DIGITAL SERVICE AT CMS

Open Source & The Digital Service at CMS.gov

Andrea Fletcher, Chief Digital Strategy Officer
Remy DeCausemaker, Open Source Program Office Lead

Centers for Medicare & Medicaid Services // Nava OSS Summit // October 2024

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf
opensource@cms.hhs.gov

Open Source and The Digital Service at CMS

What’s Coming Next

1. **The Digital Service at CMS**
2. **The First Federal OSPO**
3. **What are the Risks? What are the Benefits?**

The Digital Service at CMS

cms.gov/digital-service

What does the Digital Service at CMS do?

We work to transform the U.S. healthcare system by:

Improving the design of healthcare experiences

Delivering value to the government, healthcare providers, and patients

Modernizing systems

Participating in policy development

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf

How do we do it?

We deploy **small groups** of designers, engineers, and product managers on a "tour of duty" to work alongside **dedicated civil servants**.

These **multidisciplinary teams** bring best practices and new approaches to support government **modernization** efforts.

Who we serve: The American People (180M+)

65 M

Medicare Beneficiaries

(2022)

88 M

Medicaid Beneficiaries

(2022)

31 M

Healthcare.gov

(2021)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: Taxpayers

$ 1.7 T

CMS Budget - 12% of the federal budget

(FY 2022)

$ 829 B

Total Medicare Payments

(FY 2021)

$ 646 B

Total Medicaid Payments

(FY 2019)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

Who we serve: The Health Care System

6,244

CMS Employees

(FY 2022)

1.4M

Health Care Providers

(2022)

20%

National Health Care Spending is Medicare

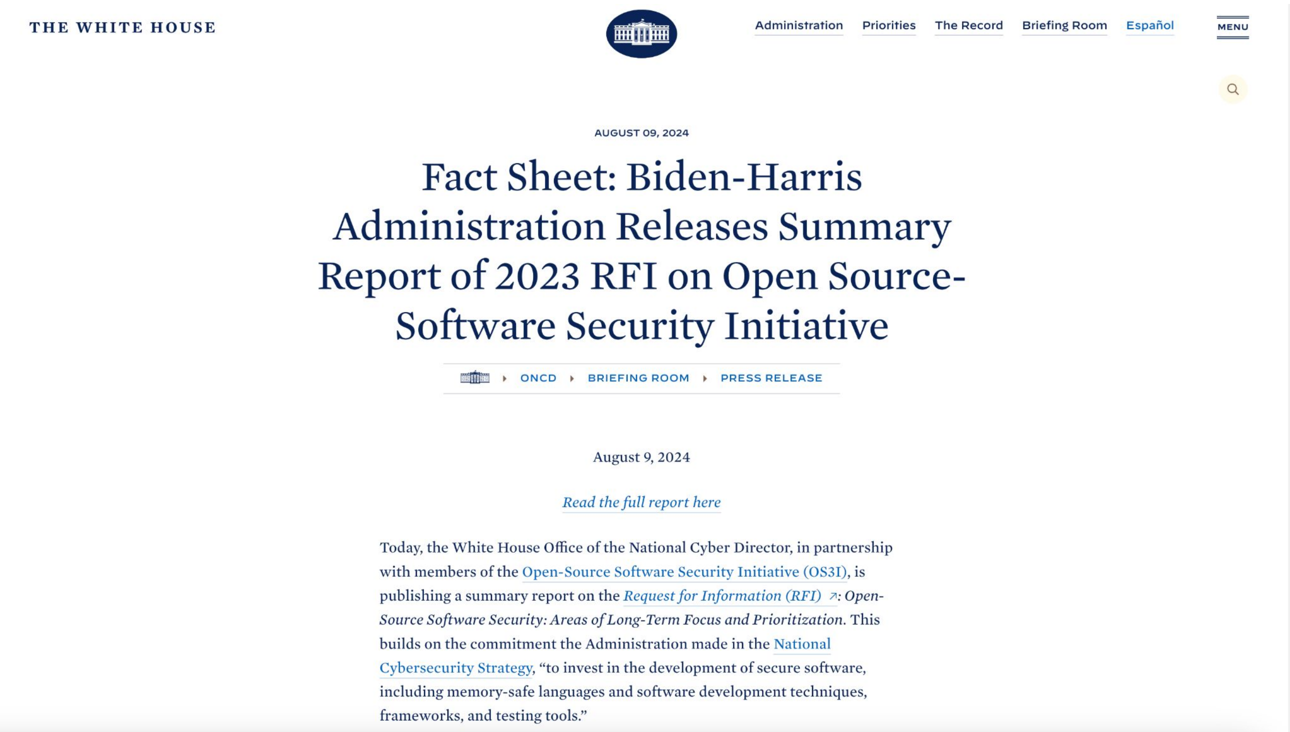
(2022)

