



MY SHORTCUTS:



CYBERSECURITY

CALENDAR DATAPOINT DIRECTORY DOCUMENTS LEGISLATION

POLITICO Pro has a new look and feel! Preview the new experience featuring a personalized feed, recommended content, and more. **Check out the new site here!**



CYBERSECURITY WHITEBOARD

All government agencies should consider CVD programs, urges industry coalition

By ERIC GELLER

Federal, state and local governments must commit to coordinated vulnerability disclosure programs to send the message that they are essential components of any organization's security posture, according to the Cybersecurity Coalition.

"Government agencies, at all levels, should be required to adopt an internal CVD program based on existing standards," the coalition said in a paper released today. "Policymakers should ensure agencies have dedicated capacity, funding, and resources necessary to receive and analyze disclosures, mitigate vulnerabilities, and manage communications with stakeholders."

The paper also recommended enhanced government support for vulnerability databases, the promulgation of international norms around CVD structure and the incorporation of CVD into federal agencies' "best practices" documents.

All organizations must recognize that their technology has bugs and that people will occasionally report them, the Cybersecurity Coalition argued. "Organizations may or may not authorize or incentivize independent security testing," the paper said, "but all organizations should be prepared to receive unsolicited vulnerability reports."

When that happens, the paper also said, "organizations should consider refraining from taking legal action or retribution against security researchers or other vulnerability finders or reporters that follow established CVD policies and procedures."

The Cybersecurity Coalition released its CVD "policy priorities" paper during a panel today at the RSA Conference in San Francisco.

"As private enterprises and government agencies worldwide are simultaneously deploying lots of technology while grappling with cybersecurity risk management, and as vulnerability discovery tools continue to evolve," it said, "now is the time to make standards-based CVD a routine and robust function."

Mar 6, 2019 1:31 PM EST[Terms of Service](#)[Privacy Policy](#)[About Us](#)[Corrections](#)[Support](#)

