This report contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. The words "anticipate," "expect," "believe," "will," "may," "should," "estimate," "project," "outlook," "forecast" or other similar words are used to identify such forward-looking statements. However, the absence of these words does not mean that the statements are not forward-looking. The forward-looking statements represent NETGEAR, Inc.'s expectations or beliefs concerning future events based on information available at the time such statements were made. Goals and targets described in this report are aspirational and not guarantees or promises that the goals or targets will be met. Historical results, and forward-looking statements, may differ from actual results due to inherent uncertainties in making estimates and assumptions that are subject to change in the future. NETGEAR, Inc. disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. The inclusion of information contained in this document should not be construed as a characterization regarding the materiality or financial impact of that information.

Website references and hyperlinks throughout this document are provided for convenience only, and the content on the referenced websites is not incorporated into this report. We assume no liability for any third-party content contained on the referenced websites.
Introduction
ESG Message from the CEO

For more than 25 years, NETGEAR has pioneered advanced networking technologies for homes and businesses around the world. That’s over a quarter century of enabling people to do more with their lives at home and at work so that they are happier and more productive. In short, our mission has always been to use innovation to power connection. We empower our customers to collaborate and connect to a world of information through our high-performance networking solutions.

We’ve made significant strides since the introduction of our first hub in 1996, when homes without wires and business networks without walls or barriers were the dreams that inspired us. Since then, we have grown to become one of the world’s most trusted brands with products installed in millions of homes and businesses in every country on the planet.

As we lead the next technological evolution, the same core values that made our original aspirations a reality continue to drive us. These values include leveraging the latest innovations to create world-class solutions that help to simplify and improve peoples’ lives, continuing our legacy of high-quality, sustainable product design, better protecting our customers’ data and privacy, maintaining an environmentally and socially responsible supply chain, and holding professional integrity and inclusion at the core of all business operations.

In the wake of the recent pandemic and with the rise of increasingly distributed workforces, our work is more important than ever. As we made the transition to working and learning and everything else from home, reliable internet rose from a given to a primary concern. With the latest wireless standards, such as 5G and WiFi 6E, we helped people to realize that they can be productive and connected from just about anywhere, ushering in a whole new idea of what an office, classroom or home can be.

Other events—such as climate change, inflation, prolonged supply chain disruption, and the ever-changing cyberthreat landscape—also have global, social and economic implications that demand action. To surmount these challenges and make a positive impact on the world around us, we must rely on the beliefs and practices that have contributed to our longevity and success.

As an industry leader, NETGEAR’s commitment to being a trusted brand that embodies our values can be seen across every aspect of our operations. As we continue to innovate and build solutions that help our customers do more than they ever thought possible, so too will we apply that creative process to improve the way we do business. We will move forward with an eye toward preserving our environment, protecting our customers, and empowering our employees within a culture of trust and integrity.

Powering a future that connects us all,

Patrick Lo
NETGEAR CEO and Co-founder
Being a Trusted Brand

From data handling to supply chain management, we are working internally and externally to promote a culture of trust and integrity. We also know NETGEAR customers are, most often, repeat customers and the relationship we develop with them is long-term. That’s why we engage in a continual conversation that goes far beyond the purchase of a product. Their voice, insights and feedback are taken seriously and are an integral consideration in all aspects of our product and marketing life cycles.

- Emphasizing the proactive nature of the company’s data and cybersecurity challenges.
- Respecting consumers’ rights to data privacy.
- Devoting internal resources to employee engagement and inclusion/diversity initiatives.
- Managing environmentally and socially responsible supply chain to manage and mitigate associated risks.
- Holding professional integrity at the core of all business operations.
- Assessing our carbon footprint to mitigate our impact on the planet.
Materiality Assessment

In the context of this report, materiality denotes the relative importance of key ESG topics to NETGEAR's business and our stakeholders. Our materiality assessment informs our prioritization of ESG issues in our operations, allowing us to focus on the topics that matter most to our employees, our consumers, and the greater community.

Materiality Assessment Process

In 2021, NETGEAR conducted its first ESG materiality assessment. Combining insights from workshops, internal discussions, industry practices, SASB standards, and rating agencies, our initial list of material ESG topics was created. Based on stakeholder interviews, these topics were validated and prioritized, generating our final materiality topic list. We plan to periodically review our material topics to ensure their relevance is maintained.

