Tech Policy Primer

Ahmed Amer
Di Cooke
Rob Lever
Julia Pan

To learn more about this project, please visit **aspentechpolicyhub.org.**

# Agency Readiness for Bug-Bounty Programs

## A toolkit for enhancing agency preparedness for bug bounty program execution

## BACKGROUND

*As part of their 10-week policy training, the scholars of the Tech Policy Primer program spent 6 weeks working on public sector challenges. In teams of 4-5, the leaders either proposed their own projects or worked with a real-world government client on a public sector problem. Below is an overview of one team's project to help the Cybersecurity and Infrastructure Security Agency (CISA) scale the use of bug bounty programs across government.*

## EXECUTIVE SUMMARY

To expand the use of bug bounty programs (BBPs) across government, the Cybersecurity and Infrastructure Security Agency (CISA) should help agencies: improve their understanding of BBPs; gauge their specific agency's readiness to execute a BBP; and assist with preparation if an agency is not yet ready to execute a BBP. To accomplish this, CISA should educate agencies on BBPs and their benefits via an information sheet; provide agencies with a BBP readiness scorecard and survey to assess their levels of BBP readiness; and give written guidance on how agencies can become more prepared.

## PROBLEM BACKGROUND

BBPs are an efficient and cost-effective way to improve a system's security, allowing for scrutiny by a broader array of cybersecurity experts than a typical agency could normally provide. Yet few agency system stakeholders (including system owners) understand the advantages of BBPs or are prepared to execute BBPs on their own systems.

## RECOMENDATION

CISA should support agencies in assessing and improving their BBP readiness, and should educate agencies on the benefits of such programs. More specifically, CISA should:

- **Circulate an informational document on BBPs.** This high-level informational document would inform agency stakeholders of the benefits of BBPs and share past examples of successful BBPs such as Hack the Pentagon and Hack the DHS. At present, most agency system stakeholders are unaware of BBPs. Those who are familiar worry about BBPs making their systems susceptible to malicious hackers during the program's execution. An information document would be a low-cost way for CISA to address these concerns.

- **Develop and provide agencies with a BPP Readiness Scorecard and Survey.** Many agencies currently do not have the knowledge or processes in place to assess their own readiness to execute a BPP. To address these issues, CISA should provide a Readiness Scorecard, accompanied by a Readiness Survey customized for federal agencies. These resources should include specific recommendations for next steps and resources agencies should pursue based on their Scorecard results.

*For more information about this proposal, please see: (1) the BBP informational document, which aims to provide federal agency stakeholders with information about BBPs; (2) a BBP readiness score guide that shares detail on how to use the survey tool and interpret results, and includes a sample BBP readiness scorecard; and (3) a demo video of the sample BBP survey tool.*

Tech Policy
Primer

### ABOUT THE TECH POLICY PRIMER

This project was completed as part of the Aspen Tech Policy Hub's Tech Policy Primer program, a 10-week, part-time program that trains science and technology experts on the policy process. Learn more at **aspentechpolicyhub.org/primer**.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

aspen institute