bugcrowd

DATA SHEET

Bugcrowd in the Public Sector

FedRAMP-authorized offensive security testing

FedRAMP™

Challenges

Every public sector organization, from local utilities to federal agencies, is under constant threat of attack at every level of sophistication, including Advanced Persistent Threats from state-sponsored actors. For these regulated organizations (and increasingly, for critical infrastructure providers and government contractors), meeting the highest standards for security means going beyond the traditional solutions.

Solutions

The FedRAMP Moderate Authorized Bugcrowd Platform helps public sector customers defend themselves against cybersecurity attacks by connecting with trusted, skilled security researchers to take back control of the attack surface. The public sector can benefit from a wide variety of Bugcrowd's solutions, including:

- **Managed Bug Bounty**
- **Vulnerability Disclosure Programs (VDPs)**
- **AI Safety and Security Assessments**
- **Penetration Testing as a Service**
- **Red Teaming as a Service**
- **Continuous API, code, and SBOM testing**

Examples of our Work in the Public Sector

- CISA VDP and Bug Bounty Program
- AI Bias Bounty Program and Rapid Response Program for CDAO
- Department of Homeland Security (Hack DHS) Bug Bounty Program
- State of Maryland and State of California VDP
- Centers for Medicare and Medicaid Services (CMS) Bug Bounty Program

Contract Vehicles for Procurement

- NASA-SEWP
- Hack DHS IDIQ
- GSA via Carahsoft
- Tradewinds AI Marketplace

> **NASA works with security researchers to protect our infrastructures and our greater mission to advance space exploration. Security researchers help us by pointing out vulnerabilities that may not have yet been identified, contributing to an improved security posture.**
>
> **Leslie Cahoon,** NASA

Public Sector Use Cases

Binding Operational Directive 20-01

VDPs are a federal mandate for Federal Civilian Executive Branch (FCEB) agencies. CISA has partnered with Bugcrowd and EnDyna to provide a VDP-as-a-service free-of-charge.

AI Safety and Security

Executive Order 14179 mandates the safe and secure development and use of AI. AI Assessments and AI Pen Tests take steps to identify and prioritize vulnerabilities and data bias flaws in LLM applications.

DoDI 8531.01 Compliance

DoDI 8531.01 requires all Department of Defense (DoD) agencies to have a VDP to help confront a landscape where asymmetric threats are the norm. By using a VDP and Managed Bug Bounty, the DoD can significantly extend their reach, tapping into a wealth of knowledge.

Workforce Development

We partner with universities to provide students with real-world training in web application security, LLM safety, and hardware hacking. By fostering a new generation of security researchers, Bugcrowd ensures that public sector organizations have access to a talent pool ready to defend against evolving national security threats.