Our Material Topics

Based on the materiality assessment, our priority ESG topics were identified based on relative importance to our business and our stakeholders. We believe that these topics will have the greatest impact on our performance and will allow us to cultivate long-term sustainability within operations. Our priority topics informed the creation of our ESG strategy and initiatives. More details about each topic can be found in the next sections of this report.
### NETGEAR’s Priority ESG Topics

<table>
<thead>
<tr>
<th>Product Security</th>
<th>Data Privacy</th>
<th>Supply Chain Management</th>
<th>Employee Engagement, Diversity &amp; Inclusion</th>
<th>Professional Integrity</th>
<th>GHG Emissions &amp; Energy Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
</tbody>
</table>
Product Security
Product Security

NETGEAR’s mission is to be the innovative leader in connecting the world to the internet. To achieve this mission, we strive to earn and maintain the trust of our customers by delivering products that are more secure and better protect the privacy and security of our customers’ data. We are committed to embedding reliable product security principles within our operations to safeguard your privacy.

Vulnerability Management

We appreciate having security concerns brought to our attention and are constantly monitoring our products to get in front of the latest threats. Being proactive rather than reactive to emerging security issues is a fundamental belief at NETGEAR. NETGEAR strives to keep up-to-date on the latest security developments by working with both security researchers and companies. We appreciate the community’s efforts in creating a more secure world.

We define a product security vulnerability as a weakness in a product or service that could allow an attacker to compromise the integrity, availability, or confidentiality of the product, service, or the environments in which they are deployed. The weakness can be the result of one or more design flaws or defects (bugs) in its software or hardware. NETGEAR aims to protect customers from malicious attacks that exploit security vulnerabilities in its products.

To do this, we have dedicated vulnerability management processes, comprised of the following:

- Centralized company-wide product vulnerability tracking and reporting
- Vulnerability classification, prioritization and remediation service level agreements (SLA)
- Vulnerability risk acceptance
- Product security incident and crisis response
- Hotfixes

Additionally, NETGEAR’s Product Security Team investigates all reports of security vulnerabilities affecting NETGEAR products and services. Instructions on how to report a vulnerability can be found on our website: netgear.com/about/security/.
### NETGEAR Product Security

#### Product Lifecycles

Product security is integrated throughout our product’s lifecycle. From product conception to production, NETGEAR proactively implements an approach to identify and manage relevant security risks. Prior to product launch, NETGEAR carries out numerous security tests based on each product’s unique data and network access needs. Risks and vulnerabilities are addressed through appropriate security measures and are incorporated into the final product as it develops and evolves.

Although the implementation of security within the lifecycle of products may vary based on the unique characteristics, an example of our approach consists of the following:

- Secure coding and design guidelines are published and reviewed by our security architect.
- We design and test products to meet full security requirements, including penetration tests and security exception risk acceptance processes.
- Upon launch, products undergo formalized bug detection, reporting, and triage processes, which are coupled with NETGEAR’s official procedure for publishing public reports of security-related corrections.
- We produce security patches for 3 years after the last production date of each product.

For additional information, please visit the NETGEAR product security website [netgear.com/about/security/](http://netgear.com/about/security/).

#### Incident Response Process

Our cybersecurity team is dedicated to responding to incidents in an efficient and effective manner to better safeguard security. Our robust incident response process allows our team to swiftly address incidents and better prevent future attacks from occurring.

#### Regulatory Compliance Policies

NETGEAR complies with the EU-US and the Swiss-US Privacy Shield Frameworks ("Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information from EU member countries, the United Kingdom, and Switzerland. NETGEAR certifies that it adheres to the Privacy Shield principles on notice, choice, accountability for onward transfer security, data integrity and purpose limitation, access, and recourse, enforcement and liability. With respect to personal information received or transferred pursuant to the Privacy Shield Frameworks, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

For more information, please read our full privacy policy, available at [netgear.com/about/privacy-policy/](http://netgear.com/about/privacy-policy/).
Products & Services

Your family and employees should have the peace of mind to browse the internet safely. We are developing products and value-added services to help safeguard this information to keep you, your household, and business online. We have built security features into our products to enhance the security of your products and the privacy of your data. NETGEAR products have numerous internal controls to address cybersecurity risks including secure password support, accessible enablement and disablement of features, automatic firmware updates and patching, and more.

Available as an add-on, NETGEAR Armor® is a one-stop internet security solution that’s more than just anti-virus software—it’s a better protective shield for the entire home. Built into NETGEAR WiFi, it automatically updates and helps protect not only computers, but also mobile phones, smart TVs, door locks, and security cameras from being hacked. It helps guard sensitive information, like credit card and social security numbers, from being stolen and helps ensure internet activity remains private.
Data Privacy and Cybersecurity
Data Privacy

At NETGEAR, we are dedicated to the privacy of your data. We aim to be fully transparent in the collection, sharing, and usage of any personal data. We only use your personal information for legitimate business purposes, such as improving our products and services, analyzing internal data, and preventing fraud. Your information is important, and you can trust us with your data.

