# How policymakers are helping expand the adoption of bug bounty programs

BY ANNA HAMMOND · DECEMBER 20, 2022 · LAST UPDATED ON MARCH 6, 2025

*Thanks to lawmakers, 2022 was one of the best years ever for the advancement, validation, and growth of the bug bounty and crowdsourced security industry.*

As we look back over the cybersecurity developments in 2022, we see a year where bug bounty programs and vulnerability disclosure policies (VDP) were increasingly mandated as part of government and non-governmental security postures.

Among the principal reasons for this increase in the mainstreaming of crowdsourced cybersecurity was major support from lawmakers across the globe, who introduced legislation and policies to support it.

This high-level recognition – and the tangible benefits of crowdsourcing – are rapidly changing the cybersecurity domain. Indeed, 2022 may well be remembered as the year this already popular security method became a standard practice.

With 2022 drawing to a close, we take stock of some of this year's most significant cybersecurity policy and legislation updates from across the globe. These can be divided into three key categories:

1. Increased adoption and mandating of crowdsourced security programs by governments
1. Legislative developments that highlight and validate bug bounty program security services
1. New policies and laws that are driving better cybersecurity across the board

## Government adoption and mandating of crowdsourced security programs

***Summary:*** *The increased adoption of bug bounty programs and VDPs by Governments, NGOs, and businesses in 2022 was a strong indicator that major institutions now consider crowdsourcing a critical element in their cybersecurity arsenal.*

Nearly every aspect of work and government has been digitized in the past decade. Pen and paper forms feel like a relic of a bygone age. This revolution has meant that securing digital assets in government, businesses, and our personal lives has never been more important.

2022 saw governments increasingly willing to legislate to ensure that any type of institution that holds digital assets – both governmental and non-governmental – use bug bounty programs and VDPs to protect themselves against the ubiquitous threat of malicious hacking and data breaches.

In many places, this has now been standardized and enthusiastically adopted as the 2022 policy record among the big players.

## Public sector VDPs

The **US government** has been leading the way for several years in moving towards ensuring all agencies have a VDP in place.

In March 2022, the Cybersecurity and Infrastructure Security Agency (CISA) VDP Platform was fully authorized to operate. The goal: improving the security of federal agencies' internet-accessible systems through a "centrally managed vulnerability intake system".

And in April 2022, the Department of Homeland Security (DHS) reported that 'Hack DHS' had successfully concluded. This first full-scale bug bounty program saw 450 vetted security researchers identify 122 vulnerabilities, of which 27 were deemed critical. DHS awarded a total of $125,600 to the participants.

## European developments

In Europe, meanwhile, the **European Commission** (EC) launched a new open source-focused security rewards program dedicated to projects underpinning its public services.

Following the EU-FOSSA program, which had been dubbed a "remarkable success", the Open Source Programme Office (EC OSPO), which is hosted by European bug bounty platform Intigriti, next offered security researchers up to €5,000 ($5,600) for unearthing vulnerabilities in LibreOffice, LEOS, Mastodon, Odoo, and CryptPad.

The EC also invited hackers to the NextGov Hackathon, which took place on April 25 to May 10 with the goal of fostering "digital sovereignty for public services".

By November of the year, the **European Union** had also become aggressive in insisting on much stronger cybersecurity across the board with its full adoption of the NIS2 directive. The scope of the directive is huge, but in a nutshell, it requires organizations to take measures to protect networks and information systems from cyberattacks. It follows that bug bounty programs will become an increasingly important part of all organizations' compliance with the directive.

To top off another year of positive developments for the bug bounty and crowdsourced security space, the consultation of the **EU Cyber Resilience Act** is currently underway, with the feedback period due to end on January 23, 2023.

Interestingly, the proposal for a regulation on "cybersecurity requirements for products with digital elements" specifically includes VDPs and bug bounties among its list of recommendations.

## More government bug bounty news

The **Swiss National Cyber Security Centre (NCSC)** also launched a private bug bounty program in 2022 following a pilot program in 2021. In this instance, security researchers have been invited to probe the federal government's web applications, APIs, and critical infrastructure.

