



Vulnerability Disclosure Policy Platform

2023 Annual Report

Publication: September 2024
Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see <https://www.cisa.gov/tlp>.

Table of Contents

- Annual Report Highlights.....1
- VDP Platform 2023 Insights.....2
 - 2023 Top Five Vulnerability Classes Found by Researchers.....2
- VDP Platform Data Since Launch.....3
- VDP Platform Value.....4
 - Time and Cost Savings.....4
 - Complementing Automated Scanning Tools4
- The Public Security Research Community5
 - Public Security Researcher Insights6
 - Researcher Leaderboard: Valid Submissions Since Launch6
 - Top 2023 Researchers (by Critical & Severe Findings)7
- The VDP Platform’s Bug Bounty Capability7
 - Bug Bounty Support7
 - 2023 Bug Bounty Highlights.....8
- Conclusion.....8

Annual Report Highlights

The Cybersecurity and Infrastructure Security Agency's (CISA) Vulnerability Disclosure Policy (VDP) Platform achieved remarkable success in 2023, its second full year of operation. Throughout 2023, CISA focused on advocating for the increased agency adoption of the VDP Platform, supporting federal civilian executive branch (FCEB) agencies in identifying vulnerabilities in their systems, and engaging the security research community.

Since launching in 2021, the VDP Platform has triaged over 12,000 submissions (over 7,000 in 2023) on behalf of 51 onboarded agency programs, saving agencies a significant amount of time and resources. Additionally, through the VDP Platform, over 2,400 unique, valid vulnerability disclosures have been identified, of which nearly 2,000 have been remediated by agencies. Since launch, over 3,200 security researchers have participated on FCEB VDPs via the VDP Platform.

While the VDP Platform's achievements are considerable, it is worth noting that vulnerability disclosure policies are only one component of a mature vulnerability management process. This report's data should be taken into consideration within the specifics of each organization before prioritizing any findings.

Security researchers play a vital role in securing our federal government's networks. As part of CISA's persistent and ongoing collaboration with the security research community, in 2020 CISA issued [Binding Operational Directive \(BOD\) 20-01](#), which requires every FCEB agency to establish a vulnerability disclosure policy. These VDPs follow industry and community best practices, including giving authorization to participating security researchers and committing to not pursue legal action for good-faith research. CISA's VDP Platform complements BOD 20-01 by giving FCEB agencies an easy way to establish a VDP and engage with security researchers. CISA appreciates the contributions by thousands of security researchers to date and looks forward to continuing to further broaden this collaboration in the future.

VDP Platform 2023 Insights

The VDP Platform saw continued growth in 2023 that can be attributed to several beneficial interdependent factors. With 11 agency programs onboarding in 2023, the VDP Platform drew heightened researcher attention and engagement, which facilitated a marked increase in the volume of vulnerability submissions received, valid vulnerabilities identified, and vulnerabilities remediated.¹

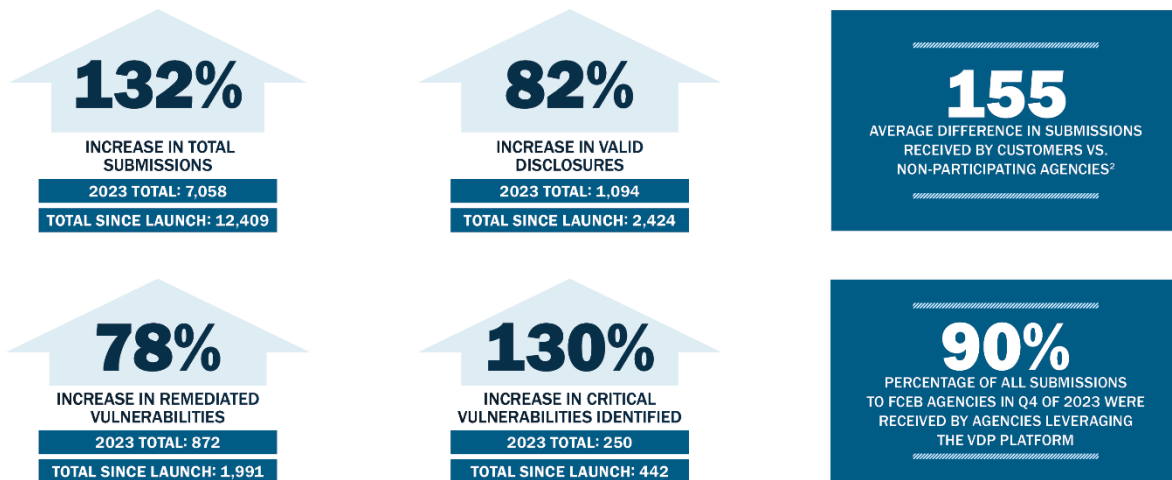


Figure 1: Graphic illustrating statistics related to VDP submissions and disclosures in 2023