Privacy Policy

NETGEAR Inc. and its affiliates and subsidiaries take your privacy seriously. Our privacy policy emphasizes the importance of personal data security and discloses the collection, use, and transfer of personal data. The policy spans all business areas and includes customer, partner, employee data, and website privacy. It also tells you about your rights with respect to your personal information, and how you can reach us to update it or get answers to questions you may have about our privacy practices.

To read our full privacy policy, please visit netgear.com/about/privacy-policy/.
Privacy Principles

At NETGEAR, we’ve been connecting people and businesses for over 25 years. That’s 25 years of enabling people to do more with their lives at home and at work, so they are happier and more productive. We create our products with this goal in mind: to simplify and improve people’s lives by helping them to collaborate and connect to a world of information and entertainment online. We care deeply about our customers and their privacy. We are not in the business of monetizing our customers’ private data by selling it. Your privacy is a right, and at NETGEAR we respect this right.

NETGEAR does not look at your private data. You store and send millions of megabytes of information over the internet daily. This information is personal, and it should be considered confidential. Your family photos, social media updates, browsing history, banking statements, and more are private pieces of data that we do not look at or have access to.

NETGEAR collects data to improve your experience with our products. We collect some product-specific data used solely to improve or recommend products and services. It is never sold to third parties.

Governance Structure

NETGEAR’s cross-functional data privacy governance structure combines efforts from our legal, customer care, IT, HR, and engineering teams. Our dedicated VP of Product Security and the Board of Directors’ Cybersecurity Committee oversee and monitor product security and data privacy. Please see Corporate Cybersecurity for additional details regarding our governance structure.

Data Protection Policy

We are committed to protecting your privacy and your data. Our Analytics Data Policy explains what data we collect, the purposes for which we use the data and your choices about NETGEAR’s data processing.

To read our full policy, please visit netgear.com/about/analyticsdatapolicy.
Cybersecurity

As technology grows more advanced so, too, do cybersecurity threats. Our dedication to robust corporate cybersecurity is upheld by our cross-functional cybersecurity team, data protection controls, vulnerability management processes, and incident response procedures. At NETGEAR, our products are backed by trusted internal operations, reinforcing reliable cybersecurity systems throughout our business.

Cybersecurity Governance

Cybersecurity for us is the people, process, and technology to better ensure that security is carried out to meet corporate specific needs. In recognition of the importance of governance in addressing cyber risks, our Board of Directors formed a Cybersecurity Committee in June 2017. We also have a Cybersecurity Governance Committee comprised of Executive staff, IT, Audit, and Cybersecurity along with various working groups that meet regularly to discuss our Corporate and Product Security Programs, including reviewing metrics and discussing open vulnerabilities, system hygiene, and remediation plans. We provide our Board with quarterly updates of these Corporate and Product Security Programs.
Customer Data Protection

Protecting our e-commerce platform is important to us, and we take precautions to better protect customer data from unauthorized access and data corruption. We only collect the most vital data that is needed for operations. We do not collect customer sensitive Personal Identifiable Information (PII) such as date of birth, social security number, health or financial information. We have defense-in-depth security, and maintain compliance with Payment Card Industry (PCI), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA).

Vulnerability Management & System Hygiene

We take infrastructure vulnerability management and system hygiene very seriously. Apart from regular vulnerability assessments on our infrastructure, we also welcome feedback on our security practices via our public bug bounty (Security Researcher Recognition) program. Concerns reported to us are thoroughly investigated and addressed.

Security Awareness and Training

We believe security awareness and training are key aspects of managing cybersecurity. Our focus is to establish a strong cybersecurity mindset at NETGEAR. Our employees are required to complete a series of security trainings such as new hire security training, an annual security refresher training and role-based security trainings. These trainings are reinforced through quarterly phishing exercises and ongoing awareness campaigns.
Product Design & Manufacturing
Product Design & Manufacturing

Our products are thoughtfully designed, manufactured, and packaged with sustainability in mind. From responsibly sourced materials to our sustainable product design, we are committed to providing you with high-quality, high-performing products that you can trust.

Product Design

Sustainable Product Design

NETGEAR is committed to the continuous improvement of the energy efficiency of our retail products. Accordingly, NETGEAR is a Signatory for the Small Network Equipment Voluntary Agreement (SNEVA) which provides the framework that limits the power consumption of in-home network equipment, and reduces power usage and indirect greenhouse gas emissions.

Responsible Packaging

Our commitment to responsible product design is reflected in our packaging. We are committed to complying with local laws and regulations in the jurisdictions in which we operate, and plan for the recycle, reuse, or reclamation of our products and packaging. This principle is a driving force at NETGEAR and is deeply ingrained in our values.

