

Notice of Exempt Solicitation

Name of Registrant: Microchip Technology Incorporated Shareholders

Name of Person relying on exemption: Rob Fohr, Presbyterian Church, U.S.A.

Address of Person relying on exemption: 100 Witherspoon St, Louisville, KY 40202

Written materials are submitted pursuant to Rule 14(a)-6(g)(1) promulgated under the Securities and Exchange Act of 1934.

Dear Fellow Microchip Shareholder,

The Presbyterian Foundation filed Proxy Item No. 7 on Microchip Technology Incorporated's ("Microchip's" or the "Company's") proxy card, "Stockholder proposal requesting that our board of directors commission an independent third-party report, at reasonable expense and excluding proprietary information, on our due diligence process to determine whether our customers' use of our products contribute or are linked to violations of international law" (the "Proposal"). The proposal will be voted on at the August 22nd Annual Meeting of Microchip.

Rationale for a FOR Vote:

1. Microchip's components and operations may be connected to end-users' violations of international law in conflict-affected and high-risk areas (CAHRA), creating potential financially material risks – ethical, regulatory, and reputational – for shareholders.
2. Presently available information regarding Microchip's policies and procedures for Know Your Customer (KYC) due diligence, heightened human rights due diligence (hHRDD), and export and sanction controls is insufficient.
3. The proposal does not request complete traceability but seeks to understand Microchip's policies and procedures for the company's KYC due diligence, hHRDD, and export and sanction controls.
4. Microchip's efforts to address human rights- and conflict-related risks in its value chain lag behind industry peers.
5. The proposal's requests will protect the interests of Microchip's shareholders.

The Proposal

Resolved:

Shareholders request that the Board of Directors commission an independent third-party report, at reasonable expense and excluding proprietary information, on Microchip's due diligence process to determine whether its customers' use of its products contribute or are linked to violations of international law.

The proposal requests an independent third-party report regarding Microchip's due diligence in order to protect investors' long-term interests. Microchip's policies and procedures for Know Your Customer (KYC) due diligence, heightened human rights due diligence (hHRDD) for conflict-affected and high-risk areas (CAHRA), and sanctions and export controls may not be sufficient to prevent Microchip's products from being connected to violations of U.S. regulatory regimes and international law. Furthermore, publicly available information regarding these procedures is inadequate and the proposal's requests are not overly burdensome, do not call for complete traceability and 100% prevention or misuse, nor are they disproportionate based on the present and increasing risks.

Microchip's components and operations may be connected to end-users' violations of international law in conflict-affected and high-risk areas (CAHRA), creating potential financially material risks – ethical, regulatory, and reputational – for shareholders.

Microchip's commercial, dual-use, and military components have been implicated in military systems deployed in CAHRA, some of which have been connected to violations of international humanitarian law (IHL). Under U.S. export regulations, Microchip is restricted from selling its components to prohibited end-users or for a prohibited end-use, which includes embargoed countries, certain military actors, and types of military-use.¹

According to the Royal United Services Institute's (RUSI) Report, *Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine*, Microchip's products were among the most prevalent in the 208 dual-use components recovered from 26 Russian weapons systems, including the Iskander 9M727 and the KH-101 ballistic and cruise missile systems.² Investigations also found Microchip's products in other weapons systems recovered from the Ukrainian battlefield, including Russian and Iranian drones,³ Russian T-72 tanks,⁴ and the Orlan-10 drone.⁵ Several types of these drones have been used by the Russian military to target Ukrainian civilians and civilian infrastructure in violation of IHL.⁶ Furthermore, the human costs of the use of Russian and Iranian weapons systems have been widespread and severe with the Ukrainian government currently investigating over 70,000 crimes of aggression and war crimes.⁷ These findings have been reported in an array of mainstream media organizations, including *Wall Street Journal*, *Financial Times*, *The New York Times*, *The Washington Post*, and CNN, creating an expanding environment of reputational risk for the company.

¹ Code of Federal Regulations (CFR) Part 744.

² James Byrne, Gary Somerville, Joseph Byrne, Jack Watling, Nick Reynolds, and Jane Baker, "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," *Royal United Services Institute*, August 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (accessed June 20, 2023).