2023 Top Five Vulnerability Classes Found by Researchers

Many classes of vulnerabilities deemed most critical by the cybersecurity community are being identified through the VDP Platform. The top vulnerability classes found through the VDP Platform, ranked in the following table, are also present within the Open Web Application Security Project (OWASP) Top Ten list.³ The findings below reflect the most common software faults identified in internet-facing systems of agencies participating on the VPD Platform. They do not necessarily represent the most critical threats requiring protective action. Organizations should quantify and internally perform any comparisons with prioritizing securing internal critical infrastructure. Any organization looking to apply the findings below to prioritizing the security of their internal critical infrastructure should first consider performing the analysis for their specific organization.

Rank	Vulnerability Class	2023 Totals (Each mark represents 10 valid vulnerabilities)	2022 Totals (Rank)	Potential Impact
1	Cross-Site Scripting (XSS)	371	400 (1)	<ul style="list-style-type: none"> Compromised accounts Reputational damage Legal and regulatory consequences
2	Server-Side Injection	178	98 (2)	<ul style="list-style-type: none"> Data breaches Service disruption Financial loss
3	Sensitive Data Exposure	172	93 (4)	<ul style="list-style-type: none"> Legal and regulatory consequences Financial loss Reputational damage
4	Server Security Misconfiguration	119	96 (3)	<ul style="list-style-type: none"> Data breaches Loss of sensitive data Reputational damage
5	Broken Access Control (BAC)	65	47 (5)	<ul style="list-style-type: none"> Legal and regulatory consequences Compromised data integrity Reputational damage

Figure 2: Table illustrating top five vulnerability classes identified through the VDP Platform in 2023

¹ Percent increase data compares 2023 calendar year data to cumulative, inception-to-date data as of Dec. 31, 2022.

² Data comparing participating and non-participating agencies is based on agency metrics reported through CyberScope. For more information on vulnerability types, see Bugcrowd's Vulnerability Rating Taxonomy (<http://bugcrowd.com/vulnerability-rating-taxonomy>).

³ The OWASP Top Ten list notes vulnerabilities that have broad consensus as the most critical security risks to web applications. For more information on the OWASP Top Ten list, see <https://owasp.org/www-project-top-ten/>.

VDP Platform Data Since Launch

The below data points represent the total submissions from participating researchers on the VDP Platform since it launched in June 2021, and the total number of valid disclosures and remediated vulnerabilities from these submissions. Each year has seen an increase in identified critical and severe vulnerability reports identified, with reports nearly doubling.