We are continuously analyzing our approach to product packaging, with sustainability as a priority. We have eliminated foam in our packaging for all Small Medium Business (SMB) products and are working to phase it out of all new products. Guided by circularity principles, we have also set Post-Consumer Waste (PCW) targets to divert waste from landfills. By 2025, we will use 20% PCW for product packaging and 60% PCW for master cartons. Looking forward, we are working to integrate sustainable packaging initiatives into our environmental strategy.

Waste Management

NETGEAR is committed to reducing the amount of e-waste that ends up in landfills as a result of the sale of our products. Across facilities in North America and APAC regions, we recovered 660.2 metric tons of scrap waste. We divert any salvageable e-waste from landfills through our circularity programs. Out of the recovered waste, a portion of the parts are refurbished into new products, and the remainder is sent for further recycling.

As electronic waste continues to grow, NETGEAR is responding by reducing or eliminating hazardous materials in our products and by helping to protect the health and safety of our employees, our customers, and the environment.
Materials Sourcing

Conflict Minerals Policy

As a part of NETGEAR’s commitment to corporate responsibility and respecting human rights, it is NETGEAR’s goal to use tantalum, tin, tungsten and gold (3TG) in our products that do not directly or indirectly finance or benefit armed groups in the DRC or adjoining countries while continuing to support responsible mineral sourcing in the region. NETGEAR has been working closely with the Responsible Business Alliance (RBA), Responsible Minerals Initiative (RMI), Smelter Engagement Team (SET) and our direct suppliers to trace 3TG back to their origin in order to ensure responsible sourcing. We continuously monitor supply chain operations in respect to conflict minerals and will take the appropriate actions to engage our suppliers in measurable risk mitigation efforts that are consistent with the OECD Guidance. NETGEAR seeks to avoid harming communities through de facto embargoes of minerals sourced from those areas. For more information, please read our full Conflict Minerals Sourcing Policy.

Critical Materials Risk Analysis

Analysis of NETGEAR products found that small quantities of 3TG, necessary to their functionality or production, are found in substantially all NETGEAR products. Because NETGEAR does not have direct contractual relationships with smelters and refiners, we rely on our direct suppliers and the entire supply chain to gather and provide specific information on 3TGs used in our products. Our due diligence processes are based on the necessity of seeking data from our suppliers and component manufacturers and those suppliers seeking similar information within their supply chains to identify the original sources of the necessary conflict minerals. We also rely, to a large extent, on information collected and provided by independent third-party audit programs.
Supply Chain Management
Supply Chain Management

Delivering products that our customers can trust starts in our value chain. We recognize the ways in which global, social, and environmental factors are pushing businesses to re-examine and reinvent the ways we work, especially regarding supply chain management. Committed to supply chain transparency, NETGEAR promotes the humane treatment of workers and mitigates potential labor and environmental risks throughout our entire value chain.

Supplier Code of Conduct

NETGEAR is committed to ensuring the highest standards of social responsibility wherever our products are made. We have a zero tolerance for both forced labor and human trafficking. NETGEAR’s program is based on our Supplier Code of Conduct, which outlines our expectations for our partners. We conduct a risk assessment of our significant suppliers. Based on the risk assessment, we then determine the appropriate audit procedures. We evaluate compliance through an auditing program and work proactively with our suppliers to drive change, as necessary. In an effort to confront slavery and human trafficking, NETGEAR assesses supply chain risk thoroughly, conducts social compliance audits of our suppliers, requires supplier compliance with our Supplier Code of Conduct, engages third-party on-site supplier audits, and conducts internal training on the Supplier Code of Conduct. For more information, please read our Statement Regarding the California Transparency in Supply Chains Act of 2010 and the UK Modern Slavery Act of 2015.

To read our full transparency statement, please visit netgear.com/files/netgear/documents/CASupplyChain.
Supply Chain Management

RBA Compliance

NETGEAR completed the Responsible Business Alliance (RBA) mid-year member compliance reporting in January 2022, covering results from the 2H ’21 audits. We noted no critical violations of policies and standards which require immediate escalation in the audits completed. All planned audits in 2021 covered over 80% of production volume, complying with our annual CSR commitment and RBA membership requirement. All audits were carried out remotely throughout 2021 to ensure the safety of our partners and auditors.

Supply Chain Audit

We actively manage the impacts of our supply chain and execute comprehensive audits of our suppliers. In FY21, our audits covered over 98% of the production volume, complying with our annual CSR commitment and RBA membership requirement. Of these suppliers, we do not have any high risk facilities. Our FY21 audits identified a total of 121 issues, including 4 priority non-conformances and 117 other non-conformances which include both major and minor non-conformances. For all priority non-conformances identified, we re-audit the facilities within six months.