https://data.cms.gov/fact-sheet/cms-fast-facts
https://www.cms.gov/files/document/2022-medicare-trustees-report.pdf

The First Federal OSPO: A Baseline Established

go.cms.gov/ospo

Biden-Harris Administration Releases End of Year Report on Open-Source Software Security Initiative (OS3I)



AUGUST 09, 2024

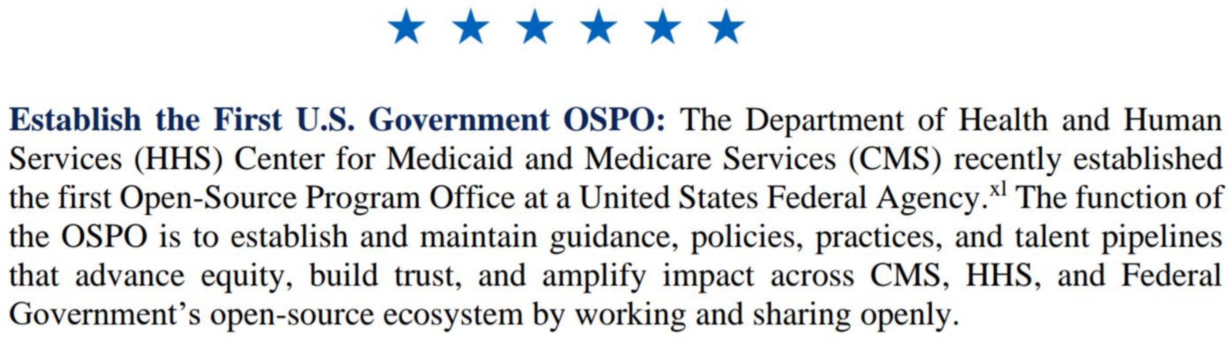
Fact Sheet: Biden-Harris Administration Releases Summary Report of 2023 RFI on Open Source-Software Security Initiative

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

August 9, 2024

Read the full report here

Today, the White House Office of the National Cyber Director, in partnership with members of the Open-Source Software Security Initiative (OS3I), is publishing a summary report on the *Request for Information (RFI)*: *Open-Source Software Security: Areas of Long-Term Focus and Prioritization*. This builds on the commitment the Administration made in the National Cybersecurity Strategy, "to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools."



Establish the First U.S. Government OSPO: The Department of Health and Human Services (HHS) Center for Medicaid and Medicare Services (CMS) recently established the first Open-Source Program Office at a United States Federal Agency.[xl] The function of the OSPO is to establish and maintain guidance, policies, practices, and talent pipelines that advance equity, build trust, and amplify impact across CMS, HHS, and Federal Government's open-source ecosystem by working and sharing openly.