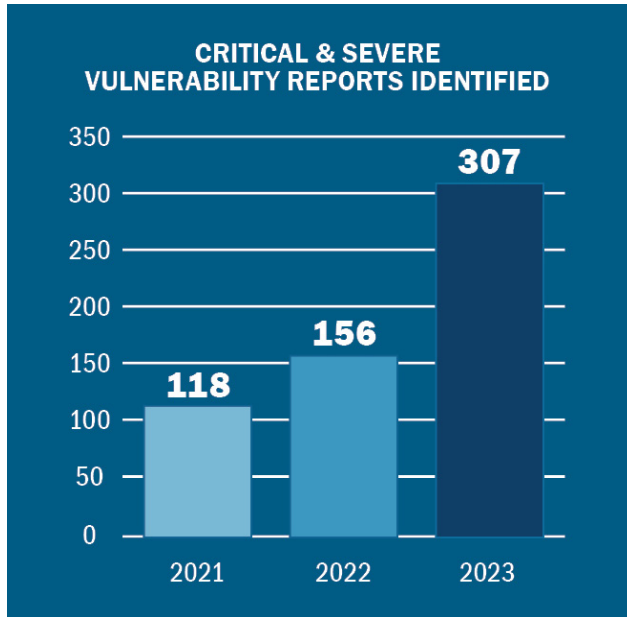
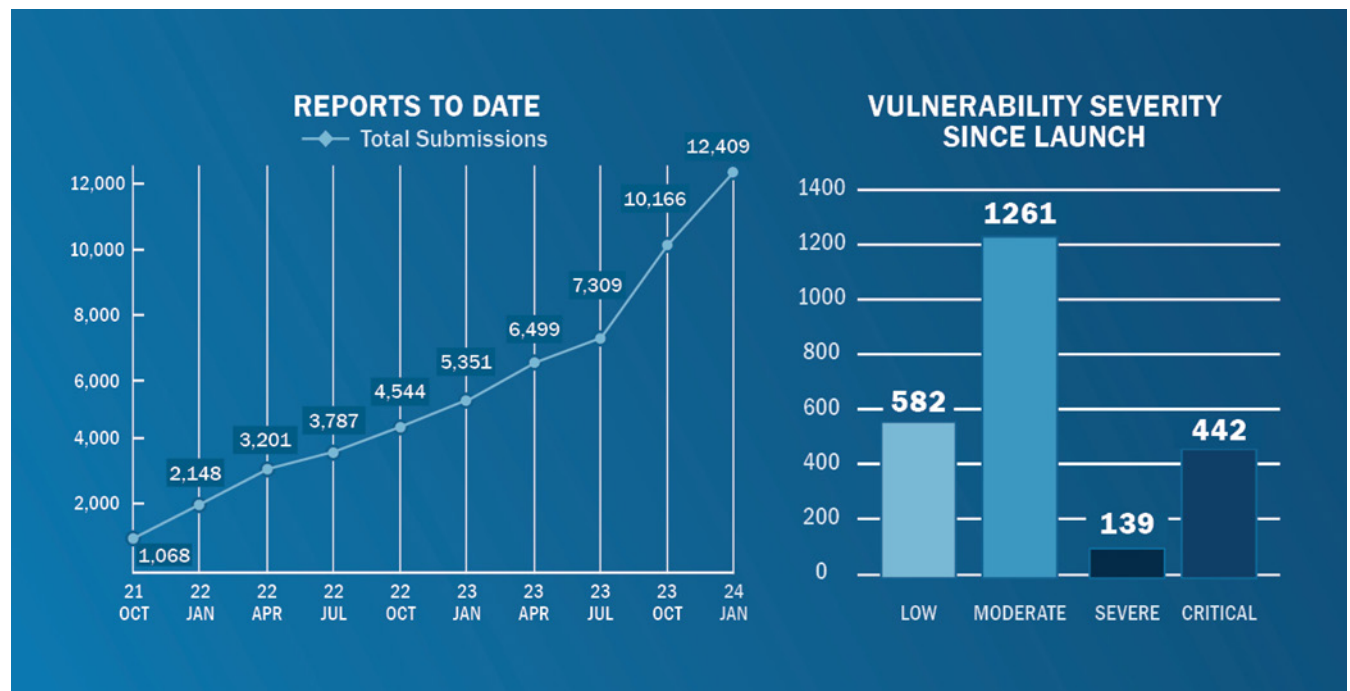


Figure 3 (left): The table above illustrates the total number of submissions received, valid disclosures identified and remediated vulnerabilities facilitated by the service since launch. The table on the left illustrates the number of critical and severe vulnerability report submissions reported to date.

Figure 4 (below): The graph on the left illustrates the number of total submissions reported since the service's launch. The graph on the right shows the quantities of each type of vulnerability (low, moderate, severe or critical) that have been identified since the service's launch.



VDP Platform Value

Time and Cost Savings

The VDP Platform offers agencies significant cost and time savings. While VDPs are a critical component of an agency's vulnerability management process, implementation and management come with associated costs for agencies. Handling disclosed vulnerabilities, triaging reports, corresponding with security researchers, and collecting and reporting required metrics are all labor-intensive steps that draw agency resources away from prioritizing valid vulnerability submissions and coordinating remediation activities.

Federal agencies often have large attack surfaces and limited resources allocated to defend them, so efficiencies offered through the VDP Platform can have a significant impact on an agency's ability to drive down cyber risk. Federal agencies safeguard vast amounts of sensitive data and are responsible for delivering crucial public services.