Potential Labor and Environmental Risks

Environmental issues such as pollution and climate change have had significant legislative and regulatory effects on a global basis, and there are expected to be additional changes to the regulations in these areas. These changes could directly increase the cost of energy, which may have an impact on the way we manufacture products or utilize energy to produce our products. In addition, any new regulations or laws in the environmental area might increase the cost of the raw materials we use in our products and the cost of compliance. Other regulations in the environmental area may require us to continue to monitor and ensure proper disposal or recycling of our products. To the best of our knowledge, we maintain compliance with all current government regulations concerning our production processes for all locations in which we operate. Since we operate on a global basis, this is a complex process that requires continual monitoring of regulations and compliance efforts to ensure that we, and our suppliers, are in compliance with all existing regulations.
Employee Engagement, Diversity & Inclusion
Employee Engagement, Diversity & Inclusion

We believe that our employee population should reflect the communities where we live and serve. We are committed to promoting and cultivating an inclusive and diverse culture that welcomes and celebrates everyone without bias. NETGEAR seeks to foster a diverse working environment, representing a broad spectrum of backgrounds and cultures that promotes innovative ideas and products. We recognize that it takes true diversity and inclusion to unleash the power of each of our employees' fullest potential. We file the Employment Information Report (EEO-1) annually which provides a demographic breakdown of our workforce by race and gender. We disclose this report on our company website. To access our EEO-1, please use the following link: NETGEAR ESG Environmental, Social, and Governance | NETGEAR.

SASB Diversity Metrics

In alignment with SASB Standards, the metrics below highlight a breakdown of NETGEAR employees’ gender and racial/ethnic group background.

<table>
<thead>
<tr>
<th>Global Employees</th>
<th>Female</th>
<th>Male</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>34%</td>
<td>66%</td>
</tr>
<tr>
<td>Technical Staff</td>
<td>24%</td>
<td>76%</td>
</tr>
<tr>
<td>All Other Employees</td>
<td>58%</td>
<td>42%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U.S. Employees Only</th>
<th>Asian</th>
<th>Black or African American</th>
<th>Hispanic or Latino</th>
<th>White</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>51%</td>
<td>3%</td>
<td>2%</td>
<td>41%</td>
<td>3%</td>
</tr>
<tr>
<td>Technical Staff</td>
<td>62%</td>
<td>5%</td>
<td>5%</td>
<td>27%</td>
<td>1%</td>
</tr>
<tr>
<td>All Other Employees</td>
<td>44.5%</td>
<td>4%</td>
<td>6%</td>
<td>39.5%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Leadership Diversity

We demonstrate diversity, equity, and inclusion at the highest levels of our company. As of December 31, 2021, 50% of our independent directors were female, and approximately 55% of our executive management team self-identify as an underrepresented minority, in terms of race, ethnicity, or gender. In addition, women represented approximately 24% of technical positions worldwide and approximately 34% of leadership roles worldwide.
NETGEAR’s Employee Engagement Initiatives

Diversity & Inclusion Training

To foster a culture of respect within our workplace, we provide employees with training on Diversity, Equity, and Inclusion (DEI) topics. Our Diversity and Inclusion course is required by all employees and helps to ensure that they understand NETGEAR’s diversity and inclusion goals, from recruitment to team development. We educate employees on belongingness, empathy, and on our internal efforts toward a more diverse workforce. Our Reflection on Bias course helps employees to recognize, deal with, and prevent bias through understanding the needs of diverse groups at NETGEAR. These training courses help equip our employees with the skillset they need to be an ally, taking us one step closer to more inclusive operations.

Employee Resource Groups

As a truly global enterprise, we work every day to go beyond accepting diversity - we celebrate it, we support it, and we cultivate it. We offer ongoing development programs, including CEO Action for Diversity & Inclusion and Employee Resource Groups (ERG): the Black Employee Resource Group, and Women in the Workplace Resource Group.

Employee Experience Surveys

We conduct regular engagement surveys every two years to increase and monitor employee engagement. The surveys help us to identify areas where we can improve our policies, maximizing the happiness and performance of our employees. Since initiating the surveys in 2014, we have never fallen below a 95% participation rate. Our most recent employee experience survey was conducted in 2021 and had a 99% participation rate.
Pay Equity and Promotion Percentage Analysis

The average annual salary for females and males is 95% and 104%, respectively, of the total company average annual salary. Female directors are paid slightly over 100%. Female VPs and managers are slightly under 100%. Management monitors and addresses all statistical outliers on a periodic basis.