SUMMARY OF THE 2023 REQUEST FOR INFORMATION ON OPEN-SOURCE SOFTWARE SECURITY

AUGUST 2024

THE WHITE HOUSE
WASHINGTON
DARPA
NSF
CISA
CMS.gov
Science and Technology
U.S. DEPARTMENT OF ENERGY
OPEN-SOURCE SOFTWARE SECURITY RFI SUMMARY
2

whitehouse.gov/wp-content/uploads/2024/08/Summary-of-the-2023-Request-for-Information-on-Open-Source-Software-Security.pdf

What is an Open Source Program Office? (OSPO)

An open source program office (OSPO) serves as the center of competency for an organization's open source operations and structure. It is responsible for defining and implementing ***strategies****,* ***programs****, and* ***policies*** *to guide these efforts***.**

CMS OSPO Functional Statement:

“Establishes and maintains guidance, policies, practices, and talent pipelines that ***advance equity****,* ***build trust****, and* ***amplify impact*** *across CMS, HHS, and Federal Open Source Ecosystems by working and sharing openly.”*

How do we “DO” Open Source at CMS?

Policies

How we **inbound** and **outbound** open source contributions and content

Projects

How we **solve real-world problems** by working in the open

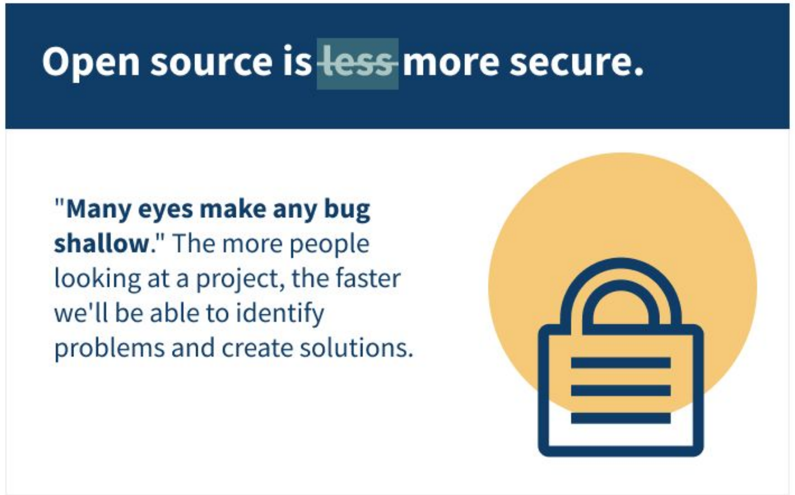
Programs

How we **measure**, and **manage** contributors, projects, **risks**, and **opportunities**

What are the Risks?
What are the Benefits?