On average, participating agencies validate submissions two days faster than non-participating agencies. Across these agencies, an estimated average of \$4.45 million in potential remediation costs for critical and severe vulnerabilities has been saved.

The potential damage caused by any of the vulnerabilities identified, particularly those categorized as critical or severe, could be widespread and catastrophic.

“The VDP Platform gets our stamp of approval. It has benefited us quite a bit ... it is very efficient. All the information is there. [The VDP Platform] has filtered tickets and allows us to streamline information to our Product team quicker.”

—National Aeronautics and Space Administration (NASA) VDP Program Manager

Figure 5 (right): VDP Platform functions

VDP PLATFORM FUNCTIONS	
Triages Vulnerabilities	✓
Filters Duplicate Submissions	✓
Manages Researcher Correspondence	✓
Tracks Remediation Performance	✓
Automates Reporting Metrics	✓
Increases Researcher Attention	✓




Complementing Automated Scanning Tools

While automated scanning tools allow for quick and efficient scanning of systems for vulnerabilities, they are not a cure-all solution for cybersecurity. Limitations include being programmed to search for only a certain set of patterns or rules.

The thousands of security researchers participating on the VDP Platform bring unique skill sets and perspectives to the hunt for vulnerabilities on agency systems. They are not confined to searching for a set list of vulnerabilities derived by algorithms, but instead are able to be creative in their approach, which supports their ability to identify new, unique, or otherwise unconventional vulnerabilities. As a result, by using the VDP Platform, security researchers have identified vulnerabilities on agency systems that existing scanning tools might have overlooked.

The Public Security Research Community

WHO ARE THE PUBLIC SECURITY RESEARCHERS PARTICIPATING ON THE VDP PLATFORM?

-  Global, diverse community
-  68% are college graduates⁴
-  Primarily Millennial and Generation Z individuals, ranging from students looking to begin their cybersecurity careers to seasoned cybersecurity professionals

WHY DO PUBLIC SECURITY RESEARCHERS PARTICIPATE ON THE VDP PLATFORM?





-  A sense of civic duty to support federal cybersecurity and help agencies address vulnerabilities before exploitation
-  Potential financial incentives (for bug bounty programs)
-  Professional and skill development opportunities
-  New challenges

Figure 6: Public Security Researchers

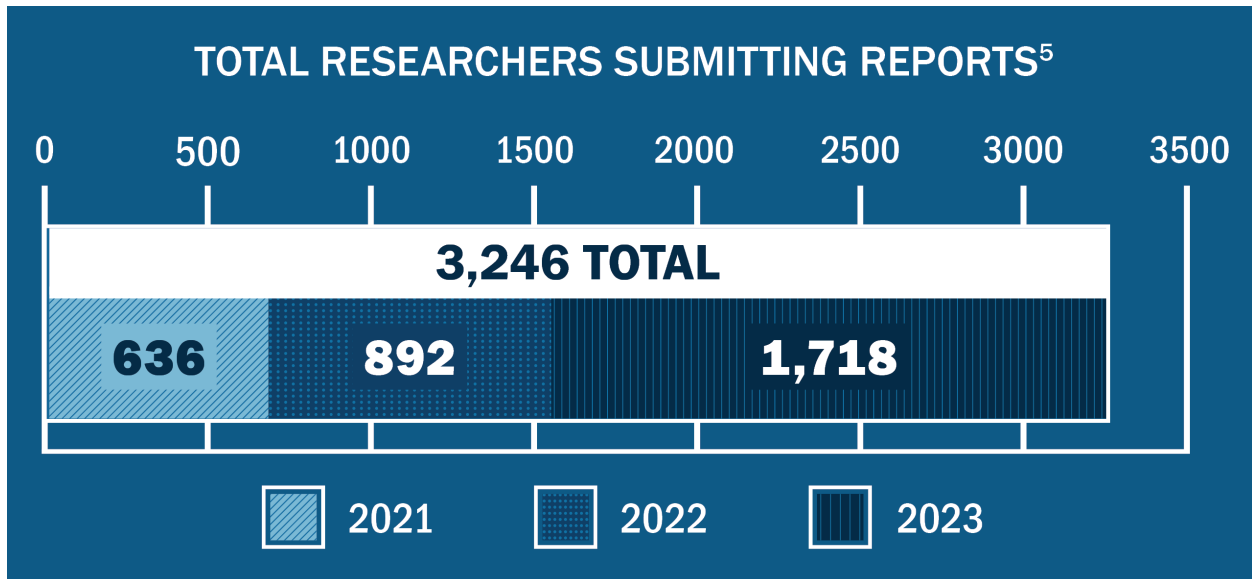


Figure 7: Graph illustrating number of total unique researchers submitting reports per year