Employee Health & Safety

The health and safety of our employees are critical to our success and thus one of our top priorities. NETGEAR frequently monitors workplace cleanliness and safety in an effort to promote hygiene and minimize injuries. Our Corporate Emergency Response Team and Business Continuity Program equip employees with essential knowledge and supplies in case of emergencies. We periodically examine various Health and Safety aspects such as safe and clean workplaces, emergency preparedness, injury and illness, industrial hygiene, ergonomics, machine safeguarding, and more. We are also dedicated to maintaining updated safety guidelines for all of our products. Health and safety are covered under our Responsible Business Alliance (RBA) guided audit program and corporate facilities.
Professional Integrity
Professional Integrity

NETGEAR’s business operations are founded on a strong sense of professional integrity. Our dedication to ‘doing the right thing’ is consistent with our history and where we want to go in the future. We foster an honest and ethical working environment through our governance structure, regulatory compliance policies, and ethical codes of conduct. Although policies are important, it is how we act on them that truly matters. It is our intention that all employees understand how to do their jobs properly within applicable legal, regulatory, and ethical standards. At NETGEAR, we actively work to maintain and improve a culture of professional integrity through everything we do.

Ethical Codes of Conduct

NETGEAR prides itself on a commitment to building our business by providing customers with high-quality and innovative products with integrity and honest conduct. NETGEAR’s high standards of ethics are outlined in our Code of Ethics and Conflict of Interest Policy, which serves both internal and supply chain purposes. This Code is designed to maintain the standards of business conduct of NETGEAR and ensure compliance with legal requirements. In 2021, 100% of NETGEAR employees and Board members and over 80% of direct suppliers signed our Code of Ethics certification. NETGEAR’s suppliers must act in accordance with our Supplier Code of Conduct, which helps to ensure that working conditions in our supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally and socially responsible. Our Anti-Corruption Compliance Program, led by the Governance, Risk and Audit, and Legal teams, meets on a monthly basis and monitors all anti-corruption compliance regulations, including FCPA and the UK Bribery Act. The program executes regular risk assessments (both for internal operations and the supply chain), conducts compliance research, promotes company awareness, and communicates externally regarding regulatory topics.
Regulatory Compliance Policies

NETGEAR aims to maintain compliance with regulatory laws, standards, and requirements of the industry. The Legal team constantly considers the impacts of emerging regulations, making sure proper consent and disclosure are in place. NETGEAR products go through vigorous testing and certification processes in every aspect of regulatory compliance, including but not limited to electromagnetic compatibility (EMC), safety, wireless, and telecom. NETGEAR follows applicable laws, directives, standards, and industry regulations. Products are accordingly marked and in compliance with, but not limited to, Federal Communication Commission (FCC) standards, European Union Directives (CE Mark), Japan’s VCCI, Australia’s RCM, and others countries marking requirements. Declarations of Conformity are kept on record and available upon request.

Board of Directors

The Board’s primary responsibility is to monitor and assist management in creating long-term value for NETGEAR’s stockholders in an ethical and socially responsible manner. Our Board currently has an Audit Committee, a Compensation Committee, a Cybersecurity Committee, and a Nominating and Corporate Governance Committee.

Ethics Training

In 2021, 100% of Board members, 99% of employees, and 92% of key suppliers completed the anti-corruption training. NETGEAR also provides numerous ethics-related courses to our employees, including Workplace Harassment Prevention, Security Awareness Essentials, and Global Anti-Bribery & Corruption trainings.

Whistleblower Protection

We take the privacy and protection of whistleblower complaints seriously. NETGEAR provides a reporting hotline for employees and suppliers to anonymously report numerous incidents.

To access our anonymous reporting hotline, please use the following link:
netgear.com/about/corporate-social-responsibility/ethics/whistleblower-protection/.
GHG Emissions &
Energy Management
NETGEAR is committed to providing our customers with high-quality products that are environmentally sound, and to conducting our operations in a responsible manner. As stewards of the environment, we consider and plan for the recycling, reuse, or reclamation of our products and packaging. NETGEAR continues to work proactively to reduce or eliminate hazardous materials in our products, helping to protect the health and safety of our employees, our customers, our manufacturing partners, the environment, and our communities. These commitments continue to be a driving force at NETGEAR and reflect principles deeply ingrained in our values.

GHG Emissions & Energy Management

NETGEAR is committed to providing our customers with high-quality products that are environmentally sound, and to conducting our operations in a responsible manner. As stewards of the environment, we consider and plan for the recycling, reuse, or reclamation of our products and packaging. NETGEAR continues to work proactively to reduce or eliminate hazardous materials in our products, helping to protect the health and safety of our employees, our customers, our manufacturing partners, the environment, and our communities. These commitments continue to be a driving force at NETGEAR and reflect principles deeply ingrained in our values.
NETGEAR’s Greenhouse Gas Emissions

Operational Emissions

We have calculated our operational emissions (Scope 1 and Scope 2 emissions) in accordance with the GHG Protocol. NETGEAR’s Scope 1 emissions are the direct greenhouse emissions that occur from sources that we directly own. Within Scope 1 emissions, stationary combustion has been identified as the only material category to our operational carbon footprint. Our FY21 Scope 1 emissions were estimated to be 223 mt of CO2e, totaling 0.01% of our total carbon footprint. Scope 2 emissions include the indirect emissions from purchased energy sources for use in our facilities. Our FY21 Scope 2 emissions were estimated to be 1,293 mt of CO2e, totaling 0.05% of our total carbon footprint.

