bugcrowd

CASE STUDY

How the State of Maryland built a researcher-first VDP

Maryland

Industry:
Government

Headquarters:
Crownsville, MD

Website:
doit.maryland.gov

Key takeaways

554 vulnerabilities surfaced

100% actionable results

The situation

Maryland's Department of Information Technology (DoIT) carries a big mandate: enabling coordinated vulnerability reporting and security engagement across all state, local, tribal, and territorial government entities. Their IT footprint is vast, as new systems, agencies, and attack surfaces are regularly added.

Maryland had previously run Hack the State 1.0, a short, time-bound private bug bounty that gave leadership an early look at the findings a motivated researcher community can surface. A number of DoIT security leaders came from the federal space, where vulnerability disclosure programs (VDPs) and crowdsourced security are more readily embraced. This created early internal momentum that most state and local governments don't have. Nevertheless, DoIT needed to bring in the expertise and resources needed to build a lasting program.

When Steve Kain joined DoIT as Director of Adversary Emulation, standing up a formal VDP quickly became one of his founding priorities.

The challenge

Maryland's IT footprint is large and constantly evolving, and the team needed additional visibility into vulnerabilities across its attack surface. The solution—continuous offensive security testing—was clear in principle but less so in practice. State and local governments face a different set of constraints than their federal counterparts when it comes to preemptive security, including tighter budgets, leaner teams, and less institutional precedent for programs like VDPs.

"There's a fear of, 'What happens when we do this? What happens when we find out?'" says Kain. "But ignorance isn't bliss. You want to know where the problems are. The real fear is, 'If I do this, what am I going to learn, and how am I going to fix it with limited resources?' We've all been told since day one to do more with less."

For Kain, the answer is straightforward math. "The time and effort you have to put into incident response when finding something the hard way, versus finding it the easy way. The math just doesn't math," he says. "If you have something vulnerable on the internet, a criminal will find it. And then you're going to have to deal with the impact."

This reasoning led Kain and the team to lay the groundwork for building a VDP. First, they did their homework by talking to peers in other states (like California, which runs one of the country's largest state VDPs through Bugcrowd), studying private-sector programs (like T-Mobile), and drawing on public resources like CISA's Binding Operational Directive 20-01 and disclose.io. This helped them understand what worked and what didn't. As Kain puts it, "Look at what everybody else is doing, whether public or private. Emulate what you really like, and refine the rest."

> **The groundwork paid off, helping them secure leadership alignment. The final step was ensuring that the program would be legally sound and durable.**

That meant close coordination with Maryland's Attorney General's office to establish safe harbor provisions and rules of engagement and researching the Code of Maryland Regulations (COMAR) to confirm the state CISO's authority to run a wide-scope program.

> There's a fear of, 'What happens when we do this? What happens when we find out?"' says Kain. "But ignorance isn't bliss. You want to know where the problems are.
>
> **Steve Kain, Director of Adversary Emulation, Maryland DoIT**

> Having Bugcrowd's Platform and team behind us meant we could focus on building the right program for Maryland. The infrastructure and expertise were already there
>
> **Steve Kain, Director of Adversary Emulation, Maryland DoIT**

The Bugcrowd solution

In 2025, Maryland launched its VDP on the Bugcrowd Platform. Getting the program live required close collaboration between DoIT, Maryland's legal team, and Bugcrowd, aligning the state's program page with Bugcrowd's platform materials to ensure a seamless, consistent experience for researchers from day one.

Building a researcher-first program was especially important for DoIT because the stakes of probing state systems without clear cover are uniquely high for researchers.

Their efforts resulted in clear safe harbor language, well-defined rules of engagement, and a commitment to responsive, genuine communication.

"Having Bugcrowd's Platform and team behind us meant we could focus on building the right program for Maryland. The infrastructure and expertise were already there," says Kain.

This researcher-first approach paid dividends when Maryland expanded its program to include a live bug bounty event, bringing 11 world-class researchers together for two days of focused testing against constituent-facing services. As one of the first state governments to host live bug bounty events, Maryland had no problem recruiting researchers because of the trust it had built with the research community through the VDP program. Researchers saw that the State of Maryland was collaborative and valued them, which increased their interest in participating. The event itself was a huge success—by day two, researchers who had arrived independently were working together, combining specialized skills in ways traditional testing cannot replicate.

The outcome

Since launching, Maryland's VDP has surfaced 554 vulnerabilities at the time of publishing this.

> **What matters as much as the volume is what Maryland actually does with it. "Every single result is 100% actionable," says Kain.**

"Bugcrowd isn't going to hand you a false positive after triage. You cannot get that out of another product or service." Kain notes that this is particularly valuable in the age of AI-generated submissions, which flood programs with noise.

The diversity of the researcher community has also helped surface findings that a traditional test (such as a regular penetration test) would be unlikely to uncover. Where a traditional engagement might use the same testers, the same techniques, and the same blind spots year after year, VDPs draw specialists and generalists alike. With each bringing a distinct lens, this means Maryland's attack surface is constantly checked for hidden vulnerabilities. The result is a steady stream of vulnerabilities that would otherwise have gone undetected until a less welcome party found them first.

An unexpected benefit has been the program's reach into the next generation of security talent. Kain has used the VDP as a platform to engage local universities, speaking to students about real-world security research. A group of University of Maryland students who contributed to the program has since participated in Capture the Flag (CTF) competitions and other VDPs across the industry.

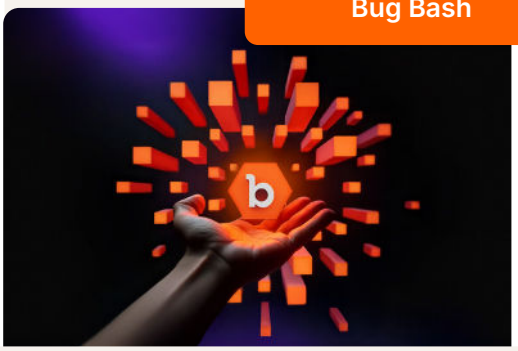
"There's a big jump between participating in CTFs and taking a class in a very controlled environment, and then venturing out into the real world," says Kain. "A VDP is that perfect gateway. You find a program, you're not under a contract, and you're not under pressure. It's a great place to begin a professional career and start building a resume."

But the VDP isn't the be-all, end-all—Kain wants to eventually grow the program by continuing bug bounty engagements and build an in-house offensive security group. His ambitions stretch beyond Maryland's own security posture. He wants to use the program as a springboard to deepen relationships with local colleges, reach underrepresented communities, and get more people involved in cybersecurity. "This is just the beginning," he says. "My intent is to just keep building up the relationship with the security community, and it would be a phenomenal honor if other states would want to steal our program or copy it."

Products involved

Vulnerability Disclosure Programs

Bug Bash



Success snapshot

- ✓ 554 vulnerabilities surfaced to date
- ✓ 11 world-class researchers at Maryland's first live bug bounty event