hackerone

February 2, 2024

William F. Clark
Director, Office of Government-wide Acquisition Policy
General Services Administration
1800 F Street NW
Washington, DC 20405

VIA ELECTRONIC SUBMISSION

Re: Comments in response to FAR Case 2021-019

Dear Mr. Clark,

HackerOne Inc. (HackerOne) submits the following comments in response to the Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration's (NASA) proposed rule to the Federal Acquisition Regulation (FAR) "Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems" (FAR Case 2021-019). HackerOne appreciates the opportunity to provide input, and we commend the Government for its openness and commitment to working with industry stakeholders to update cybersecurity provisions in the FAR.

HackerOne is the global leader in human-powered security. We leverage human ingenuity to pinpoint the most critical security flaws across your attack surface to outmatch cybercriminals. HackerOne's Attack Resistance Platform combines the most creative human intelligence with the latest artificial intelligence to reduce threat exposure at all stages of the software development lifecycle. From meeting compliance requirements with pentesting to finding novel and elusive vulnerabilities through bug bounty, HackerOne's elite community of ethical hackers helps organizations transform their businesses with confidence. HackerOne has helped find and fix more vulnerabilities than any other vendor for brands including Coinbase, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, and the U.S Department of Defense. In 2023, HackerOne was named a Best Workplace for Innovators by Fast Company.

Threat Hunting, Vulnerability Assessments, Bug Bounty Programs, and Vulnerability Disclosure Policies

In the proposed rule, the Government "requires a contractor that develops, implements, operates, or maintains a Federal Information System (FIS) using non-cloud computing services and that FIS is designated as a moderate or high FIPS Publication 199 impact" to 1) conduct annually a cyber threat hunting and vulnerability assessment to search for vulnerabilities, risks,

and indicators of compromise; and 2) perform to an annual, independent assessment of the security of each FIS."[1]

As a global leader in implementing and managing tailored programs for protecting governments and organizations from the most sophisticated adversaries, HackerOne understands how important threat hunting and vulnerability assessment programs are for protecting sensitive information. To ensure that FIS are effectively protected, we recommend that the Government state that the use of bug bounty programs (BBPs) meets the requirements of the annual vulnerability assessment.

By implementing bug bounty programs as part of a holistic security program, organizations can benefit from the experience of the global ethical hacker community and test the security of their most important systems. BBPs are a continuous security test that rewards ethical hackers for finding vulnerabilities and payment is made only when an in-scope vulnerability is found.

Bug bounty programs also hold a competitive advantage over automated vulnerability scanning to protect sensitive information. While automated scanning capabilities are useful tools, they can generate false positives that limited security staff must investigate. Leveraging human professionals to identify vulnerabilities better simulates real attack conditions and can provide an in-depth assessment of the organization's exposures and defenses.

Additionally HackerOne recommends that all federal contractors providing or operating FISs using cloud or non-cloud services be required to implement Vulnerability Disclosure Policies (VDPs), consistent with the National Institute of Standards and Technology SP 800-216 guidance on VDPs.[2] VDPs play an essential role in ensuring that software and systems owners and operators are aware of vulnerabilities. This awareness ensures that vulnerabilities are mitigated and that sensitive information remains confidential.

Incorporating VDPs into FAR Case 2021-019 would not create an undue burden on organizations. As noted in NIST's SP 800-53r5, "vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports."[3] In comparison to other practices required in the FAR, VDPs are not especially complex or resource-intensive. In fact, the Office of Management and Budget stated that VDPs "are among the most effective [cybersecurity] methods" and "provide high return on investment."[4]

---

[1] https://www.govinfo.gov/content/pkg/FR-2023-10-03/pdf/2023-21327.pdf
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf
[3] NIST, SP 800-53 Rev. 5, pg. 243, Sep. 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[4] OMB Memo 20-32, Improving Vulnerability Identification, Management, and Remediation, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

hackerone

Access to Contractor Systems

The proposed rule would allow the Government to gain "full access" to federal contractor systems after a cybersecurity incident. Clause 52.239–ZZ(a) scopes "full access" to include "other infrastructure housed on the same computer network," and "other infrastructure with a shared identity boundary or interconnection to the Government system." This broad definition would allow the Government access to nearly all of a federal contractor's systems.

Not only is this definition unnecessarily broad, it has the potential to expose data and information from the contractor's non-federal customers. This data may be subject to contractual requirements prohibiting its disclosure. Non-federal customers may be reluctant to continue working with federal contractors, potentially forcing federal contractors to choose between selling to non-federal customers or the Government.

HackerOne recommends that the Government remove the provision allowing for "full access" to federal contractor systems. However, if the Government insists on including a provision permitting access to contractor systems, it should at least define specific criteria, tied to incident severity and impact to Government data or operations, and limit access to only federal Government data, defining when the Government can request access to federal contractor systems.

Conclusion

HackerOne appreciates the opportunity to provide comments on this proposed rule. We look forward to continued engagement with policymakers on these issues and are happy to discuss our response at any time.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne