2025 SASB Index

Introduction

Our annual **2025 Impact Report** presents information for ADT Inc. (the "Company", "ADT" or "we") relating to certain sustainability related focus areas.

The information below reports certain additional information and metrics with reference to the Sustainability Accounting Standards Board ("SASB") framework. SASB has developed industry-based standards to identify and standardize disclosures for the sustainability issues most relevant to investor decision-making. The tables reflect ADT's reporting metrics utilizing several SASB industry standards including Professional & Commercial Services [SV-PS], Software & IT Services [TC-SI], Road Transportation [TR-RO], and Waste Management [IF-WM]. The data provided represents the metrics as of or for the year ended December 31, 2025. Inclusion of information in this report is not an indication that we deem such information to be material or important to an understanding of our business or an investment decision with respect to our securities or for any other purpose under U.S. federal securities law.

Management is responsible for the completeness, accuracy, and validity of the metrics included in this report and has established processes for the collection, quantification, and presentation of the metrics. Management is also responsible for the selection of the criteria, which provide an objective basis for measuring and reporting the metrics. For the purposes of limited assurance, management asserts that the metrics reported in this report are presented in accordance with the assessment criteria, specifically the SASB codes below. We engaged SGS United Kingdom Ltd. ("SGS") to conduct an independent assurance review that provides limited assurance on specified metrics, which are identified by the "♦" symbol throughout this report. SGS Assurance Statement can be found **here**.

SASB Topics

- Greenhouse Gas Emissions
- Fleet Fuel Management
- Environmental Footprint of Hardware Infrastructure
- Workforce Diversity & Engagement
- Data Privacy & Freedom of Expression
- Data Security
- Managing Systemic Risks from Technology Disruptions

Note About Forward-Looking Statements

This report includes estimates, projections, and statements regarding corporate responsibility-related plans, objectives, and goals that are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995, Section 27A of the Securities Act of 1933, and Section 21E of the Securities Exchange Act of 1934 (the "Exchange Act"). Forward-looking statements may appear throughout this report. These forward-looking statements generally are identified by words such as "ongoing," "expects," "intends," "will," "anticipates," "believes," "confident," "continue," "propose," "seeks," "could," "may," "should," "estimates," "forecasts," "might," "goals," "objectives," "targets," "planned," "projects," and similar expressions. Forward-looking statements are based on current expectations and assumptions that are subject to risks and uncertainties that may cause actual results to differ materially from those expressed in our forward-looking statements. In evaluating these statements, you should consider various factors, including the risks and uncertainties we describe in the "Risk Factors" sections of our Forms 10-K and 10-Q and other reports we file with the Securities and Exchange Commission ("SEC"). The inclusion of forward-looking and other statements in this report is not an indication that they are necessarily material to investors or required to be disclosed in our filings with the SEC. Such statements may contain estimates, make assumptions based on developing standards that may change, and provide aspirations and commitments that are not intended to be promises or guarantees. Readers are cautioned not to place undue reliance on forward-looking statements and such other statements, which speak only as of the date they are made. We undertake no obligation to update or revise publicly any forward-looking or such other statements, whether because of new information, future events, or otherwise.

TOPICS & METRICS	SASB CODE	RESPONSE
Greenhouse Gas Emissions		
Gross global Scope 1 emissions	TR-RO-110a.1	41,965 $MTCO_2e$♦ gross Scope 1 emissions, which are primarily mobile combustion from our vehicle fleet. Please refer to our 2025 Impact Report for additional information.
Discussion of long- and short-term strategy or plan to manage Scope 1 emissions, emissions reduction targets, and an analysis of performance against those targets	TR-RO-110a.2	In 2025, ADT launched its transition to more sustainable hybrid vehicle fleet, which will help reduce Scope 1 emissions. ADT has not set emissions reduction targets at this time. Please refer to our 2025 Impact Report for additional information.
(1) Total fuel consumed, (2) percentage natural gas and (3) percentage renewable	TR-RO-110a.3	630,374 GJ♦ total fuel consumed, 5%♦ natural gas, 0%♦ renewable Please refer to our 2025 Impact Report for additional information.
Fleet Fuel Management		
(1) Fleet fuel consumed, (2) percentage natural gas and (3) percentage renewable	IF-WM-110b.1	598,027 GJ♦ fleet fuel consumed, 0%♦ natural gas, 0%♦ renewable Please refer to our 2025 Impact Report for additional information.
Percentage of alternative fuel vehicles in fleet	IF-WM-110b.2	5% hybrid electric vehicles in fleet. In 2025, ADT launched its transition to a more sustainable vehicle fleet. Please refer to our 2025 Impact Report for additional information.
Fleet vehicle size	IF-WM-000.B	3,400 fleet vehicles, approximately
Environmental Footprint of Hardware Infrastructure		
(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	TC-SI-130a.1	734,786 GJ♦ [(a)] total energy consumed, 14%♦ grid electricity, 4.4%♦ renewable energy[(b)]. Energy sources include vehicle fleet fuel, natural gas, generator fuel, and purchased grid electricity. Please refer to our 2025 Impact Report for additional information. (a) ADT is unable to track specific energy consumption for all its locations, where, for example, electricity is included in lease charges. Estimates of electricity consumption are included based on facilities square footage. (b) ADT purchased renewable energy certificates (RECs) for 30 facilities across 10 states. We are continuing to sign multi-year contracts with wind-based Green-e RECs.
(1) Total water withdrawn, (2) total water consumed; percentage of each in regions with High or Extremely High Baseline Water Stress	TC-SI-130a.2	145,894 m^3♦ [(a)] withdrawn/consumed, all sourced from municipal water supplies. ADT does not store water, so our withdrawal and consumption statistics are the same. 8%♦ withdrawn/consumed in regions with High or Extremely High Baseline Water Stress (a) ADT does not utilize water in its core operations and therefore does not track specific usage for all its locations where, for example, water is included in lease charges. Estimates of water usage are included based on facilities square footage.
Discussion of the integration of environmental considerations into strategic planning for data center need	TC-SI-130a.3	ADT is committed to ensuring environmental sustainability and operational efficiency at its data centers. We have invested significant time and resources focusing on efficiency improvements in data operations, air handling, and lighting. We meet or exceed industry-standard best practices at all our facilities. At our larger data centers, we have replaced older hardware with energy-efficient alternatives, updated cooling and lighting systems where environmentally friendly alternatives are available, and employ dynamic operations methods to improve overall network efficiency.