⁴ "2023 Inside the Mind of a Hacker Report." Bugcrowd. Accessed June 7, 2024. <https://ww1.bugcrowd.com/inside-the-mind-of-a-hacker-2023/>.

⁵ Researcher count is based on individuals submitting a report to participating agencies.

Public Security Researcher Insights

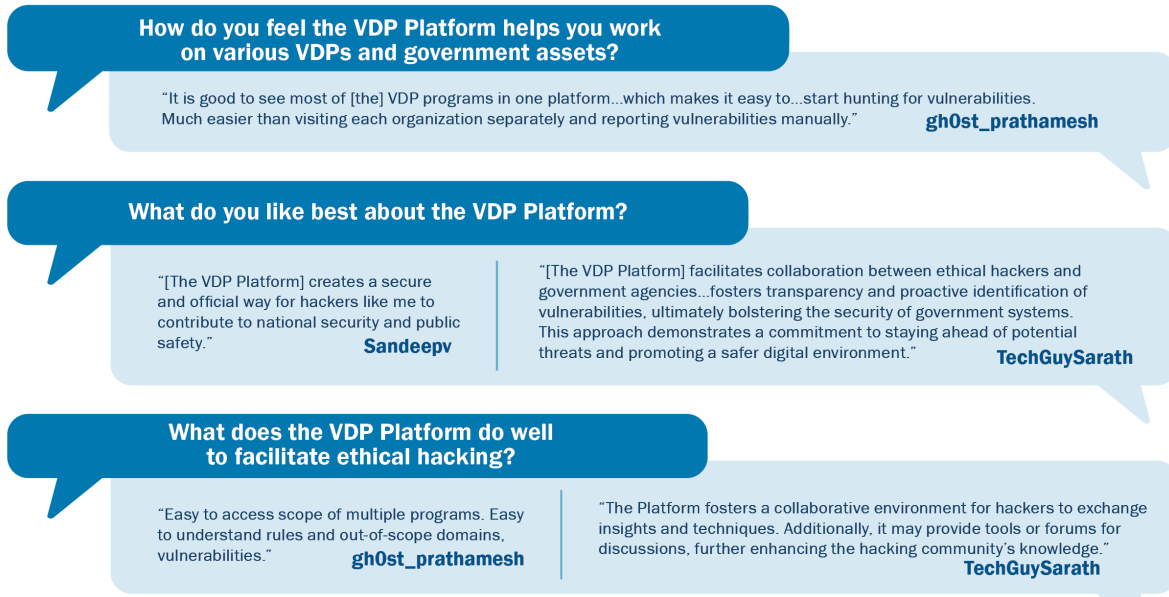


Figure 8: Public Security Researcher Q & A

Researcher Leaderboard: Valid Submissions Since Launch⁶

RANK	RESEARCHER	VALID SUBMISSIONS	RANK	RESEARCHER	VALID SUBMISSIONS
01	frostb1te	104	14	kauenavarro	19
02	PrIvate User	69	15	3th1c_yuk1	18
03	edoardottt	56	16	Surya_Appsec	17
04	mouka	51	17	MorningStar	16
05	takshal	51	18	Cybercrook	14
06	thlrup	48	19	TechGuySarath	14
07	joe-grizzly	44	20	gregaal	14
08	Galapag0s	37	21	Private User	14
09	sharl7a0x	31	22	Private User	13
10	mysanlsmIne	29	23	Miguel_Segovia	13
11	tmz900	21	24	Private User	13
12	Private User	19	25	ravlmahlle	12
13	Private User	19			

Figure 9: Graphic showing the researchers with the most valid vulnerability submissions since the VDP Platform launch

⁶ Researcher leaderboard is based on Bugcrowd's review of vulnerability submissions to federal programs.