Election Security

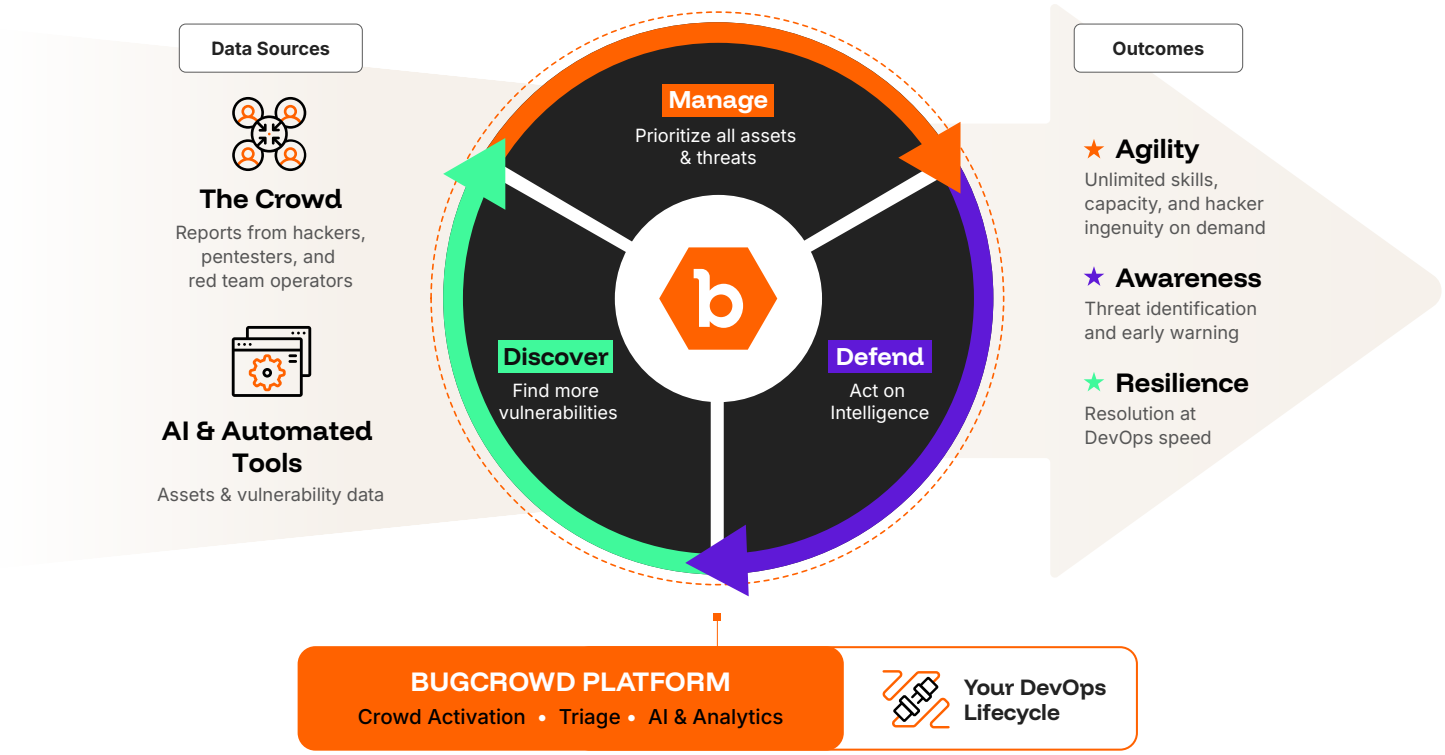
Fears that U.S. election integrity is at risk for compromise are widespread. By leveraging a VDP for digital assets and a Managed Bug Bounty engagement for hardware assets, election technology providers can ensure election security and integrity.

Fuzzing and Dynamic Code Analysis

Industry-leading technology that fulfills requirements for fuzzing and dynamic code analysis—like SA-11(5) and SA-11(8)—prior to fielding new systems, such as sensors, C2/C4I platforms, weapons systems, unmanned aircrafts, and autonomous vehicles.

> **We have found our engagement with Bugcrowd to be valuable. We have received useful submissions that we would never have found with our automated scanning tools. It has been a great addition to our overall security toolkit.**
>
> **Dan Auger,** Office of the Minnesota Secretary of State

Bugcrowd Platform



The Bugcrowd Platform fuses AI with real-time, crowdsourced intelligence from the world's top ethical hackers, pentesters, and red teamers (aka The Crowd), as well as from automated tools that generate asset, threat, and vulnerability data. The powerful combination of human creativity and automation empowers you to continuously:

Agility

Augment Your Team On Demand

- Attacker mindset on tap for vulnerability discovery, pen testing, and red teaming
- 350+ skill sets and certifications available
- Crowd curation and activation guided by data and AI

Awareness

See and Prioritize Emerging Threats

- Continuous vulnerability intake, validation, and triage at scale
- 24/7 triage coverage with same-day response for P1s
- Early warning of emerging vulnerabilities

Resilience

Continuously Improve Security Posture

- Actionable reporting, benchmarking, and recommendations
- Directly integrates with existing tools for change at DevOps speed
- Deep bench of solution & support specialists at your side for quick wins and long-term ROI