TOPICS & METRICS	SASB CODE	RESPONSE
Workforce Diversity & Engagement		
(1) Voluntary and (2) involuntary turnover rate for employees	SV-PS-330a.2	33%♦ voluntary[(a)] turnover rate[(c)(d)] 10%♦ involuntary[(b)] turnover rate[(c)(d)] (a) Voluntary turnover is defined as an employee that leaves the Company on their own initiative and includes retirement. (b) Involuntary turnover is defined as termination of employment of an employee at ADT. (c) Modified to align with ADT turnover calculations using the average number of employees for the denominator. All data is sourced from ADT's Human Resources Management System. (d) ADT workforce has many commission-based compensation employees, which increases turnover rates.
Employee engagement as a percentage	SV-PS-330a.3 TC-SI-330a.2	79%♦ employee engagement[(a)] (a) ADT conducted an annual Employee Sentiment Survey that was administered by a third party, Perceptyx Inc. Employee engagement is measured based on four specific questions that are directly tied to engagement (1. I would recommend ADT as a good place to work; 2. I intend to stay with ADT for at least the next 12 months; 3. My work gives me a strong sense of personal accomplishment; 4. I am proud to work at ADT). The percentage is calculated as the weighted average of employees who responded favorably (strongly agree or agree) to the questions out of the total number of employees who responded to the survey. All employees were invited to participate, excluding employees recently hired and those who were on a leave of absence, and 72% of employees responded to the survey.
Percentage of employees that require a work visa.	TC-SI-330a.1	0.5%♦ of employees require a work visa. ADT completed I-9 digitization for all employees in 2025.
Number of employees by: (1) full-time and part-time, (2) temporary, and (3) contract	SV-PS-000.A	12,109♦ full-time[(a)] and 63♦ part-time[(a)]; 18♦ temporary[(a)]; N/A contractors[(b)] (a) Employee headcount is based on data from ADT's Human Resources Management System (HRMS) as of December 31, 2025. Full-time is defined as an employee working 35 hours or more a week. Part-time is defined as an employee working less than 35 hours a week. Temporary employees are typically interns. (b) ADT works with several companies to fulfill contractual employment needs that arise. Contractors are not currently tracked in HRMS.

TOPICS & METRICS	SASB CODE	RESPONSE
Data Privacy & Freedom of Expression		
Description of policies and practices relating to targeted advertising and user privacy.	TC-SI-220a.1	ADT is committed to protecting the data we maintain on behalf of our customers, employees, contractors, and applicants. Our data security program is based on: centralized coordination; administrative, technical, and procedural safeguards; risk assessment and management; monitoring, testing, and reporting; and clear training and awareness. ADT's information security policies include our: IT Security Policy, Vulnerability Management Policy, IT Security Acceptable Use Policy, Risk Management Policy, Personal Data Protection and Privacy Policy, Information Classification Guidelines, and Code of Conduct, as well as internal data privacy and retention policies.
Number of users whose information is used for secondary purposes.	TC-SI-220a.2	Per our Privacy Policy, ADT does not sell customer personally identifiable information ("PII") to third parties for their own marketing purposes. ADT shares PII with partners for our specified business purposes and thus, these partners may use such PII as necessary to provide services to ADT. To the extent that a partner intends to use PII information for other purposes, customers must provide authorization and have the option to revoke or modify such authorization.
Total amount of monetary losses as a result of legal proceedings associated with user privacy.	TC-SI-220a.3	We are required by the Securities and Exchange Commission to disclose, in our Annual Report on Form 10-K, any material litigation or legal proceedings. In our Form 10-K for the year ended December 31, 2025, we do not disclose any material litigation or legal proceedings associated with user privacy.
(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	TC-SI-220a.4	From time to time, ADT receives formal requests that comply with legal process and procedure from state and federal law enforcement agencies. We are required by the Securities and Exchange Commission to disclose, in our Annual Report on Form 10-K, any material litigation or legal proceedings. In our Form 10-K for the year ended December 31, 2025, we do not disclose any material litigation or legal proceedings associated with law enforcement requests for user information.
List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	TC-SI-220a.5	ADT's core products and services are offered only in the United States and Puerto Rico. ADT is also occasionally required to provide services in other jurisdictions outside of the U.S. for our U.S.-based customers.

