9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

Cybersecurity and Infrastructure Security Agency

Availability of Draft Binding Operational Directive 20-01.

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS.

ACTION: Notice of availability; request for comments.

SUMMARY: Through this notice, CISA is making available a draft binding operational directive that will apply to all Federal, executive branch departments and agencies relating to vulnerability disclosure policies. The draft binding operational directive proposes requiring agencies to develop and publish a vulnerability disclosure policy (VDP) and maintain supporting handling procedures. This notice also requests comment on the draft binding operational directive.

DATES: Comments are due by December 27, 2019.

ADDRESSES: You may send comments by any of the following methods:

- Agency Website: For instructions on how to provide comments, please follow the instructions provided at https://cyber.dhs.gov/bod/20-01/.

- Email: BOD.Feedback@cisa.dhs.gov. Include "Draft Binding Operational Directive 20-01" in the subject line of the email.

Instructions: The full text of the draft Binding Operational Directive 20-01 is available at https://cyber.dhs.gov./bod/20-01/. Do not submit comments that include trade secrets, confidential commercial or financial information, Chemical-terrorism Vulnerability Information (CVI), Protected Critical Infrastructure Information (PCII), or Sensitive Security Information (SSI). All written comments received will be posted without alteration at https://github.com/, including any personal information. Contact information submitted through email will not be posted to https://github.com/, except for any name and affiliation included in the comment.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security ("DHS" or "the Department") has the statutory responsibility, in consultation with the Office of Management and Budget, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections. 44 U.S.C. 3553(b). As part of that responsibility, the Department is authorized to "develop[] and oversee[] the implementation

of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director [of the Office of Management and Budget] and [certain] requirements of [the Federal Information Security Modernization Act of 2014.]" 44 U.S.C. 3553(b)(2). A binding operational directive ("BOD") is "a compulsory direction to an agency that (A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; [and] (B) [is] in accordance with policies, principles, standards, and guidelines issued by the Director[.]" 44 U.S.C. 3552(b)(1). Agencies are required to comply with these directives. 44 U.S.C. 3554(a)(1)(B)(ii).

OVERVIEW OF DRAFT BOD 20-01

On November 27, 2019, CISA posted draft directive 20-01, titled "Develop and Publish a Vulnerability Disclosure Policy," for public feedback at https://cyber.dhs.gov/bod/20-01. This directive requires each agency to develop and publish a vulnerability disclosure policy (VDP), enable receipt of unsolicited vulnerability reports, maintain supporting handling procedures for any vulnerability reports received, and report certain metrics to CISA. DHS is publishing this

notice of availability to provide awareness of the draft binding operational directive being available now for review and comment.

Dated: December 13, 2019.

_____

Richard Driggers,
Deputy Assistant Director,
Cybersecurity Division,
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security.

[FR Doc. 2019-27307 Filed: 12/18/2019 8:45 am; Publication Date: 12/19/2019]