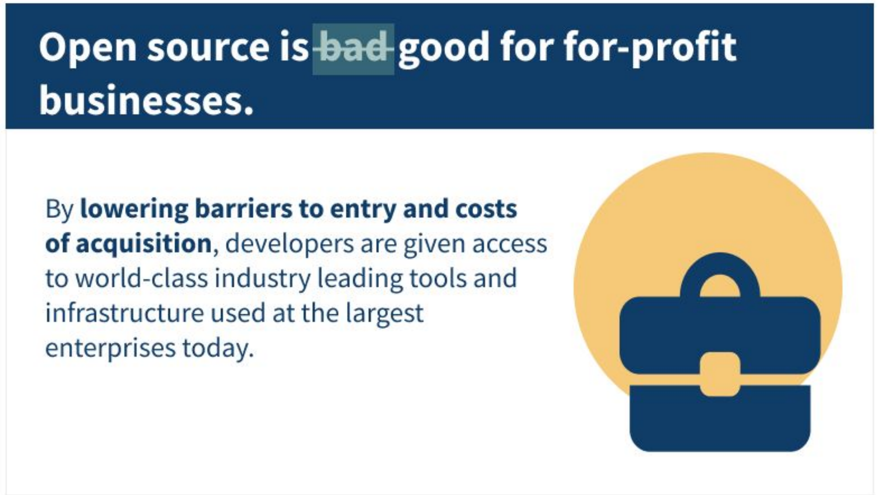
cms.gov/digital-service

“Risks” (aka Myths) of Open Source



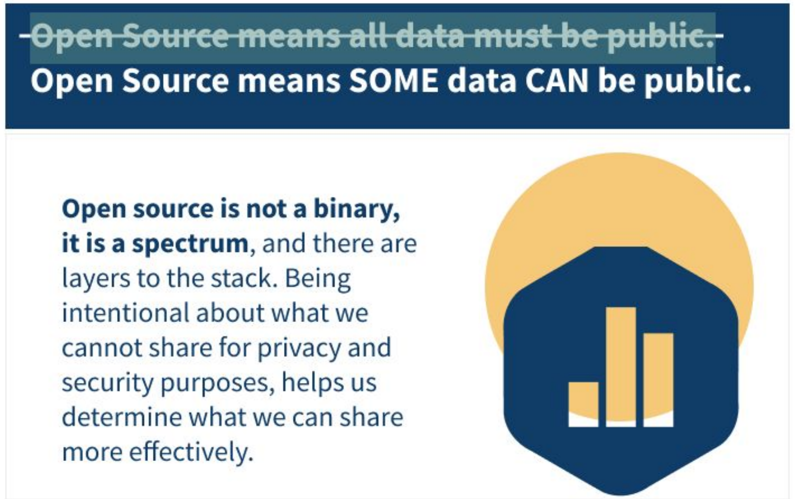
Open source is ~~less~~ more secure.

"**Many eyes make any bug shallow.**" The more people looking at a project, the faster we'll be able to identify problems and create solutions.



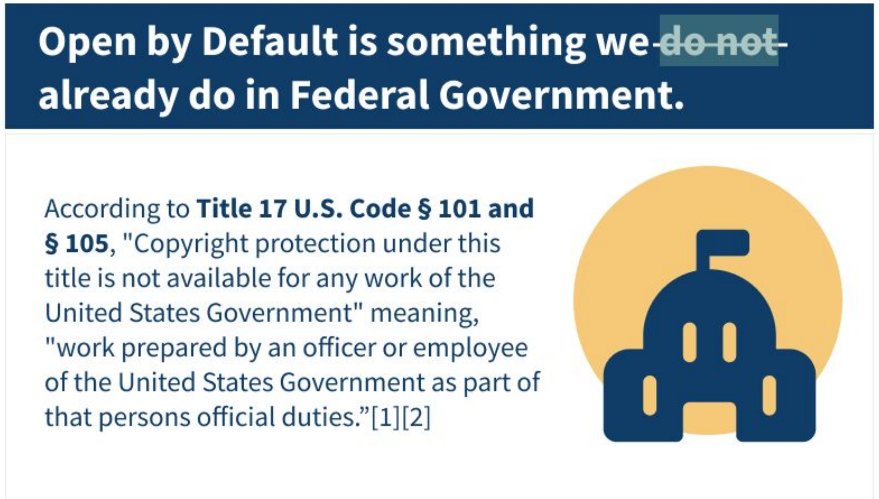
Open source is ~~bad~~ good for for-profit businesses.

By **lowering barriers to entry and costs of acquisition**, developers are given access to world-class industry leading tools and infrastructure used at the largest enterprises today.



~~Open Source means all data must be public.~~ Open Source means SOME data CAN be public.

Open source is not a binary, it is a spectrum, and there are layers to the stack. Being intentional about what we cannot share for privacy and security purposes, helps us determine what we can share more effectively.



Open by Default is something we ~~do not~~ already do in Federal Government.

According to **Title 17 U.S. Code § 101 and § 105**, "Copyright protection under this title is not available for any work of the United States Government" meaning, "work prepared by an officer or employee of the United States Government as part of that persons official duties.”[1][2]

https://www.law.cornell.edu/uscode/text/17
https://www.law.cornell.edu/uscode/text/17/105

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf

What are the *actual* Risks in Open Source?

