Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

October 15, 2024
Contact: Nathan Miller
nathan.miller1@maryland.gov
443-346-3972

State of Maryland Launches Widest-Reaching State-Level Bug Bounty Program in the U.S.

Crownsville, MD:

Today, the Maryland Department of Information Technology (DoIT) is announcing the results of the State's first bug bounty program, the widest-reaching State-level program of its kind in the United States.

Maryland's first bug bounty program launched as a focused assessment of 12 key State web assets. After a successful initial phase, DoIT expanded the program to include all public-facing web assets on *.maryland.gov, *.md.gov, and *.state.md.us. More than 40 exploitable vulnerabilities were identified. Only the federal government has publicly known bug-bounty programs with such a wide scope.

This initiative enhances the security of the state's critical IT systems and information by using trusted security researchers to test publicly-facing web assets. These tests allowed the State to identify and remediate critical vulnerabilities, safeguarding valuable private information and systems. Security researchers, vetted by the State and HackerOne, identified vulnerabilities in publicly-facing websites and applications.

This partnership with the security research sector allowed the State to identify and remediate cybersecurity vulnerabilities before threat actors could exploit them. This initial program has established a strong relationship that will enable DoIT to orchestrate future bug bounties and other cybersecurity vulnerability programs.

Bug bounty programs reward and financially compensate researchers based on the vulnerabilities they discover. The Maryland bug bounty program is modeled after a similar program conducted by the Department of Defense (DoD) to identify vulnerabilities in federal defense systems. DoIT Secretary Katie Savage previously led the Defense Digital Service within the DoD, where she and her team ran "Hack the Pentagon" and facilitated multiple bug bounty programs.

"Bug bounty programs have completely changed how the federal government identifies and remediates cybersecurity vulnerabilities," says Savage. "By implementing the widest state-level bug bounty program in our nation, the State of Maryland will identify vulnerabilities more quickly,

establish strong, long-term ties with the security researcher community, and keep our state secure."

Bug bounty programs and security researchers have become standard at the federal level, with the Cybersecurity and Infrastructure Security Agency (CISA) encouraging federal agencies to adopt the approach. By implementing federal-level cybersecurity standards into its playbook, Maryland is leveraging federal best practices and demonstrating its desire and ability to keep residents safe.

Bug bounty programs can be more effective than traditional testing programs in several ways. The Maryland bug bounty program helps the State identify more vulnerabilities more quickly, establish relationships with the broader security research community, and more efficiently use taxpayer dollars. Cybersecurity breaches are expensive to remediate, expose critical state data, and jeopardize the safety of state systems, services, and infrastructure.

Gregory Rogers is the State's Chief Information Security Officer (SCISO) and leads the Office of Security Management (OSM) within DoIT. In coordination with Governor Moore and the State legislature, Rogers develops and oversees a State-wide cybersecurity strategy and information security program focusing on cyber maturity and risk management. Rogers' team in OSM facilitated the bug bounty program; they continue implementing cutting-edge strategies and technologies to keep Maryland secure.

"The Office of Security Management is taking advantage of the latest strategies, innovations, and policy frameworks to achieve whole-of-State cybersecurity and protect against threat actors," says Rogers. "By strengthening our ties with our nation's thriving security researcher community, we are building a secure State that can protect itself and its constituents, now and in the future."