³ Dave Ross, "Ross: Drones used in Ukraine invasion use western chips," *Kiro News Radio*, January 5, 2023, <https://mynorthwest.com/3769594/ross-drones-used-in-ukraine-invasion-use-western-chips/> (accessed June 20, 2023).

⁴ Anton Mykytiuk, "How foreign microchips end up in Russian tanks despite sanctions," *Euromaidan Press*, September 28, 2022, <https://euromaidanpress.com/2022/09/28/how-foreign-microchips-end-up-in-russian-tanks-despite-sanctions/> (accessed June 20, 2023).

⁵ Maria Zholobova, Stephen Gray, and Maurice Tamman, "The West has banned the sale of components for the production of weapons to Russia. But she successfully buys them," *The Independent*, December 15, 2022, <https://storage.googleapis.com/istories/stories/2022/12/15/zapad-zapretit-prodavati-rossii-komplektuyushchie-dlya-proizvodstva-oruzhiya-no-ona-ikh-uspeshno-pokupaet/index.html> (accessed June 20, 2023).

⁶ Alisha Rahaman Sarkar, "US claims Iran-made 'kamikaze' drones used by Russia to bomb Ukraine breach international law," *The Independent*, October 18, 2022, <https://www.independent.co.uk/news/world/americas/us-kamikaze-drone-ukraine-russia-b2204841.html> (accessed June 20, 2023).

⁷ Офіційний твіттер Офісу Генерального прокурора / Prosecutor General's Office of Ukraine, Official Twitter [@GP_Ukraine] (2023, February 24) #RussianWarCrimes statistics for the past week: February 17 - 24, 2023. 1 141 new crimes registered. At least 461 children killed, 927 injured (the data without full consideration of places of active hostilities) [Tweet]. Twitter. https://twitter.com/GP_Ukraine/status/1629144987207184384 (accessed June 20, 2023).

In its *Opposition Statement*, Microchip highlights how semiconductor components found in military weapons could have been taken from commercial devices, transferred through multiple parties, or significantly dated. While this is an accurate depiction of the challenges in maintaining effective compliance procedures in this industry, missile systems found in Ukraine included Microchip components classified as dual-use and manufactured in the summer and fall of 2022.⁸ This finding indicates western components may still be being diverted to Russian entities despite sanctions⁹, as reaffirmed in the July 21 segment on *PBS News Hour*; “Parts made by U.S. companies used to build Russian cruise missiles.”¹⁰

Presently available information regarding Microchip’s policies and procedures for KYC due diligence, hHRDD, and export and sanction controls is insufficient.

Microchip’s *Opposition Statement* describes how its “trade control policies and procedures address the review of our supply chain, our customers, distributors, and transactions.” It further directs investors to the company website to find more information. Filer acknowledges that on July 7, 2023, Microchip released a statement¹¹ describing a limited number of the steps and tools used by the company to mitigate the risks associated with its customers and distributors use of its products. While we recognize this as a positive step towards improved disclosure, the purpose of the proposal is to analyze the sufficiency of Microchip’s policies and procedures. Further, the disclosure’s vague references to a base-line and already legally-required compliance program does not provide sufficient information for shareholders to determine if Microchip’s KYC, hHRDD, and regulatory compliance processes adequately address increased geopolitical conflict, product diversion by authoritarian regimes, and product misuse in violations of international law.

Given the recent investigations that have found dozens of Microchip’s unique components in Russian and Iranian weapons systems, ensuring the company’s processes are sufficiently robust is essential to protecting investors’ interests, especially in light of rapidly evolving regulatory, legal, reputational, and financial risks.¹² Furthermore, this proposal seeks a third-party expert to analyze these policies, procedures, and outcomes as opposed to relying on Microchip’s board, which lacks membership with adequate human rights or conflict risk experience.¹³

Filer’s proposal does not request complete traceability but seeks to understand Microchip’s policies and procedures for the company’s KYC due diligence, hHRDD, and export and sanction controls.

To support its contention that the proposal is not in the best interest of investors, Microchip’s *Opposition Statement* argues that complete supply chain traceability is impossible. In fact, Microchip’s statement goes into great detail regarding the complexity of its operations and industry challenges.