TOPICS & METRICS	SASB CODE	RESPONSE
Data Security		
Description of approach to identifying and addressing data security risks , including use of third-party cybersecurity standard	SV-PS-230a.1 TC-SI-230a.2	Cybersecurity at ADT focuses on the prevention, detection, and correction of any unauthorized presence on our information systems that jeopardizes the confidentiality, integrity, or availability of our systems and data. We believe that the safety, security, and privacy of our customers and employees are fundamental to the services we provide, and we continuously enhance methods, best practices, and technologies to monitor and protect customer data. Our Chief Information Security Officer ("CISO") is responsible for developing and implementing plans and strategies to mitigate cybersecurity risks. Our CISO also leads our cybersecurity risk assessment, which includes security posture scoring, vulnerability assessments, process maturity, and tooling coverage, and collaborates with the Cybersecurity Leadership Team to identify risks and determine the best ways to address them. We leverage recognized cybersecurity frameworks, including National Institute of Standards and Technology, to drive strategic direction and maturity improvement and engage third-party security experts as needed for risk assessments, risk mitigation actions, vulnerability identification, and program enhancements, as appropriate. The Audit Committee receives quarterly updates on the status of the cybersecurity program. Please refer to our 2025 Form 10-K for additional information
Description of policies and practices relating to collection, usage, and retention of customer information	SV-PS-230a.2	ADT's information security policies include: Risk Management Policy; IT Security Policy; Vulnerability Management Policy; IT Security Acceptable Use Policy; ADT Code of Conduct; Information Classification Guidelines; Protecting Personal Identifiable Information (PII) Policy; Personal Data Protection and Privacy Policy; Addendum A to ADT Interim Remote Work Policy; ADT Asset Protection Policy; ADT IT Security Standards; ADT Records Management Policy; ADT Contact Center Remote Work Policy; and ADT Social Media Policy. We reinforce these policies through regular trainings for the relevant employees, as well as annual security awareness training for all ADT team members. ADT maintains automated cybersecurity monitors in addition to a round-the-clock team of certified security operations professionals to detect potential malicious activity.
(1) Number of data breaches, (2) percentage that (a) involve customers' confidential business information and (b) are personal data breaches, (3) number of (a) customers and (b) individuals affected	SV-PS-230a.3 TC-SI-230a.1	We have no material data breaches that could have a material adverse effect on our financial position or the business. Data breaches that may have a material adverse effect on ADT's financial position or the business would be disclosed in our public filings with the Securities and Exchange Commission.

TOPICS & METRICS	SASB CODE	RESPONSE
Managing Systemic Risks from Technology Disruptions		
Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	TC-SI-550a.1	The scope of performance issues, service disruptions, and total customer downtime is limited to security monitoring system incidents[(a)] that result in a delay in the answering of high-priority customer alarms[(b)]. 3 performance issues[(c)] and 0 service disruptions[(d)]. There were no significant service disruptions[(f)]. 0.3 security monitoring service subscription-days total customer downtime[(e)]. (a) Security monitoring system incidents are limited to those tracked in ADT's Service Now IT system, classified as high- or critical-priority, and that require a root cause analysis. (b) High-priority customer alarms are fire, burglar, smoke, heat, and carbon monoxide. (c) Modified to define performance issues as any unplanned security monitoring system incidents causing a delay, of more than 10 minutes but less than or equal to 30 minutes, in the answering of individual high-priority customer alarms. (d) Modified to define service disruptions as any unplanned security monitoring system incidents causing a delay, of more than 30 minutes, in the answering of individual high-priority customer alarms. (e) Modified to define customer downtime as the total delay in answering high-priority customer alarms related to performance issues and service disruptions, reported in security monitoring service subscriber-days. (f) A service disruption is considered significant when the cost to correct is material or it is disruptive to a large number of customers.
Description of business continuity risks related to disruptions of operations	TC-SI-550a.2	To minimize business interruption, ADT maintains a Business Continuity Management Office ("BCMO") to ensure operational contingency for business operations, employee safety, customer services, product availability, and brand protection. The BCMO collaborates with key functional partners to develop Business Interruption Plans for our business-critical functions. ADT performs annual disaster recovery exercises for life safety and mission-critical applications based on guidelines put in place by the BCMO.
(1) Number of licenses or subscriptions, (2) percentage cloud-based	TC-SI-000.A	Approximately 6.1 million♦ security monitoring service subscribers. 0% in public cloud. ADT's security monitoring service is not cloud-based.