ITEM 1B. UNRESOLVED STAFF COMMENTS

We have received no written comments regarding our periodic or current reports from the staff of the Securities and Exchange Commission that were issued 180 days or more preceding the end of our fiscal year 2024 that remain unresolved.

ITEM 1C. CYBERSECURITY

RISK MANAGEMENT AND STRATEGY

Microsoft plays a central role in the world's digital ecosystem. We have made it the top corporate priority to protect the computing environment used by our customers and employees and to support the resiliency of our cloud infrastructure and services, products, devices, and our internal corporate resources from determined adversaries. In response to the evolving cybersecurity threat landscape, we launched the Secure Future Initiative ("SFI") in November 2023 and expanded the scope of SFI in May 2024. The SFI focuses our business strategy and efforts on continual improvement in cybersecurity protection, and is aligned around three security principles:

- **Secure by Design:** Security comes first when designing any product or service.
- **Secure by Default:** Security protections are enabled and enforced by default, require no extra effort, and are not optional.
- **Secure Operations:** Security controls and monitoring will continuously be improved to meet current and future threats.

We operate a cybersecurity program and governance framework designed to protect our computing environments against cybersecurity threats, and we have controls, policies, and procedures to identify, manage, and mitigate cybersecurity threats. Annually, we assess our cybersecurity program's alignment with the National Institute of Standards & Technology's Cyber Security Framework ("NIST") and other applicable industry standards. We also undertake integrated planning and preparedness activities to support business continuity and operational resiliency. We assess our program's effectiveness through various exercises, including tabletop simulations and production environment tests, penetration and vulnerability tests, red team exercises, and other related activities. We conduct mandatory cybersecurity training, provide employees with tools to report suspected incidents and assess their own security posture, and conduct real-time simulated employee education exercises, such as phishing email campaigns designed to emulate real-world attacks. We also engage in robust cybersecurity assessments and remediation efforts for acquired companies.

Our computing environments, products, and services are reviewed by our internal audit teams as well as independent third-party assessors. We are committed to managing the most significant risks to our strategies and ambitions, including cybersecurity risks. The Enterprise Risk Management ("ERM") organization supports management in this commitment by facilitating the semiannual risk assessment, which documents the priority and status of these risks and aligns them with our strategic mitigation efforts. ERM is structured using a framework based on the Committee of Sponsoring Organization ("COSO") guidance on Enterprise Risk Management Integrating Strategy with Performance and it also aligns with the International Organization for Standardization 31000:2018 Risk Management Standard.

We continuously monitor our computing environments, products, and services for vulnerabilities and signs of compromise, and we utilize our own security products to combat cybersecurity threats. We integrate security into our computing environments, products, and services through our Security Development Lifecycle ("SDL"). Our SDL introduces security and privacy considerations throughout all phases of our development process and through the adoption of zero-trust end-to-end architecture. We utilize machine learning and AI-powered security tools to gain insights from over 78 trillion signals per day and over 135 million managed devices. We track over 300 unique threat actors, including 160 nation-state actors and 50 ransomware groups. To support our efforts, we operate a Cyber Defense Operations Center connected to over 10,000 security and threat intelligence experts, including engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

When appropriate, we utilize external service providers to assess, test, or otherwise assist our program. We also leverage third parties by working with external researchers, operating bug bounty programs, and managing coordinated vulnerability disclosure programs with security organizations. We maintain a systematic approach to assessing and controlling the cybersecurity risks presented by third-party service providers. We require third-party service providers to manage their cybersecurity risks in defined ways, undergo cybersecurity reviews, notify us of cyber events, and satisfy additional contractual requirements.

We seek to improve the entire cybersecurity ecosystem through multistakeholder diplomacy to set and uphold expectations for state behavior, advancement of government policy that strengthens cybersecurity and resiliency, disruption and deterrence of cybercrime, protection of national security interests, and disruption of digital threats to democracies. We also establish processes and innovate solutions for us and our customers to address the growing number and complexity of cybersecurity regulations.

When we experience a cybersecurity incident, we utilize our well-established incident response plans that operate both across the company and at the product and services level. Incidents are first triaged for severity, and then more deeply assessed to establish a plan of record and activate internal and external notification, disclosure, and communication plans, as applicable. Engineering and development resources are mobilized to resolve or remediate the incident. After the incident is resolved, a comprehensive post-incident review process is conducted.

We describe the risks from cybersecurity threats, including previous cybersecurity incidents, in section “Risk Factors” (Part I, Item 1A of this Form 10-K). As of the date of this Form 10-K, we do not believe any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect us, including our results of operations or financial condition. However, the cybersecurity threat environment is increasingly challenging, and we, along with the entire digital ecosystem, are under constant and increasing threat. As discussed above, our business strategy is tied to the SFI and we are committed to continuously monitoring cybersecurity threats, enhancing the security of our products, investing in our cybersecurity infrastructure, and collaborating with peers, customers, service providers, regulators, and governments to advance our and the entire digital ecosystem’s cybersecurity defenses and resiliency.

