Comments on Latvia's Proposed Amendments to the National Cybersecurity Act

August 28, 2026

The Hacking Policy Council ("HPC") appreciates the opportunity to comment on Latvia's proposed Amendments to the National Cybersecurity Act (Project ID 26-TA-1830).

The HPC is a group of experts dedicated to creating a more favorable legal, policy, and business environment for good-faith security research, penetration testing, independent repair for security, and vulnerability disclosure and management. From this perspective, we offer the following recommendations to strengthen the proposed framework and provide greater legal certainty for good-faith security researchers.

HPC generally supports Latvia's effort to establish a legal framework for the participation of good-faith security researchers in the coordinated vulnerability disclosure process and create clearer legal protections for good-faith security research. HPC has consistently advocated for governments to establish clear legal protections for good-faith security research, including safe harbor provisions, that shield responsible researchers from liability when they discover and disclose vulnerabilities in good faith.

Good-faith security research plays an important role in helping organizations identify and remediate vulnerabilities before they can be exploited by malicious actors. To support this work, researchers need clear legal protections that distinguish legitimate security research from malicious cyber activity. When governments fail to make that distinction, researchers may hesitate to conduct or disclose responsible security testing out of concern that they could face legal liability despite acting in good faith. This uncertainty can discourage vulnerability discovery and responsible disclosure, reducing opportunities to remediate security flaws before they are exploited.

The explanatory materials accompanying Latvia's proposed amendments correctly recognize that legal uncertainty can discourage researchers from identifying and reporting vulnerabilities, ultimately weakening cybersecurity outcomes overall. We are concerned, however, that the proposed language focuses too heavily on the outcome or impact of the research, rather than the researcher's intent and good-faith conduct.

In the proposed language to amend Article 39 of the National Cybersecurity Act, the amendments would permit vulnerability research where the researcher's actions do not impose a disproportionate burden and do not compromise the security of the system or network, the confidentiality, integrity, or availability of data, or continuity of operations. Legitimate good-faith

security research can sometimes produce unintended consequences. A researcher acting responsibly could inadvertently encounter data, trigger an error, or temporarily affect a system while attempting to verify a vulnerability. For this reason, we recommend a clearer, intent-based standard so that unintended consequences do not expose legitimate researchers to legal liability when they are acting in good faith.

Therefore, HPC recommends that the amendments instead emphasize research conducted ethically, in good faith, and consistent with responsible vulnerability disclosure practices. To define responsible or good-faith vulnerability research, HPC recommends terminology used in United States law as a model. Under 37 C.F.R. § 201.40(b)(18), "'good-faith security research' means accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."

This standard provides a useful model because it focuses on the researcher's purpose and whether the activity was designed to avoid harm, rather than requiring that no unintended impact occur. Latvia should adopt a similarly clear, intent-based standard so that good-faith researchers will be protected when they act responsibly. Malicious or reckless conduct remains outside the scope of this definition.

HPC also recommends that Latvia's law encourage companies to adopt best-practice vulnerability rewards programs (VRPs) as an important mechanism for facilitating good-faith vulnerability research. VRPs, also referred to as bug bounty programs (BBPs), offer structured opportunities for independent researchers to find and responsibly report vulnerabilities in exchange for financial incentives. Such programs establish clear parameters for security testing and typically direct researchers to conduct testing in ways that minimize the risk of disrupting company systems or accessing unauthorized data. VRPs therefore create incentives for good-faith security researchers to identify and report vulnerabilities while minimizing operational disruption and access to unauthorized data.

Latvia's proposal is an important step toward improving vulnerability discovery and coordinated disclosure. A clear, intent-based protection for good-faith researchers would better achieve the law's purpose while preserving appropriate safeguards against malicious or reckless conduct. Thank you for the opportunity to provide input to the consultation. If we can be of additional assistance, please contact Bri Law at BLaw@Venable.com.

Sincerely,

Hacking Policy Council