E-ISSN: 2962-6110
P-ISSN: 2964-7843
JSRET
jsret.knpub.com
Journal of Scientific Research, Education, and Technology

A Government-Oriented Vulnerability Disclosure Program Model Based on Ethical Hacker Perspectives

Rio Putra Suryana, Suyud Widiono
Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia

ABSTRACT

Digital transformation within government agencies has expanded the number of public-sector digital assets requiring continuous cybersecurity protection. However, vulnerability reporting mechanisms in Indonesia remain fragmented, unstandardized, and legally ambiguous, limiting effective collaboration between ethical hackers and government institutions. This study explores the motivations, preferences, and challenges experienced by active vulnerability researchers in participating in government-led Vulnerability Disclosure Programs (VDPs). A descriptive qualitative approach was applied using open-and closed-ended online questionnaires completed by six respondents with proven experience in legal vulnerability reporting. The findings reveal that clear scope definition, transparent rules, timely responses, and legal protection (safe harbour) are the primary determinants of participation, outweighing financial incentives. Although monetary rewards are beneficial, most participants are willing to report without them if non-financial recognition—such as points, badges, or official acknowledgment—is provided. This study contributes to the literature by proposing a specialized VDP framework for developing nations where legal protections are nascent. The proposed model emphasizes clear policies, triage transparency, and non-monetary recognition systems to strengthen national cybersecurity resilience through collaborative public engagement.

Keywords: *Vulnerability Disclosure Program (VDP), Vulnerability Reporting, Ethical Hacking, Cybersecurity, Government Digital Assets, Bug Hunter Participation, Safe Harbour.*

Corresponding author
Name: Rio Putra Suryana
Email: rioputrasuryana80@gmail.com

INTRODUCTION

Digital transformation across government agencies has rapidly increased the number of public-sector digital services and online infrastructures, making them more exposed to cybersecurity risks such as data breaches, defacement, unauthorized access, and exploitation of newly emerging vulnerabilities. While many countries have adopted structured Vulnerability Disclosure Programs (VDPs) to strengthen their security posture, the mechanisms for reporting vulnerabilities within the Indonesian public sector remain fragmented, informal, and unstandardized. As a result, ethical hackers often encounter unclear procedures, inconsistent responses, and legal uncertainties when attempting to

report security weaknesses to government institutions(Thomas Walshe & Simpson, 2023). Strengthening national cybersecurity resilience requires a reporting ecosystem that enables coordinated disclosure, provides clear rules, and protects researchers acting in good faith (Saleh & Winata, 2023).

Prior studies demonstrate that well-designed vulnerability disclosure programs (VDPs) bridge communication between security researchers and system owners by establishing a formal reporting channel, defining in-scope assets and acceptable testing, and implementing triage and remediation workflows that reduce duplicate reports and speed response. Evidence for these design elements appears in government guidance and industry/practice reports such as Australia's VDP guide, CISA's VDP Platform materials, and practitioner best-practice writeups(Australi Signal Director, 2022). Research in various countries demonstrates that clear guidelines, predictable response times, and safe-harbour clauses significantly increase ethical hacker engagement, resulting in faster vulnerability mitigation and improved public-sector security (Chatfield & Reddick, 2017). However, existing literature also highlights persistent challenges in government VDPs, such as unclear reporting channels, limited institutional awareness, and weak feedback mechanisms, which undermine trust and discourage researcher participation (T. Walshe & Simpson, 2022). While several government VDP implementations such as the U.S. Department of Defense VDP and GovTech Singapore have shown strong results, academic research focusing on developing VDP frameworks for Southeast Asian or Indonesian contexts is still limited (GovTech Singapore, 2019).

Despite the growing interest in collaborative cybersecurity models, there remains a gap in understanding the motivations, barriers, and expectations of ethical hackers with respect to government-run vulnerability disclosure programs (VDPs) in developing nations. Most empirical research to date has examined corporate bug-bounty ecosystems or Western public-sector initiatives and has highlighted issues such as unclear reporting procedures, limited institutional capacity, and weak legal safeguards for researchers factors that reduce trust and deter participation. However, comparative evidence on how these problems play out where legal protection and structured reporting mechanisms are nascent is limited, slowing policy learning for governments seeking to adopt VDPs(Li & Zhao, 2022). Empirical studies that specifically investigate ethical-hacker behaviour in lower-resource governance contexts are therefore urgently needed. Furthermore, few studies propose reporting models or system frameworks built directly from the perspectives and real-world experiences of vulnerability researchers.