Value Chain Emissions

We have also calculated emissions associated with our value chain (Scope 3 emissions) in accordance with the GHG Protocol. We have identified and calculated the following Scope 3 categories that are relevant to our operations: Purchased Goods & Services, Upstream Transportation & Distribution, Operational Waste, Business Travel, Employee Commuting, Downstream Transportation & Distribution, Use of Sold Products, and End of Life Treatment of Sold Products. We use specific emissions calculations methodologies based on the data availability for each Scope 3 category. We continue to improve the precision and depth of our emissions data to report accurate GHG estimates. As such, methodologies to calculate Scope 3 emissions may change in future years as more data becomes available. Based on estimates of each material category, our total Scope 3 emissions for FY21 was 2,816,957 mt of CO2e, totaling 99.9% of our total carbon footprint. Of our Scope 3 categories, Use of Sold Products emits the most carbon emissions, making up 92% of our total GHG emissions. Our entire GHG inventory breakdown is provided in the Appendix.
Renewable Energy Usage

In 2021, NETGEAR procured 50% renewable energy and 80% carbon-free energy for our San Jose Headquarters. In 2023, we plan to implement sustainability initiatives to further reduce our operational emissions.

Environmental Targets & Initiatives

We recognize the environmental impact of our operations and continue to seek ways to better understand, measure, and reduce our environmental footprint. Since 2014, we have participated in the Carbon Disclosure Project (CDP). We are also in the process of aligning our future reporting with the Taskforce on Climate-Related Financial Disclosures (TCFD).

NETGEAR is committed to the continuous development of our environmental initiatives to better the environment in which we operate. In 2022, we began the process of aligning our greenhouse gas (GHG) reporting with the GHG Protocol to more accurately capture the emissions associated with our operations and complete value chain. Understanding our carbon footprint will allow us to develop targeted reduction plans in future years. We are currently analyzing climate strategies that will help reduce our current carbon emissions. In 2023, we plan to set an emissions reduction goal aimed at mitigating our impact on the climate. As we develop our climate strategy, we will work continuously to improve the accuracy of our environmental data and calculations.

Water Usage

The total water usage from NETGEAR’s facilities was 3,928,546 gallons for FY21.
**GHG Emissions & Energy Management**

**NETGEAR FY21 Greenhouse Gas Emissions**

- Use of Sold Products: 92.38%
- Purchased Goods & Services: 4.80%
- Upstream Transportation & Distribution: 1.99%
- Downstream Transportation & Distribution: 0.73%
- Scope 2: 0.05%
- End-of-Life Treatment of Sold Products: 0.02%
- Scope 1: 0.01%
- Business Travel: 0.01%
- Employee Commuting: 0.01%
- Operational Waste: 0%

1 Refer to appendix for all categories of Scope 3
# SASB Disclosures

## Hardware Disclosures

<table>
<thead>
<tr>
<th>Topic</th>
<th>SASB Code</th>
<th>Metric</th>
<th>NETGEAR FY22 Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Security</strong></td>
<td>TC-HW-230a.1</td>
<td>Description of approach to identifying and addressing data security risks in products</td>
<td>See the Product Security section of our ESG Report for information on our identification and management of security risks in our products.</td>
</tr>
<tr>
<td><strong>Employee Diversity &amp; Inclusion</strong></td>
<td>TC-HW-330a.1</td>
<td>Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees</td>
<td>See the Employee Engagement, Diversity &amp; Inclusion section of our ESG Report for information on our diversity metrics.</td>
</tr>
<tr>
<td><strong>Product Lifecycle Management</strong></td>
<td>TC-HW-410a.1</td>
<td>Percentage of products by revenue that contain IEC 62474 declarable substances</td>
<td>All NETGEAR products contain a small amount of one or more of the compounds on the IEC 62474 declaration substances list. However, all NETGEAR products comply with the regulations listed in IEC 62474, including RoHS, REACH, Prop 65, TSCA, and POPs, etc.</td>
</tr>
<tr>
<td></td>
<td>TC-HW-410a.2</td>
<td>Percentage of eligible products, by revenue, meeting the requirements for EPEAT registration or equivalent</td>
<td>Not applicable. NETGEAR products are not eligible for EPEAT registration.</td>
</tr>
<tr>
<td></td>
<td>TC-HW-410a.3</td>
<td>Percentage of eligible products, by revenue, meeting ENERGY STAR® criteria</td>
<td>Not applicable. NETGEAR does not pursue ENERGY STAR criteria.</td>
</tr>
<tr>
<td></td>
<td>TC-HW-410a.4</td>
<td>Weight of end-of-life products and e-waste recovered, percentage recycled</td>
<td>NETGEAR is committed to reducing the amount of e-waste that ends up in landfills as a result of the sale of our products. Please reference the Waste Management section, under the Product Design and Manufacturing portion, of our ESG Report for more information.</td>
</tr>
</tbody>
</table>
## Hardware Disclosures