Overdifferentiation

- Unnecessarily duplicating work
- Unnecessarily dividing your resources

Examples

- “Not Invented Here Syndrome”

Proliferation

- Unnecessarily duplicating communities and projects
- Unnecessarily dividing your addressable market

Examples

- License Proliferation
- Event/Conference Proliferation

Fragmentation

- Unnecessarily dividing your community of contributors

Examples

- Hostile Forks
- Internal Forks

How does our OSPO benefit the Agency?

Save us Money

Save us Time

Accountability for Contract Performance

Engine for Talent

Reduce Duplicate Work

Reduce Duplicate Costs

Reduce Security Risk

Reduce Continuity Risk

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf

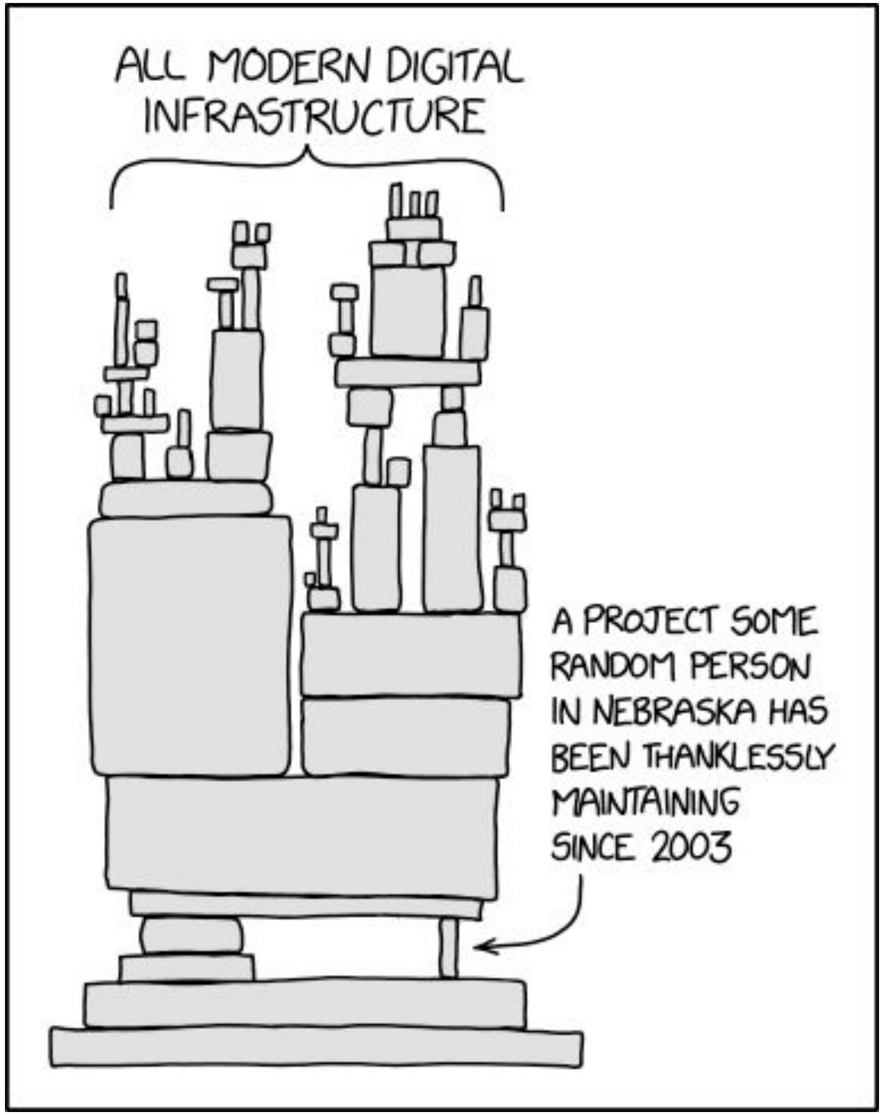
RISK: OSS Supply Chain Attacks

Thanks to XKCD, Open Source software supply chain vulnerabilities like those seen in the recent XZ vulnerability are being referred to as a “Nebraska problems” or, when a component of software that is critical to much of the world is inadequately funded, maintained, or staffed.