GOVERNANCE

Our Board of Directors oversees cybersecurity risk. Cybersecurity reviews by the Board are scheduled to occur at least quarterly, or more frequently as determined to be necessary or advisable. Presentations to the Board of Directors are made by senior management, including our Chief Information Security Officer (“CISO”), our EVP of Microsoft Security, and the head of our Customer Security and Trust organization. The presentations address topics such as cybersecurity threats, incidents, top risks and related remediation efforts, results from internal and third-party assessments, progress towards risk-mitigation goals, the functioning of our incident response program, regulatory developments, and digital diplomacy efforts. In addition, we have an escalation process in place to inform senior management and the Board of significant issues. Cybersecurity issues are also considered during separate Board meeting discussions regarding important matters like ERM, audit issues, operational budgeting, business continuity planning, mergers and acquisitions, brand management, and other relevant matters.

Our CISO leads the strategy, engineering, and operations of cybersecurity across the company, and reports to the EVP of Microsoft Security. Our CISO has extensive experience assessing and managing cybersecurity programs and cybersecurity risk. Before joining Microsoft, our CISO served in a prior Chief Technology Officer role as well as in senior leadership, engineering, and operational roles within multiple organizations. In addition to the Board’s oversight of cybersecurity risk, to support the CISO, we have established a Cybersecurity Governance Council (“CGC”) charged with overseeing initiatives that safeguard Microsoft’s infrastructure. The CGC is comprised of an executive-level team of Deputy CISOs with cybersecurity backgrounds and expertise relevant to their roles. The CGC responsibilities include approving our enterprise security risk assessment process and results, determining the appropriate cybersecurity risk level and mitigations, reviewing the NIST CSF alignment, and supporting compliance with cybersecurity regulations. Our cybersecurity efforts are supported directly by Microsoft’s security and threat intelligence experts and our employees across the company, all of whom receive cybersecurity awareness training and education and are expected to support our efforts.

ITEM 2. PROPERTIES

Our corporate headquarters are located in Redmond, Washington. We have approximately 15 million square feet of space located in King County, Washington that is used for engineering, sales, marketing, and operations, among other general and administrative purposes. These facilities include approximately 12 million square feet of owned space situated on approximately 530 acres of land we own at our corporate headquarters, and approximately 3 million square feet of space we lease.

We own and lease other facilities domestically and internationally, primarily for offices, datacenters, and research and development. The largest owned international properties include space in the following locations: China, India, Ireland, and the Netherlands. The largest leased international properties include space in the following locations: Australia, Canada, China, France, Germany, India, Ireland, Israel, Japan, the Netherlands, and the United Kingdom. Refer to Research and Development (Part I, Item 1 of this Form 10-K) for further discussion of our research and development facilities.

The table below shows a summary of the square footage of our properties owned and leased domestically and internationally as of June 30, 2024:

(Square feet in millions)

Location	Owned	Leased	Total
U.S.	**30**	**20**	**50**
International	**10**	**25**	**35**
Total	**40**	**45**	**85**

ITEM 3. LEGAL PROCEEDINGS

Refer to Note 15 – Contingencies of the Notes to Financial Statements (Part II, Item 8 of this Form 10-K) for information regarding legal proceedings in which we are involved.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS, AND ISSUER PURCHASES OF EQUITY SECURITIES

MARKET AND STOCKHOLDERS

Our common stock is traded on the NASDAQ Stock Market under the symbol MSFT. On July 25, 2024, there were 81,346 registered holders of record of our common stock.

SHARE REPURCHASES AND DIVIDENDS

Following are our monthly share repurchases for the fourth quarter of fiscal year 2024:

Period	Total Number of Shares Purchased	Average Price Paid Per Share	Total Number of Shares Purchased as Part of Publicly Announced Plans or Programs	Approximate Dollar Value of Shares That May Yet Be Purchased Under the Plans or Programs
				(In millions)
April 1, 2024 – April 30, 2024	**2,444,905**	**$ 413.75**	**2,444,905**	**$ 12,138**
May 1, 2024 – May 31, 2024	**2,233,450**	**416.85**	**2,233,450**	**11,207**
June 1, 2024 – June 30, 2024	**1,963,873**	**436.58**	**1,963,873**	**10,349**
	6,642,228		**6,642,228**	

All share repurchases were made using cash resources. Our share repurchases may occur through open market purchases or pursuant to a Rule 10b5-1 trading plan. The above table excludes shares repurchased to settle employee tax withholding related to the vesting of stock awards.

Our Board of Directors declared the following dividends during the fourth quarter of fiscal year 2024:

Declaration Date	Record Date	Payment Date	Dividend Per Share	Amount
				(In millions)
June 12, 2024	**August 15, 2024**	**September 12, 2024**	**$ 0.75**	**$ 5,575**

We returned $8.4 billion to shareholders in the form of share repurchases and dividends in the fourth quarter of fiscal year 2024. Refer to Note 16 – Stockholders' Equity of the Notes to Financial Statements (Part II, Item 8 of this Form 10-K) for further discussion regarding share repurchases and dividends.

ITEM 6. [RESERVED]