To address this gap, this study seeks to answer the following research questions: (1) What motivates ethical hackers to participate in government-led Vulnerability Disclosure Programs? (2) What barriers or concerns do they face when attempting to report security vulnerabilities to government institutions? (3) What features and mechanisms should an effective government vulnerability reporting system include based on researcher perspectives? These questions aim to capture both the behavioral and technical dimensions of reporting activities.

This research contributes to the existing body of knowledge by presenting empirical findings derived from active vulnerability researchers with verified experience in legal vulnerability reporting. Unlike prior studies that focus on organizational readiness or policy frameworks, this study synthesizes direct insights from the bug-hunting community to propose a conceptual model for a government-oriented vulnerability reporting system. The model emphasizes clear scope definition, triage transparency, non-monetary recognition mechanisms, and safe-harbour protections elements identified by participants as critical to increasing participation and trust. By grounding the framework in real practitioner experiences, this study provides actionable guidance for policymakers and public-sector cybersecurity teams seeking to design or improve VDP implementations (ENISA, 2023).

This direction is supported by international policy research showing that governments implementing coordinated vulnerability disclosure should provide legal clarity and protections to researchers (Herpig, 2024), and by OECD policy analysis emphasizing both the value and limits of safe-harbour provisions in VDPs (OECD, 2021)

METHOD

This study is classified as non-experimental research using a descriptive qualitative approach with an exploratory design. The selection of this design aligns with the research objective, which focuses on identifying ethical hacker motivations, barriers, and preferences related to participation in government-led Vulnerability Disclosure Programs (VDPs). The qualitative approach, as explained by Creswell (2017), is grounded in the interpretivist paradigm, which emphasizes understanding human experiences, perspectives, and meanings through narrative data rather than numerical measurement(Creswell, 2017). Meanwhile, exploratory qualitative research, according to Braun and Clarke, aims to investigate emerging phenomena for which theoretical development is still limited, making it suitable for cybersecurity reporting contexts that lack established empirical frameworks(Braun, Clarke, & Hayfield, 2022). Thus, this design is considered appropriate for answering research questions centered on the subjective experiences of vulnerability researchers in interacting with government reporting mechanisms.

The population in this study includes individuals engaged in cybersecurity activities, specifically ethical hackers, bug bounty hunters, and cybersecurity practitioners with experience in legally reporting vulnerabilities. In qualitative research, the population is defined as all individuals who possess specific characteristics relevant to the research topic (Palinkas et al., 2015). From this population, the researcher employed a non-probability sampling technique using purposive sampling, which involves selecting participants based on predetermined criteria aligned with the research objectives (Sugiyono, 2014). The criteria for respondents include: (1) individuals who have conducted security vulnerability reporting, (2) have participated in VDP or bug bounty programs, and (3) possess prior experience with legal vulnerability disclosure. Based on these criteria, six

respondents were obtained who met the requirements to be included as information-rich participants in this study.

Data collection was conducted in a single stage using an online questionnaire distributed through Google Forms. This instrument was selected due to the participants' high digital literacy and the sensitivity of cybersecurity topics that require secure and flexible participation. The questionnaire contained both closed-ended and open-ended questions designed to capture demographic information, vulnerability reporting experience, motivational factors, legal concerns, and expectations for a government VDP platform. Participants completed the questionnaire independently after reading the study's goals and providing informed consent. During the screening process, no duplicate or invalid responses were identified, and all six completed submissions were retained for analysis.

The research instrument consists of an open-ended qualitative questionnaire developed based on theoretical indicators from previous VDP, coordinated disclosure, and cybersecurity participation studies. According to Kallio et al. (2016)(Kallio, Pietilä, Johnson, & Kangasniemi, 2016), qualitative instruments must represent key conceptual elements of the studied construct to ensure data relevance and depth. In this study, the questionnaire included items addressing: (1) motivations for participating in VDPs, (2) perceived barriers when reporting vulnerabilities to government institutions, (3) expectations regarding scope clarity, reward mechanisms, and legal protection, and (4) preferences for features in a government vulnerability reporting system. These items were structured to encourage detailed narrative responses, allowing participants to express personal experiences and perspectives comprehensively.