Stakeholders must pay attention to the critical projects that they depend on, and support programs that fund, hire, and train maintainers.

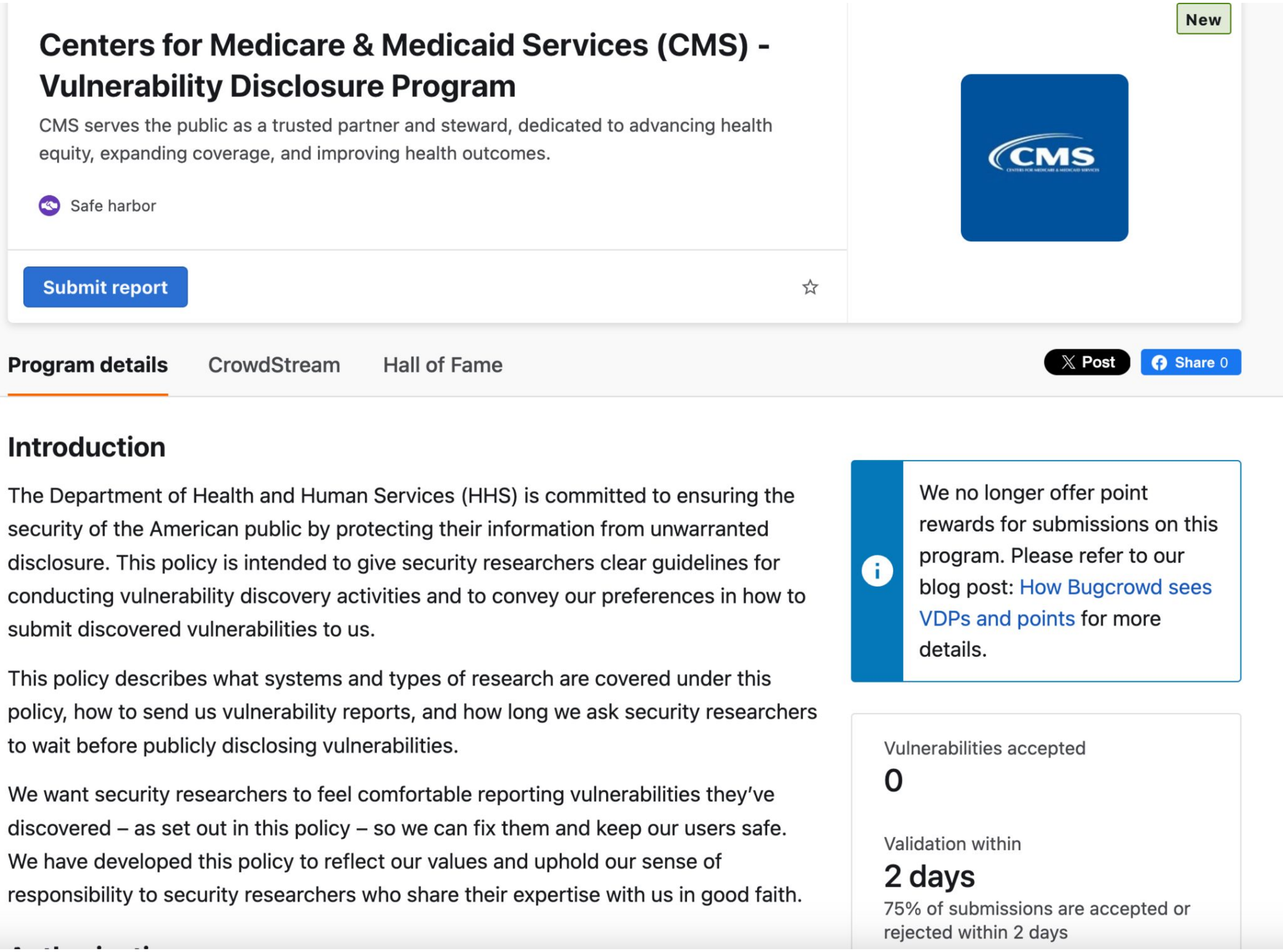
CISA writes on their blog that *“every technology manufacturer that profits from open source software must do their part by being responsible consumers of and sustainable contributors to the open source packages they depend on.”*

