VDP ACTION PLAN FOR GOVERNMENT AGENCIES

Vulnerability disclosure policies, or VDPs, have become a best practice for organizations and government agencies worldwide. However, some organizations have yet to open their door to security researchers who are interested in submitting vulnerabilities.

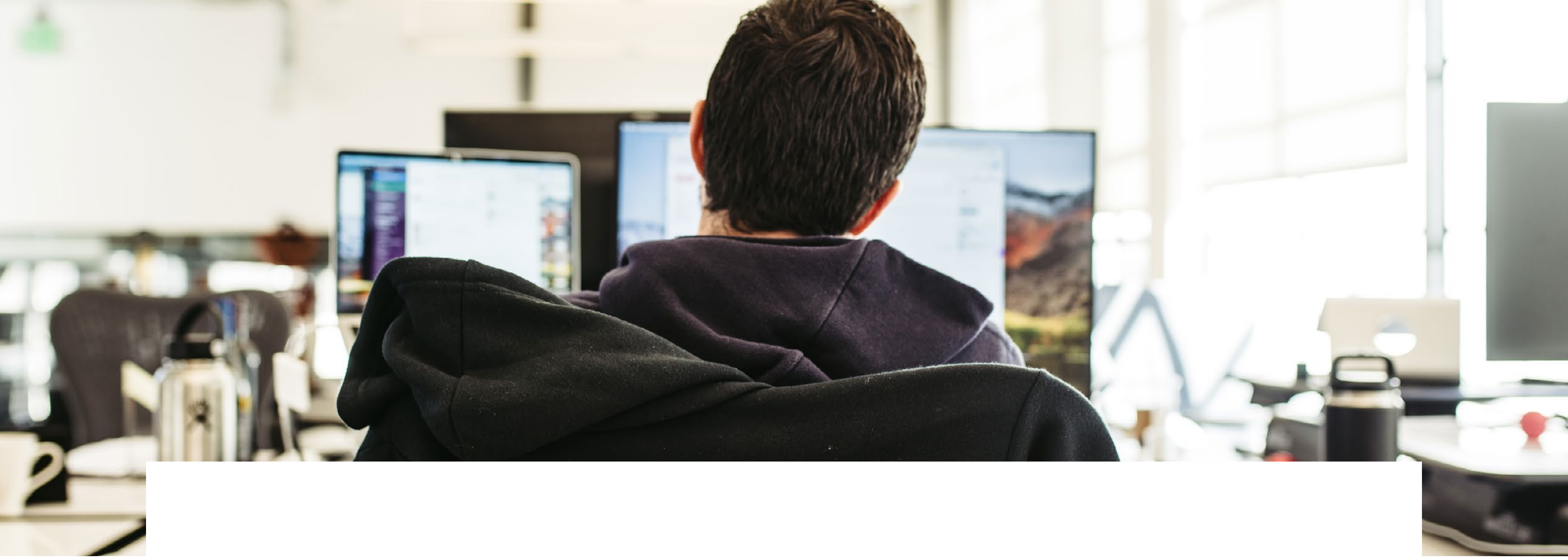
Federal agencies are uniquely vulnerable to cyber threats. Water and sewage systems, public transportation, driver's licensing, libraries, and schools all handle sensitive information that's attractive to bad actors. Regardless of the threat, federal agencies do not have a budget or staff proportionate to their needs. And with decreased visibility and control over their expanding network, agencies' overburdened IT teams are likely to experience compliance challenges.

To mitigate risk, establishing a VDP is the best starting point. Here's a quick action plan that can help you lay the foundation for a VDP and level up your agency's security strategy.

1. **Get buy-in.**
   Setting up a VDP is a cross-functional endeavor. Make sure you loop in all necessary stakeholders before you get started. To start, speak with your partners on the legal team, communications, and IT.

2. **Draft your brand promise.**
   The opening section of your VDP is known as the "brand promise". The DoD's brand promise reads: "The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and DoD recognizes that fostering a close relationship with the community will help improve our own security." Your brand promise should explain your agency's commitment to security and invite security researchers to submit vulnerabilities.

3. **Identify the scope.**
   Figure out what properties, products, and vulnerability types are covered. Most federal agencies are in the middle of a digital transformation, grappling with more devices, apps, software licenses, and cloud storage solutions than ever before. It's important to nail down exactly which elements are fair game for a security researcher.



4. **Promise your reporters safe harbor.**
   Your VDP must include language that assures security researchers that they will not be legally penalized for identifying vulnerabilities.

5. **Establish a process.**
   Drafting your VDP is only the beginning. You'll need to create a process for triage and remediation: assessing, prioritizing, mitigating, and addressing incoming vulnerability reports. If mismanaged, publishing your VDP will result in an onslaught of reports for which you're unprepared, an overwhelmed internal team, and disgruntled security researchers—severely compromising your security strategy.

   But if properly managed, you can use your VDP to start building out a mature security strategy. Federal agencies like the Department of Defense, the Air Force, and federal civilian agencies like GSA's Technology Transformation Service have partnered with HackerOne to take control of vulnerability disclosure and coordination. These agencies benefit from HackerOne's community of researchers and robust technology to streamline the process from start to finish.

For more information on leveling up your agency's security strategy, check out https://www.hackerone.com/resources/government

Contact us at
www.hackerone.com/contact
sales@hackerone.com
+1 (415) 891-0777