<table>
<thead>
<tr>
<th>Topic</th>
<th>SASB Code</th>
<th>Metric</th>
<th>NETGEAR FY22 Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain Management</td>
<td>TC-HW-430a.1</td>
<td>Percentage of Tier 1 supplier facilities audited in the RBA Validated Audit Process (VAP) or equivalent, by (a) all facilities and (b) high-risk facilities</td>
<td>FY21 audits covered over 98% of NETGEAR’s production volume, complying with our annual CSR commitment and RBA membership requirement. No high-risk facilities were identified.</td>
</tr>
<tr>
<td></td>
<td>TC-HW-430a.2</td>
<td>Tier 1 suppliers’ (1) non-conformance rate with the RBA Validated Audit Process (VAP) or equivalent, and (2) associated corrective action rate for (a) priority non-conformances and (b) other non-conformances</td>
<td>FY21 audits identified a total of 121 issues, including 4 priority non-conformances and 117 other non-conformances which include both major and minor non-conformances. For all priority non-conformances identified, NETGEAR re-audits the facilities within six months.</td>
</tr>
<tr>
<td>Material Sourcing</td>
<td>TC-HW-330a.1</td>
<td>Description of the management of risks associated with the use of critical materials</td>
<td>See the Materials Sourcing section, under the Product Design and Manufacturing portion, of our ESG Report or our Conflict Minerals Sourcing Policy for a description on our management of critical materials, such as tantalum, tin, tungsten, and gold, in our supply chain and operations.</td>
</tr>
</tbody>
</table>

## Activity Metrics

<table>
<thead>
<tr>
<th>Activity Metric</th>
<th>SASB Code</th>
<th>Metric</th>
<th>NETGEAR FY22 Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of units produced by product category</td>
<td>TC-HW-000.A</td>
<td>Number</td>
<td>16,079,508 products across SMB and CHP product categories.</td>
</tr>
</tbody>
</table>
## GHG Inventory Data

<table>
<thead>
<tr>
<th>Scope</th>
<th>Category</th>
<th>FY2021 (in MT CO2e)</th>
<th>% of Total GHG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope 1</strong></td>
<td>Stationary Emissions</td>
<td>223</td>
<td>0.01%</td>
</tr>
<tr>
<td></td>
<td>Total Scope 1</td>
<td>223</td>
<td>0.01%</td>
</tr>
<tr>
<td><strong>Scope 2</strong></td>
<td>Purchased Electricity</td>
<td>1,293</td>
<td>0.05%</td>
</tr>
<tr>
<td></td>
<td>Total Scope 2</td>
<td>1,293</td>
<td>0.05%</td>
</tr>
<tr>
<td><strong>Scope 3</strong></td>
<td>Purchased Goods &amp; Services</td>
<td>135,338</td>
<td>4.80%</td>
</tr>
<tr>
<td></td>
<td>Upstream Transportation &amp; Distribution</td>
<td>56,160</td>
<td>1.99%</td>
</tr>
<tr>
<td></td>
<td>Operational Waste</td>
<td>6</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Business Travel</td>
<td>253</td>
<td>0.01%</td>
</tr>
<tr>
<td></td>
<td>Employee Commute</td>
<td>206</td>
<td>0.01%</td>
</tr>
<tr>
<td></td>
<td>Downstream Transportation &amp; Distribution</td>
<td>20,679</td>
<td>0.73%</td>
</tr>
<tr>
<td></td>
<td>Use of Sold Products</td>
<td>2,603,618</td>
<td>92.38%</td>
</tr>
<tr>
<td></td>
<td>End of Life</td>
<td>697</td>
<td>0.02%</td>
</tr>
<tr>
<td></td>
<td>Total Scope 3</td>
<td>2,816,957</td>
<td>99.95%</td>
</tr>
<tr>
<td><strong>Total Emissions</strong></td>
<td></td>
<td>2,818,473</td>
<td>100.00%</td>
</tr>
</tbody>
</table>