

The Hack the Pentagon Bug Bounty Playbook

October 2022

The information below will position you to understand the program, the process, and provide you with the necessary forms to execute a successful Bug Bounty.

Beginning To End In Detail

After the acquisition process results in an award to a vendor to manage the researchers, the typical DDS Bug Bounty process follows a three phase, 4 week x 4 week x 4 week, readiness, on target, and wrap up sequence.

Phase 0: Documentation and set-up

- Send required forms to WHS/Funding Party (forms available for download further down the page)
- Forms include Technical Scoping Document, PWS, & IGCE
- Forms to be completed by COR and sent to WHS/Funding Party
- Forms include Non-Personal Services Certificate, Section 508 Form, QASP, Inherently Govt. Functions Certificate Form
- RFP and vendor selection/award

Phase 1: Bug Bounty prep (readiness) - 4 weeks

- Kickoff call with vendor, CDAO/DDS, & asset owner
- Obtain rules of engagement from vendor
- Technical scoping document adjustments
- Backend coordination (tech leads across all parties ensure connectivity of systems)
- Select a bounty launch date
- Training on vendor portal for asset owner

Phase 2: Launch/start the bug bounty (on target) - 4 weeks

- Monitoring vulnerability reports
- Monitoring bounty pool (\$\$\$)
- Communicating with vendor & asset owner
- Remediation of reports by asset owner

Phase 3: Post-Mordem, review metrics, out-briefs, & final remediation (wrap up sequence) - 4 weeks

- Review of metrics
- Internal presentation: CDAO/DDS, vendor, asset owner
- Executive presentation: Greater DoD leadership (if necessary)

Bug Bounty Complete!