SASB Index

AR = 2022 Annual Report
PS = 2023 Proxy Statement

Accounting Metric	Code	Boeing Metric or Qualitative Disclosure(s) and Disclosure Location(s)
Energy Management		
Total energy consumed	RT-AE-130a.1	Key ESG Data, Page 74 CDP Climate Report[1]
Percentage of grid electricity	RT-AE-130a.1	Key ESG Data, Page 74
Percentage of renewable energy	RT-AE-130a.1	Key ESG Data, Page 74; Sustainability Goals, Page 12
Hazardous Waste Management		
Amount of hazardous waste generated	RT-AE-150a.1	Key ESG Data, Pages 75-76
Percentage of hazardous waste recycled	RT-AE-150a.1	Key ESG Data, Pages 75-76
Number and aggregate quantity of reportable spills	RT-AE-150a.2	Key ESG Data, Page 76
Quantity recovered from reportable spills	RT-AE-150a.2	Key ESG Data, Page 76
Data Security		
Description of approach to identifying and addressing data security risks in company operations	RT-AE-230a.2	We rely extensively on information technology systems and networks to operate our company and meet our business objectives. As cyber threats increase in volume and sophistication, the risk to the security of these systems and networks — and to the confidentiality, integrity and availability of the data they house — continues to evolve, requiring constant vigilance and concerted, companywide risk management efforts. Boeing takes a risk-based approach to managing the security of its data and has a documented low-risk appetite for cybersecurity and data protection, while recognizing that business requirements may necessitate adjustments to that risk tolerance. To address these risks, we maintain an extensive network of technical security controls, policy enforcement mechanisms, monitoring systems and management oversight. We also have established a Security Council to strengthen governance and coordination of cyber and physical security activities. While these measures are designed to prevent, detect and respond to unauthorized activity, there is no guarantee that they will be sufficient to prevent or mitigate the risk of a cyberattack or data loss or the potentially serious reputational, operational or financial impacts that may result. A strong partnership exists between IT, Enterprise Security, Corporate Audit, and Legal to ensure identified issues are addressed in a timely manner and incidents are reported to the appropriate regulatory bodies as required.
Description of approach to identifying and addressing data security risks in products	RT-AE-230a.2	Product Security Engineering provides a disciplined approach to the development and sustainment of our products, which is essential to ensuring mission assurance, resiliency and security. Security is integrated into our engineering processes, starting from concept development, ensuring that we develop products that are secure by design. Key cyber attributes and adversity (or threat) to the system are identified during requirements engineering, allocated throughout design, implemented and validated during development, fully tested and supported during sustainment. Additionally, Boeing works to ensure that our products are designed to anticipate, withstand, recover and adapt to cyberattack. Specifically, our security processes ensure that we have high-level requirements to baseline and monitor data flow and system behavior, detect anomalies and actively manage system configuration. The ability of our systems to understand normal operations and rapidly detect and mitigate the abnormal, combined with the security engineering focus of our development processes, provides Boeing's programs with a proactive approach to risk management. Product Security is also integrated into the Boeing enterprise Incident Response process, and we work seamless with stakeholders to rapidly identify, analyze, and mitigate vulnerabilities and breaches across our portfolio.

1. Boeing participates annually in the CDP Climate Report. Our most recent response is available on our website here in accordance with the CDP reporting schedule.