24 May 2024

Senator Mark Warner
United States Senate
Chairman, Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

Arm
120 Rose Orchard Way
San Jose, CA
95134-1358

T 408-576-1500
arm.com

Re: Response to Letter on Election Security

Dear Chairman Warner,

Thank you for your letter dated 14 May, 2024 regarding Arm's work to advance election integrity and Arm's joining the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections* announced during the 2024 Munich Security Conference.

As we've discussed, Arm develops intellectual property in the form of computer architecture, central processing units (CPUs), graphics processing units (GPUs), neural processing units (NPUs), and related technology that is used to develop semiconductor designs and ultimately physical chips. Given this position in the supply chain, Arm has significant influence to develop and enable security features to protect against some of the most widely utilized vulnerabilities against computer hardware. This is a position which Arm takes incredibly seriously. Arm has worked for decades to increase the security of its products, and in 2021 released the Arm Security Manifesto, challenging ourselves and the industry to do more in this area.[1] Arm has worked to develop a holistic approach to providing technologies that protect against entire classes of known attacks and vulnerabilities.[2]

Specifically to your questions, Arm does not offer social media, content creation, or related consumer facing technology or platforms. That said, Arm was a founding member of the Coalition for Content Provenance and Authenticity ("C2PA").[3] The C2PA is the leading organization developing standards and specification that are used to convey the provenance of digital media content. The role Arm's technology provides in this process is encryption during digital content creation to convey provenance information; that information is cryptographically protected, and alteration or manipulation of the digital content is captured and visible in that encrypted information chain. These tools can significantly reduce the ability of digital content to be used for disinformation and misinformation. The C2PA engages with governments to educate them on the availability of the technology, its use on various platforms, and its applicability to areas like election integrity. Further, the C2PA has worked with organizations like the Center for Strategic and International Studies to raise awareness of the importance of content provenance and the tools being developed.[4]

---

[1] See https://newsroom.arm.com/blog/the-2021-arm-security-manifesto
[2] See https://www.arm.com/architecture/security-features
[3] See https://c2pa.org/
[4] See https://www.csis.org/events/we-hold-these-truths-how-verified-content-defends-democracies

Arm
120 Rose Orchard Way
San Jose, CA
95134-1358

T 408-576-1500
arm.com

Arm was also a founding member of the Cybersecurity Tech Accord in 2018, which has grown from 30 to more than 100 companies, working together and with external stakeholders and governments to protect online users and strengthen cybersecurity protections. As you stated, there is "an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press." The Cybersecurity Tech Accord exists to engage and work with governments and related entities to protect trust in online platforms and technology. As an example, the CTA has engaged the United Nations[5], the European Union[6], and various other government entities to improve cybersecurity and online trust.

While Arm does not directly operate in the social media or online platform space, Arm's customers use our IP and technology to create a wide range of products and applications that feed into these areas from artificial intelligence and content creation on client and mobile devices, to cloud and web services in the data center. Because of the breadth and scale of Arm's technology, we take that responsibility incredibly seriously and work closely with our customers to ensure we are delivering security features that enable them to build secure products, address evolving threats, and maintain and build trust in digital technology. This is a constant and evolving challenge that can only be addressed through collective action amongst industry, governments, and other trusted parties.

Digital security will continue to be a top priority for Arm, and we will gladly work with you and your colleagues to provide additional information on these efforts, and advance policies and work that creates a more secure and trusted digital experience.

Respectfully,

Rene Haas
Chief Executive Officer
Arm

[5] See https://cybertechaccord.org/responsible-state-behaviour-in-cyberspace-calling-for-a-new-norm-on-ict-supply-chain/
[6] See https://cybertechaccord.org/eus-network-and-information-system-directive-nis-2-can-restore-access-to-critical-whois-data/