Affirming that the trend towards crowdsourced security is not localized to the northern hemisphere, on the other side of the globe, **New Zealand's Government Communications Security Bureau (GCSB)** also called on government agencies to introduce vulnerability disclosure policies, making it possible for researchers to report bugs on a no-blame basis.

Perhaps ill-advisedly for adoption rates, at least, the GCSB is currently offering no bug bounties. Still, it is a strong first step in the crowdsourced security direction and contains a stipulation that all vulnerabilities uncovered should be patched, mitigated, or managed within 90 days.

## Legislative developments in recognition of the bug bounty industry

***Summary:*** *In 2022, lawmakers around the world passed legislation to improve transparency for organizations considering taking out a bug bounty, and for ethical hackers who may previously have been operating in a legal grey area due to the ambiguous wording of aging laws.*

2022 brought fresh legislation recognizing and validating the important role crowdsourced security programs like bug bounties and VDP now play in maintaining cybersecurity.

Legislation changes also recognized that laws designed to prosecute malicious hacking from previous epochs were actually deterring the adoption of crowdsourced security practices. Legislation was therefore amended in several territories to bring greater transparency to crowdsourced cybersecurity.

Perhaps the most impactful example of this will be the changes made to the **US government's Computer Fraud and Abuse Act (CFAA)**. We wrote about this at the time on the Intigriti Blog.

READ MORE US Justice Department will no longer bring charges against good-willed security researchers

The core takeaway is that the Department of Justice will officially no longer prosecute security researchers acting "in good faith". While this has been a *de facto* reality for some years, it is finally in the law books and will provide security researchers with much-needed assurances as they go about their valuable work.

Academic research on the possibilities of regulated ethical hacking opened up by **International, European, and Spanish law** also contributed to improving the standards and processes that underpin bug bounty programs. Stringent research like this on the effectiveness of crowdsourced security should enhance the benefits for both businesses and cybersecurity professionals everywhere.

## Other developments pointing to wider official adoption of bug bounty programs/VDP

***Summary:*** *Beyond the targeted legislation and policy changes around bug bounty programs in 2022, many other laws were enacted that underline the need for businesses to get serious about cybersecurity. Again, with crowdsourced security now in the mainstream, compliance will involve further adoption and growth in the bug bounty sector.*

2021 ended with slightly encouraging news about trends in cyberattacks. However, given the still staggering number of cybersecurity breaches, lawmakers continued to look for additional ways to improve the security landscape. A diverse array of new policies therefore came into play.

**In Australia**, for example, after the massive Optus and Medibank customer data breaches, businesses hit by serious or repeated data breaches now face fines of up to $50m. Obviously, this is a major incentive for all businesses to get robust cybersecurity in place proactively and stands to benefit anyone whose data is at risk of being targeted by malicious hackers.

**In the USA,** in the absence of a preemptive federal privacy law, **individual states** also took the initiative by enacting so much data privacy legislation during the 2022 legislative cycle that even industry legal experts described it as "overwhelming".

These advances included **Connecticut** and **Utah** following on the heels of **Virginia** and **Colorado**, who in 2021 put in place privacy laws based on the 2021 Washington Privacy Act (Senate Bill 5062). These laws again emphasize the need for businesses to be proactive in providing adequate cybersecurity and will include stiff new penalties for failing to protect personal data.

Finally, 2022 also saw a new **European Union directive** on the books that changed the game for digital goods producers. We reported on this in June, and it's worth a read if you want to understand how new legislation is impacting purely digital businesses.

## Closing thoughts

While 2022 has already given governments, businesses, and NGOs a lot to digest in terms of new legislation, the trend towards more legislative and policy action is likely to continue in 2023 as the potential for serious damage from cybercrime continues to escalate.

The far-reaching consequences of the Russian war in Ukraine war have provided just one of many sobering examples of how cybersecurity is critical for the stability and safety of individuals and economies.

In 2023, governments already seem poised to increase the stringency of their policies and laws. One example of note for the infosec community is the Digital Operational Resilience Act (DORA).

It is in line with the European Commission's priorities to make the eurozone "fit for the digital age", **DORA** includes provisions related to threat-led pentesting, adversary simulation, and the use of third-party threat intelligence.

We'll have more on DORA and all the other cybersecurity developments that relate to bug bounty programs and VDP in 2023, so stay tuned to this space and we'll see you then!