Data were analyzed using thematic analysis following the six-phase framework proposed by Braun and Clarke (Braun et al., 2022). The analysis process began with familiarization with all responses, followed by generating initial codes that captured recurring ideas related to motivations, barriers, and reporting preferences. Themes were then developed, reviewed, and refined to ensure coherence and alignment with the dataset. Finally, the themes were defined and interpreted to produce a narrative that addressed the research objectives. Validity was strengthened through cross-checking participant responses and verifying publicly available information such as historical vulnerability reports and professional cybersecurity profiles, following recommendations for ensuring credibility in qualitative research (Nowell, Norris, White, & Moules, 2017) This multi-step approach ensures that the findings accurately represent the perspectives and experiences of vulnerability researchers in the context of government VDP participation.

FINDING AND DISCUSSION

RESEARCH RESULT

The study collected responses from six participants who had experience in cybersecurity activities such as bug hunting, vulnerability reporting, and participation in VDP or bug bounty platforms. Four participants had used international reporting platforms, while two had previously submitted reports directly to organizations. Three respondents

were students with cybersecurity backgrounds, and three were working cybersecurity practitioners.

Motivational data showed that financial rewards were selected by four respondents. Recognition, including certificates and acknowledgment, was selected by three respondents. Contributions to national security and skill development were each selected by two respondents.

Table 1: Summary of Reported Motivations

NO	Motivation Factor	n
1	Financial Reward	4
2	Recognition	3
3	National Contribution	2
4	Skill Development	2

Five respondents stated they were willing to join a government-managed VDP even if no financial rewards were provided, while one respondent chose not to participate.

Table 2: Willingness to Participate in Government VDP

Response	n
Yes	5
No	1

Respondents also selected features they considered necessary in a government VDP. Five respondents selected a points or badge system. Four respondents selected a Hall of Fame page and official certificates. Transparent triage processes were selected by three respondents, and two respondents still preferred financial rewards as an additional feature.

Table 3: Preferred VDP Features

NO	Feature	n
1	Points / Badges	5
2	Hall of Fame	4
3	Certificate	4
4	Transparent Triage	3
5	Financial Reward	2

Participants also identified several barriers encountered or anticipated when reporting vulnerabilities to government entities. Unclear scope and reporting rules were selected by four respondents. Lack of government response was selected by three respondents. Legal concerns and distrust toward the government were each selected by two respondents.

Table 4: Reported Barriers

NO	Barrier Type	n
1	Unclear Scope / Rules	4
2	No Government Response	3
3	Legal Concerns	2
4	Distrust	2

Finally, respondents identified the elements they viewed as most essential for an effective government VDP. Clear scope documentation was selected by five respondents. A recognition system was selected by four respondents. Legal clarity through safe harbour and transparent response workflows were each selected by three respondents.

Table 5: Critical Elements for an Effective VDP

NO	Element	n
1	Clear Scope Documentation	5
2	Recognition System	4
3	Safe Harbour	3
4	Transparent Response Flow	3

DISCUSSION

The findings of this study show that ethical hackers have a strong intention to participate in a government-managed Vulnerability Disclosure Program (VDP), even when financial incentives are not the primary motivator. Respondents consistently emphasized the need for clear scope documentation, legal protection, and transparent response processes. The high importance placed on non-financial recognition—such as certificates, badges, or a Hall of Fame—indicates that participants value professional acknowledgment and career-related benefits. These results suggest that ethical hackers are motivated not only by financial gain but also by opportunities to contribute to national cybersecurity and build their professional reputation. The identification of unclear rules, lack of responsiveness, and legal concerns as major barriers highlights gaps in current government vulnerability reporting practices and the need for structured, accessible, and researcher-friendly programs.

The results align with international research on coordinated vulnerability disclosure. Studies on the U.S. Department of Defense VDP and GovTech Singapore show that program success is strongly linked to transparency, clear rules, and safe harbour protections rather than financial rewards alone (Chatfield & Reddick, 2018; GovTech Singapore, 2020). ENISA's recommendations also highlight the importance of scope clarity and legal assurances to encourage researcher participation, which closely matches the concerns expressed by respondents in this study. Previous research similarly notes that delayed responses and unclear triage processes discourage ethical hackers from submitting

vulnerabilities (Arora & Nandkumar, 2012). Overall, this study's findings confirm global patterns regarding the conditions needed for effective public-sector VDP implementation.

This study has several limitations that should be considered when interpreting the results. First, the sample size is limited to six respondents, which may not fully represent the broader ethical hacking community in Indonesia. Second, the study relies solely on self-reported questionnaire data, which may introduce bias in how respondents describe their experiences or motivations. Third, the research does not include government stakeholders, which limits the ability to compare researcher expectations with institutional readiness. Finally, the study focuses on perceptions rather than direct observation of VDP processes, which may reduce the generalizability of findings in real operational contexts.