Top 2023 Researchers (by Critical & Severe Findings)



Figure 10: Graphic presenting top three researchers from 2023 in terms of number of valid critical and severe findings

The VDP Platform's Bug Bounty Capability

Bug Bounty Support

Bug bounty programs provide financial incentives to encourage the public to further research specific systems for vulnerabilities. While an optional feature of the VDP Platform, bug bounty programs are the next step in maturing and strengthening an agency's vulnerability disclosure processes. Although bug bounties require funding allocations, a bounty payment is a fraction of the cost incurred by a breach⁷ and serves as a major incentive in attracting an elite group of vetted security researchers with experience in finding critical and severe vulnerabilities. In 2023, the VDP Platform supported two agencies in launching bug bounty programs and coordinated with several agencies on maturing disclosure processes to support them.

“The researchers are very engaging. They want to help us find bugs ... and are very excited to engage with us.”

—National Aeronautics and Space Administration (NASA) VDP Program Manager

“Excellent transparency by the team, great payouts and communication.”

—Bug Bounty Researcher

⁷ According to findings by IBM and the Ponemon Institute, the average cost of a data breach in 2023 was \$4.45 million. See full report: <https://www.ibm.com/reports/data-breach>

2023 Bug Bounty Highlights

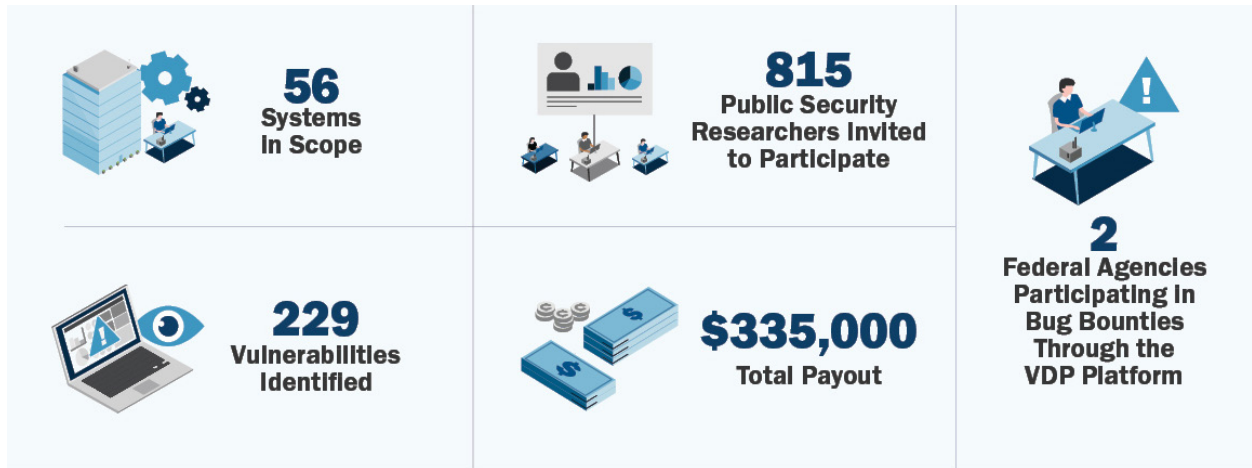


Figure 11: Graphic highlighting 2023 VDP Platform bug bounty metrics

Conclusion

By deploying the VDP Platform, CISA has set a standard for vulnerability management across the federal government. All FCEB agencies are required to publish a VDP, and through the VDP Platform, CISA plays a critical role in supporting agencies in making their VDPs more effective and efficient. As additional agencies continue to onboard to the VDP Platform, the number of vulnerabilities identified and remediated will continue to increase, leading to a more secure federal environment. Likewise, agencies will continue to mature their VDP and bug bounty programs, which will have cascading positive effects on federal cybersecurity.

Through the VDP Platform, CISA continues to advance its visibility into vulnerability disclosures and threat trends across the FCEB. With its ability to share that information across communities, the VDP Platform serves as a model for crowdsourced cybersecurity solutions beyond the FCEB. Organizations in all levels of government and critical infrastructure should consider exploring further the value these solutions offer to enhance their cybersecurity posture.

For more information, email CyberSharedServices@cisa.dhs.gov