⁸ John Ismay, “Russian Cruise Missiles Were Made Just Months Ago Despite Sanctions,” *New York Times*, December 5, 2022, <https://www.nytimes.com/2022/12/05/us/politics/cruise-missiles-russia-ukraine-sanctions.html> (accessed June 20, 2023).

⁹ Anton Mykytiuk, “How foreign microchips end up in Russian tanks despite sanctions,” *Euromaidan Press*, September 28, 2022, <https://euromaidanpress.com/2022/09/28/how-foreign-microchips-end-up-in-russian-tanks-despite-sanctions/> (accessed June 20, 2023).

¹⁰ Simon Ostrovsky, “Parts made by U.S. companies used to build Russian cruise missiles,” *PBS News Hour*, July 21, 2023, <https://www.pbs.org/newshour/show/parts-made-by-u-s-companies-used-to-build-russian-cruise-missiles> (accessed July 22, 2023).

¹¹ Microchip, “Position on Russia and Trade Controls,” July 7, 2023 <https://www1.microchip.com/downloads/aemDocuments/documents/announcements/microchip-position-on-russia-and-trade-controls.pdf> (accessed July 20, 2023).

¹² Ibid; “American CPUs found in Iran-made Kamikaze drones,” *Ukrainska Pravda*, September 26, 2022, <https://www.yahoo.com/video/american-cpus-found-iran-made-122325552.html> (accessed June 20, 2023).

¹³ Microchip, “Leadership,” <https://www.microchip.com/en-us/about/investors/investor-information/leadership> (accessed June 20, 2023).

However, the proposal does not request Microchip attempt to achieve “complete traceability of standard semiconductor products to every end use and 100% prevention” of product misuse. Filer recognizes the dual-use nature of semiconductor components, the industry’s reliance on retail markets and third-party distributors, and the long lifespan of chips that makes tracking the end-users of thousands of different products to over 125,000 customers practically unfeasible. Filer is instead requesting Microchip take the appropriate steps to ensure its KYC due diligence, hHRDD, and other regulatory compliance are effective in light of the recent, widespread, and detailed reporting that has directly connected Microchip’s components to prohibited end-users and uses that constitute violations of international law.

For example, recent reporting discovered Microchip has supplied high-risk importers, such as ZAO Radiotekhnokomplekt (RTKT), a company with a long history of supplying the Russian military, with the precise types of semiconductors at risk of prohibited end-user and uses.¹⁴ Further, in November 2022, the U.S. Department of Commerce’s Bureau of Industry and Security launched an investigation after American components were found in downed Iranian drones, including products from Microchip.¹⁵ Iranian Shahed-136 “kamikaze” and other drones have been used by the Russian military to target Ukrainian civilians and civilian infrastructure in violation of international law.¹⁶ The fact that non-profit organizations with far fewer resources, such as RUSI, are able to trace dual-use Microchip semiconductors from point of manufacture to point of end use suggests that the company can and should do more regarding the chain of custody of its products.

Microchip’s efforts to address human rights- and conflict-related risks in its value chain lag behind industry peers

While Microchip’s website includes references to human rights considerations, such as a human rights policy, its peers in the semiconductor industry are taking proactive steps to better integrate human rights due diligence across organizational departments.

For example, Qualcomm, a similarly situated American semiconductor company, has implemented a Human Rights Working Group that is “composed of representatives from legal; procurement; corporate responsibility; government affairs; environmental, health and safety; diversity and inclusion; supply chain; ethics and compliance; and privacy and security.” The working group reports regularly to senior management and the Board of Directors, indicating that human rights is considered a governance priority. Further, the company notes that it regularly conducts, “human rights impact assessments, including company-wide and within certain regions,” and materiality assessments that identified “product misuse” as a salient human rights risk.

¹⁴ James Byrne, Gary Somerville, Joseph Byrne, Jack Watling, Nick Reynolds, and Jane Baker, “Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine,” *Royal United Services Institute*, August 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (accessed June 20, 2023).