See: https://github.com/DSACMS/ospo-guide/blob/main/resources/XZ_Supply_chain_attack.md


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

https://xkcd.com/2347

BENEFIT: CMS Vulnerability Disclosure Program Partnership with CISA.gov



New

Centers for Medicare & Medicaid Services (CMS) - Vulnerability Disclosure Program

CMS serves the public as a trusted partner and steward, dedicated to advancing health equity, expanding coverage, and improving health outcomes.

Safe harbor

Submit report ☆

Program details | CrowdStream | Hall of Fame | Post | Share 0

Introduction

The Department of Health and Human Services (HHS) is committed to ensuring the security of the American public by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

We no longer offer point rewards for submissions on this program. Please refer to our blog post: How Bugcrowd sees VDPs and points for more details.

Vulnerabilities accepted
0

Validation within
2 days
75% of submissions are accepted or rejected within 2 days

bugcrowd.com/cms-vdp

Prerequisite to launching CMS' first ever Bugbounty Program!

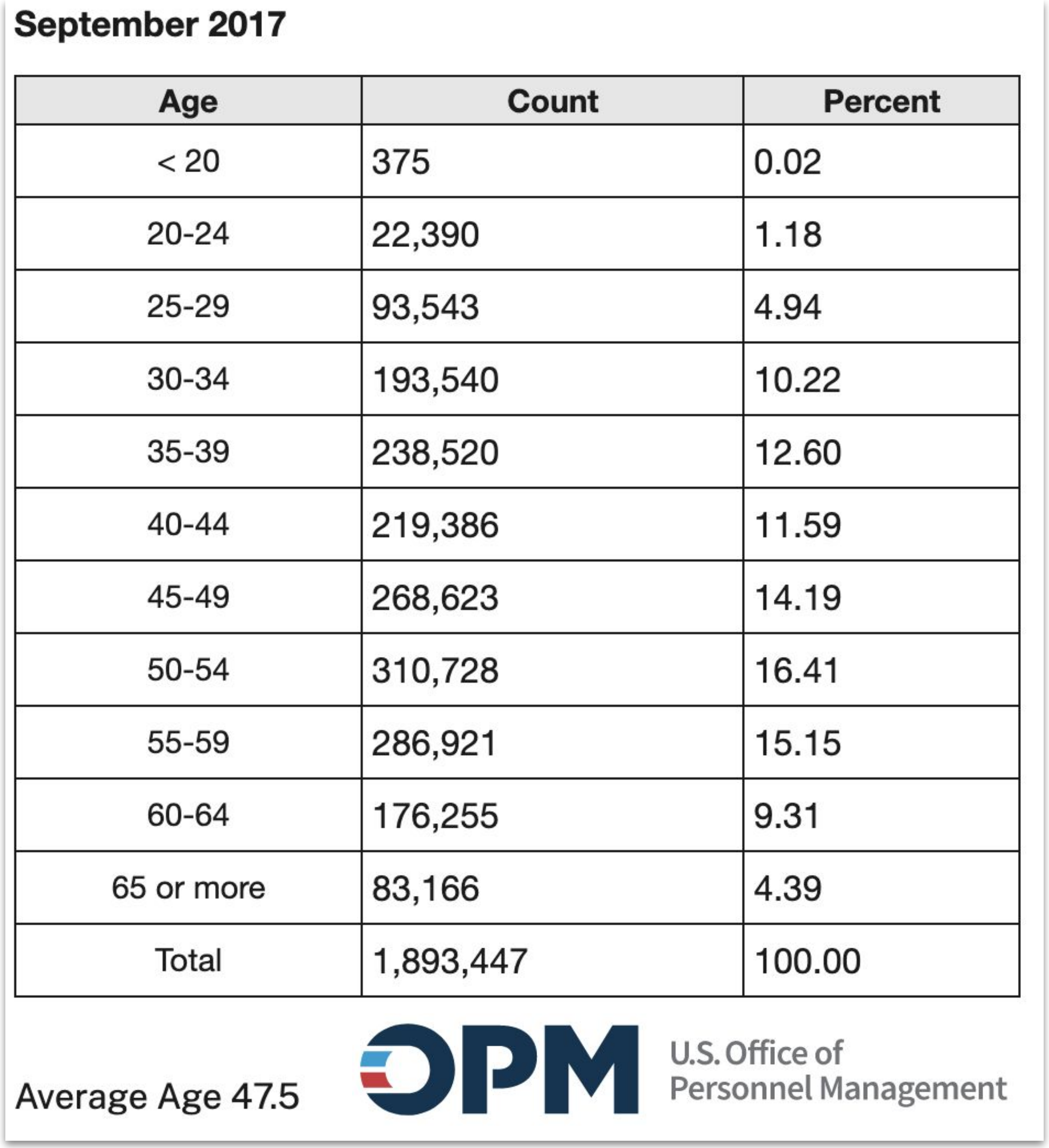
- Launched in Early October 2024
- $70K+ Bounty Pool funded!