The findings provide several implications for both practice and future research. For government agencies, the results highlight the need to establish a formal VDP framework that includes clear scope definitions, safe harbour legal protections, transparent communication channels, and a structured recognition system. Such a framework would likely increase participation and improve the quality of vulnerability reporting. For researchers, the study indicates that further investigation with larger and more diverse samples is needed to validate these findings. Future research could explore government perspectives, compare multiple reporting models, or evaluate pilot VDP implementations in public institutions. Practically, the results support the development of a national, centralized reporting platform to facilitate secure and consistent communication between ethical hackers and government cyber teams.

CONCLUSION

This study investigated the perceptions, motivations, and barriers experienced by ethical hackers toward the implementation of a government-managed Vulnerability Disclosure Program (VDP). The results showed that respondents are willing to participate in a government VDP even in the absence of financial rewards, provided that the program offers clear scope documentation, transparent reporting procedures, and non-financial recognition such as certificates, badges, or public acknowledgment. The primary barriers identified include unclear rules, lack of government responsiveness, and legal concerns, indicating that current reporting channels may not adequately support responsible disclosure efforts.

The findings highlight the importance of establishing a structured and researcher-friendly VDP framework for government institutions. Clear operational guidelines, safe harbour protections, and consistent communication processes are essential to encourage participation and build trust with the cybersecurity community. Implementing these elements would support more effective vulnerability reporting and strengthen national cybersecurity resilience.

For future research, larger and more diverse samples are recommended to validate these findings across broader segments of the ethical hacking community. Studies involving government agencies or comparative analyses of existing VDP models in other countries may also provide deeper insights. Practically, the results support the development and

testing of a centralized national VDP platform that integrates clear rules, recognition systems, and transparent workflows.

REFERENCES

Australi Signal Director. (2022). *Vulnerability Disclosure Programs Explained*.

Braun, V., Clarke, V., & Hayfield, N. (2022). 'A starting point for your journey, not a map': Nikki Hayfield in conversation with Virginia Braun and Victoria Clarke about thematic analysis. *Qualitative Research in Psychology*, *19*(2), 424–445. https://doi.org/10.1080/14780887.2019.1670765

Chatfield, A. T., & Reddick, C. G. (2017). Cybersecurity Innovation in Government. *Proceedings of the 18th Annual International Conference on Digital Government Research*, 64–73. New York, NY, USA: ACM. https://doi.org/10.1145/3085228.3085233

Creswell, J. W. . (2017). *Research design : qualitative, quantitative, and mixed methods approaches*. SAGE.

ENISA. (2023). *Vulnerability Disclosure Guidelines for Public Sector*. https://doi.org/10.2824/69116

GovTech Singapore. (2019). *Government Vulnerability Disclosure Programme Annual Report 2019*.

Herpig, S. (2024). *Europe Vulnerability Disclosure: Guiding Governments from Norm to Action*.

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Li, Y., & Zhao, L. (2022). Collaborating with Bounty Hunters: How to Encourage White Hat Hackers' Participation in Vulnerability Crowdsourcing Programs through Formal and Relational Governance. *Information & Management*, *59*(4), 103648. https://doi.org/10.1016/j.im.2022.103648

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis. *International Journal of Qualitative Methods*, *16*(1). https://doi.org/10.1177/1609406917733847

OECD. (2021). *ENCOURAGING VULNERABILITY TREATMENT OVERVIEW FOR POLICY MAKERS OECD DIGITAL ECONOMY PAPERS Foreword*. Retrieved from http://www.oecd.org/termsandconditions.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Saleh, A. I., & Winata, M. D. (2023). *Indonesia's Cyber Security Strategy: Problems and Challenges*. https://doi.org/10.2991/978-2-38476-152-4_169

Walshe, T., & Simpson, A. C. (2022). Coordinated Vulnerability Disclosure programme effectiveness: Issues and recommendations. *Computers & Security*, *123*, 102936. https://doi.org/10.1016/j.cose.2022.102936

Walshe, Thomas, & Simpson, A. (2023). Towards a Greater Understanding of Coordinated Vulnerability Disclosure Policy Documents. *Digital Threats: Research and Practice*, *4*(2), 1–36. https://doi.org/10.1145/3586180