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 2021-017

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 amend the Federal Acquisition Regulation (FAR) to "implement an Executive order on cyber threats and incident reporting and information sharing for Federal contractors and to implement related cybersecurity policies" (FAR Case 2021-017). 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

Vulnerability Disclosure Policies

In the proposed rule, the agencies ask "what is the appropriate balance between the Government and the contractor, when monitoring SBOMs for embedded software vulnerabilities as they are discovered?" HackerOne believes that software producers should take steps to actively identify and mitigate vulnerabilities in their software. Once mitigated, those vulnerabilities should be disclosed to customers, including the federal Government.

To assist contractors in the identification of vulnerabilities, HackerOne recommends that the Government require all federal contractors and software producers to implement Vulnerability Disclosure Policies (VDPs), consistent with the National Institute of Standards and Technology SP 800-216 guidance on VDPs,[1] as part of the risk management programs required by FAR Case 2021-017. VDPs play an essential role in ensuring that software and systems owners and operators are aware of vulnerabilities. This awareness allows software producers to establish mitigations for vulnerabilities before they can be exploited. Congress recognized the value of VDPs when it established a prohibition on agencies from using Internet of Things devices obtained from a contractor that does not have a VDP in place.[2]

Incorporating VDPs into FAR Case 2021-017 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]

Incident Reporting Requirements

The proposed rule would require federal contractors to report cybersecurity incidents within "eight hours of discovery" and to "update the submission every 72 hours thereafter" until remediation activities are completed.

HackerOne believes that these reporting requirements create an unnecessary burden for contractors without providing a commensurate amount of value to enhance cybersecurity. The requirement to update reports every 72-hours regardless of whether there has been any update to the status of the incident, is at best a nuisance and may disrupt the contractor's response and recovery efforts. Therefore, HackerOne recommends that the Government narrow this requirement to updates solely "when material changes occur."

HackerOne also believes that the requirement to report "within 8 hours of discovery that a security incident may have occurred" is unreasonable. Reporting to the Government that an incident "may have occurred" is overly burdensome and will result in an overwhelming number of false positives. Each of false positives will distract both contract and Government resources from focusing on higher priority cybersecurity issues. HackerOne believes the Government should adopt the approach established in the Cyber Incident Reporting for Critical Infrastructure

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf
[2] https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.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

Act. That law requires reporting "72 hours after confirmation that a covered cybersecurity incident has occurred."[5]

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

[5] https://www.congress.gov/117/bills/hr5440/BILLS-117hr5440ih.pdf