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf

RISK: *For every* ***1*** *Federal Employee under the age of* **30**, *there are* ***7*** *over the age of* ***50*** **...**

The Federal Retirement Cliff

https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/full-time-permanent-age-distributions/



September 2017

Age	Count	Percent
< 20	375	0.02
20-24	22,390	1.18
25-29	93,543	4.94
30-34	193,540	10.22
35-39	238,520	12.60
40-44	219,386	11.59
45-49	268,623	14.19
50-54	310,728	16.41
55-59	286,921	15.15
60-64	176,255	9.31
65 or more	83,166	4.39
Total	1,893,447	100.00

Average Age 47.5

OPM U.S. Office of Personnel Management

BENEFIT: Early Career Talent Pipeline in Open Source

Digital Service at CMS.gov DIGITAL SERVICE AT CMS	**Up to 4 year tour of duty** for established professionals in **Engineering, Product management, Design, and Data science**. GS-13+	https://cms.gov/digital-service-cms
DigitalCorps at GSA.gov UNITED STATES DIGITAL CORPS	**2 year tour of duty** for **early-career** technologists, eligible to convert to full-time, career positions in the competitive service at their agency. GS-9 to 12, + **50% recruitment Incentive**.	https://digitalcorps.gsa.gov
Summer Fellowship at CodingItForward.com coding it forward >	**Paid 10 week summer internship** program for **currently enrolled** undergrad, grad, bootcamp students **or recent graduates**.	https://www.codingitforward.com
Internships at CodeInTheSchools.org	**Paid 5-10 week summer experience** for **Baltimore City residents** between the ages of **14 and 21**, with YouthWorks Summer Jobs Program, managed by Mayor's Office of Employment Development.	https://codeintheschools.org

Thank You Nava OSS Summit!

creative commons

PUBLIC DOMAIN

Questions or Comments?

https://go.cms.gov/ospo

https://github.com/DSACMS/decks/blob/main/navaosssummit2024.pdf

Open Source Questions?
opensource@cms.hhs.gov

Digital Service Questions?
DigitalService@cms.hhs.gov

Help Answer The Call!

Digital Service at CMS.gov
https://cms.gov/digital-service

DigitalCorps Fellowships
https://digitalcorps.gsa.gov

CodingItForward Summer Internships
https://codingitforward.com