¹⁵ Inder Singh Bisht, “US Orders Probe After Western Components Found in Iranian Drones: Report,” *The Defense Post*, November 17, 2022, <https://www.thedefensepost.com/2022/11/17/western-components-iranian-drones/> (accessed June 20, 2023).

¹⁶ Alisha Rahaman Sarkar, “US claims Iran-made ‘kamikaze’ drones used by Russia to bomb Ukraine breach international law,” *The Independent*, October 18, 2022, <https://www.independent.co.uk/news/world/americas/us-kamikaze-drone-ukraine-russia-b2204841.html> (accessed June 20, 2023).

Similarly, Intel, another leader in the American semiconductor space, has multiple teams, including a cross functional human rights steering committee, that are responsible for conducting due diligence and implementing policies and procedures to address salient human rights risks and support adherence to its human rights policy. Under “Product Responsibility,” Intel notes that, “Where we become aware of a concern that Intel products are being used by a business partner in connection with abuses of human rights, we will restrict or cease business with the third party until and unless we have high confidence that Intel’s products are not being used to violate human rights.”

The limited information Microchip has disclosed regarding its human rights practices indicates Microchip has not prioritized human rights and/or conflict related risks to the same extent as its peers and may be falling behind industry standards.

In Microchip’s *Opposition Statement*, the company further argues that disclosing the information requested by the Proposal will further facilitate bad actors in circumventing Microchip’s compliance measures. However, Filers are not requesting Microchip disclose the complete contours of its compliance systems so as to put the company at risk of greater proximity to prohibited end uses, users, or violations of international law. To this point, Microchip’s industry peers have provided robust disclosures of its human rights and other compliance practices without indicating a negative outcome.

The proposal’s requests will protect the interests of Microchip’s shareholders.

Filer believes understanding Microchip’s proximity to human rights and conflict-related risk is material to protecting the value of their assets as more evidence regarding the financial impact of proximity to human rights abuses and violations of international law becomes available. Furthermore, Filers are not alone in prioritizing these issues. Investors representing over \$11 trillion assets under management signed public statements concerning these risks in Ukraine,¹⁷ Myanmar,¹⁸ and Xinjiang Autonomous Region, China.¹⁹ Similarly, “conflict risk” is now the second leading environmental, social, and governance (ESG) criteria among institutional investors, according to The Forum for Sustainable and Responsible Investment’s 2022 *Report on US Sustainable, Responsible and Impact Investing Trends*.²⁰

Finally, as opposed to Microchip’s contention in its *Opposition Statement*, the proposal does not seek to micromanage the company’s business or impose an unproductive administrative burden as it seeks non-proprietary information at a reasonable expense. In fact, the proposal specifically seeks a third-party to conduct the review and draft the report in an effort to obtain an expert opinion and will therefore require limited resources from company management.

¹⁷ “Investor Statement on the Crisis in Ukraine,” Business & Human Rights Resource Centre, May 16, 2022, https://media.business-humanrights.org/media/documents/Investor_Statement_on_the_Crisis_in_Ukraine_16_May_2022.pdf (accessed June 20, 2023).

¹⁸ “Investor Statement on Human Rights and Business Activities in Myanmar,” Business & Human Rights Resource Centre, June 9, 2021, <https://www.business-humanrights.org/en/latest-news/investor-statement-on-human-rights-and-business-activities-in-myanmar/> (accessed June 20, 2023).

¹⁹ “Investor Expectations on Human Rights Crisis in the Xinjiang Uyghur Autonomous Region,” *Investor Alliance for Human Rights*, April 2022, <https://investorsforhumanrights.org/sites/default/files/attachments/2022-04/XUAR%20Investor%20Expectations%20Statement%20-%20April%202022.pdf> (accessed June 20, 2023).

²⁰ “Report on US Sustainable, Responsible and Impact Investing Trends,” *US SIF Foundation*, 2022, <https://www.ussif.org/Files/Trends/2022/Institutional%20Investors%202022.pdf>, (accessed on June 20, 2023).

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, EMAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY ONE OR MORE OF THE CO-FILERS. PROXY CARDS WILL NOT BE ACCEPTED BY ANY CO-FILER. PLEASE DO NOT SEND YOUR PROXY TO ANY CO-FILER. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.