Responses to Written Questions Submitted by Honorable Jerry Moran to Art Manion

Question 1. 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. Although they are closely related, vulnerability disclosure programs are a necessary prerequisite to bug bounties. A bug bounty adds financial incentives to a vulnerability disclosure program. Bug bounties can be useful to focus researcher attention on finding vulnerabilities at an optimal point in the development lifecycle (for example, Microsoft has used bug bounties to motivate vulnerability reports during the beta phase for new versions of software rather than waiting for post-release reports to trickle in). Bounties can also be used to focus attention on specific software products or components, such as the Department of Defense Vulnerability Disclosure Program scoped to cover internet-facing DoD web sites. But a bug bounty alone will not lead to addressing of vulnerabilities unless it is backed by a well-functioning coordinated vulnerability disclosure program that includes deploying fixed software.

A bug bounty could be used to discover vulnerabilities in supply chain components like common libraries or protocols; however, the complexity arises in the resulting coordinated disclosure process, not the bounty program itself. A bounty program aimed at supply chain components may need to consider longer embargos and the question of who owns the program and pays the bounty. Open source projects that create many supply chain components often cannot afford to operate or pay for bounty programs.

Question 2. 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in an effort to bolster agencies' capabilities to defend themselves from cyber threats at home and abroad by replacing outdated and vulnerable systems.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. In general, older systems and software are less likely to receive security updates, and creating and obtaining updates or otherwise defending these systems is more costly. In the case of some long-lived devices, including industrial control systems, hardware can long outlive the software running on it. To mitigate the issue we can:

Identify and assign ownership of legacy systems so that we do not have "orphaned assets" that add to our risk exposure. Some very significant and successful attacks have occurred because a piece of legacy IT was not properly managed and remained unpatched. Regular scanning should be done from both inside and outside of networks to ensure that all assets are properly identified.

Once assets are identified, proper management will include dispositioning the risks that the legacy IT poses to the enterprise. In some cases isolation and access control will help to quarantine the risks of the legacy IT. Ensure that those devices and capabilities are not directly accessible from the internet. In cases where this is not possible, system hardening and monitoring are ways to disable unnecessary services (such as the SMB Protocol) that can pose risks.

Finally, investment in upgrading critical services and assets that are living on legacy IT must be made. There are some activities that are so significant and critical to organizations that they may need to eliminate the risk of legacy IT use.

Question 3. As one of a many industry standards for addressing coordinated disclosures, the CERT Coordination Center's guidance suggests that a third-party coordinator may relay or broker information between stakeholders for complicated coordinated vulnerability disclosure (CVD) cases. Could you please describe why this approach may be preferable and in what circumstances?

Response. Coordinating organizations like the CERT/CC and DHS NCCIC can provide the following capabilities for complex CVD cases:

Understanding the problem — Some vulnerabilities are technically complicated and require a nuanced understanding in order to completely remediate them. Coordinators have access to technical analysts who can provide an objective assessment of the severity and impact of a vulnerability or help to refine the vendors' understanding of the scope of the problem. This can work in both directions: increasing the scope for vulnerabilities that appeared to be simple but turn out to be more complex, or reducing concern for vulnerabilities that initially appeared to be severe but pose less risk once they are better understood.

Coordinating creation of solutions — Researchers and vendors may not know whom to contact in regards to widespread vulnerabilities that affect more than just the products they are aware of. Coordinators maintain contacts across a wide swath of vendors. As neutral third parties, coordinators are also unconstrained by concerns about competitive advantage when vulnerabilities affect competing vendors. Furthermore, a message from a coordinator to a vendor security team can carry more weight than a random report received through the help desk, and sometimes this additional leverage is what is needed to induce vendors to act.

Amplifying public notifications — Public messaging by coordinators usually gets the attention of system deployers as well, which can help to amplify the vendors' attempts to reach their users.