company by a researcher, either through a bug bounty program or not, begins the process of assessing the vulnerability, developing any necessary mitigation, distributing the mitigation, and ultimately making a public disclosure about the vulnerability. Thank you for your work on, and support of, bug bounty programs as they contribute to responsible cybersecurity practices.