Sustainability Accounting Standards Board (SASB) Disclosure 2025

BAE Systems plc
Industry: Aerospace and Defence

BAE SYSTEMS

Topic	Metric	BAE Systems Response	Code
Energy Management	**(1)** Total energy consumed (gigajoules) **(2)** Percentage grid electricity (%) **(3)** Percentage renewable (%)	**(1)** 4,928,851 gigajoules Total energy consumed – Scope 1 and 2. This disclosure is consistent with the corresponding disclosure in our 2025 Annual Report, which reports in kilowatt hours rather than gigajoules. See page 230 of our 2025 Annual Report. **(2)** 55.7% **(3)** 5.3% Notes: (2) (3) These figures are different from the corresponding figures on page 58 of our 2025 Annual Report in order to comply with the different SASB reporting requirements. (3) The reported percentage includes renewable electricity that is directly produced by the Company and renewable energy purchased by the Company.	**RT-AE-130a.1**
Hazardous waste management	**(1)** Amount of hazardous waste generated (metric tonnes, T), **(2)** percentage recycled (%)	**(1)** 7,408T **(2)** 36% Hazardous waste is defined by reference to relevant local laws and regulations. The reported percentage recycled includes non-hazardous and hazardous waste recycling. See page 58 of our 2025 Annual Report.	**RT-AE-150a.1**
	Number of aggregate quantity of reportable spills, quantity recovered	0 reportable spills (following CERCLA requirements) in respect of US facilities where we have operational control. CERCLA only applies in the US. We can confirm that in other jurisdictions in which we operate, zero spills occurred in 2025 requiring enforcement action under relevant local environmental legislation.	**RT-AE-150a.2**

Data security	**(1)** Number of breaches **(2)** Percentage involving confidential information	We do not report this information in the public domain due to confidentiality and security reasons.	**RT-AE-230a.1**
Data security	Description of approach to identifying and addressing data security risks in **(1)** company operations **(2)** products	**(1) Company operations** As a major defence, aerospace and security company, the Group faces significant risks in respect of its information security, continuity of operations, integrity of its products and physical security. These threats are continuous and evolving, and are posed by organisations with a broad range of capability, from criminals to nation states. The Board and senior management regularly consider security risk. These senior level reviews cover evolving threats, the Group's planned responses and the effectiveness of security controls and security investments in meeting intended objectives. Security risk is also reviewed at a functional and operating business level. The Group's internal Cyber Security Standards are aligned to the National Institute of Standards and Technology framework. A formal, three layers of defence assurance programme, which is reviewed both internally and externally, is operated to check adherence to these standards and customer requirements. Additionally, resulting from the need to comply with government customer requirements, certain of the Group's IT networks are formally accredited by those customers. Education and awareness to embed a strong security culture across the Group is a vital part of its preventative activities. Employees are required to complete mandatory training which (depending on role) covers cyber security, physical and personal security, document marking, security of export-controlled information and personal data protection. As many cyber-attacks involve email, the Group runs a programme of phishing exercises for all email users across the enterprise.	**RT-AE-230a.2**

Data security		To increase the Group's resilience against security threats, the Group performs protective monitoring of activity on the Group's core networks via the Group's Security Operations Centres, maintains incident response and crisis management plans with updates following regular test exercises and obtains threat intelligence to the Group, utilising its internal security capabilities and from external partners including governments. To address the heightened risk to the security of the Group's personnel, additional communications and advice are provided to all employees on personal safety precautions. To mitigate the cyber security risk posed by working with suppliers, the Group performs risk-based due diligence and assurance and (where relevant) seeks to require suppliers to comply with cyber security-related contractual provisions. In addition to the above, the Group purchases cyber and property insurance, however, as with all insurance, it does not provide full cover against all potential loss scenarios. For further details, please see our 2025 Annual Report. **(2) Products** Product data security risks and vulnerabilities come together as an aspect of Product Security Engineering, which is the ability of a product to remain appropriately secure and resilient within its intended operational environment. Our Product Security Engineering principles and internally mandated Product Security Standard are the foundation of how we work with our customers and supply chain partners to design, develop, manufacture and support our goods and services throughout the product lifecycle, and additionally to ensure the product can, in line with our contractual obligations, address the continually evolving threat of cyber-attack. Engineering teams use a number of sources for threat intelligence, including HMG / MOD supplied data, open source threat intelligence and Technology Focussed Threat Intelligence Reports which are produced internally. Threat intelligence can be used to help evaluate exposure to threat actors and vulnerabilities, which can be mitigated by putting appropriate safeguards in place	**RT-AE-230a.2**

Data security		Product performance, including for product data security, is jointly agreed, as part of the contract with the customer, throughout a product development lifecycle at the point of contractual negotiations, certification and acceptance. Where the Company is made aware of customer data security incidents, we will, where possible, support analysis and mitigation as required.	**RT-AE-230a.2**
Product safety	Number of recalls issued Total units recalled	We do not ordinarily put this information in the public domain. BAE Systems' Engineering function leads a cross-functional activity to actively addresses and monitor Product Safety issues across the business, and works with customers and suppliers to address any issues raised or identified.	**RT-AE-250a.1**
	Number of counterfeit parts detected Percentage avoided	We do not ordinarily put this information in the public domain. We seek to prevent the use of counterfeit parts, through contractual requirements within our Standard Conditions of Purchase as well as through our Supplier Code of Conduct. We expect our suppliers to develop, implement and maintain methods and processes appropriate to their products to prevent counterfeit parts and materials being delivered. Effective processes should be in place and regular training undertaken to detect, report and quarantine counterfeit parts and materials and prevent such parts from re-entering the supply chain. BAE Systems expects our suppliers to only use parts from original equipment or component manufacturers or their authorised sources, and to comply with applicable laws, regulations, and industry 'best practice' protocols when conducting business with BAE Systems. We expect suppliers to inform us immediately if counterfeit parts and/or materials are detected or suspected. https://www.baesystems.com/en/sustainability/responsible-business/responsible-supply-chain Supply chain management starts with the Group's Global Procurement Policy which defines the requirements to be implemented by each of the Group's sectors for the establishment of procurement controls and the management of supplier-related risk to a minimum set of standards. Our Global Procurement Policy requires our sectors to communicate our Supplier Code of Conduct to our suppliers.	**RT-AE-250a.2**

Product safety	Number of Airworthiness Directives received Total units affected	**Civil Airworthiness Directives** Below is a list of the Civil Airworthiness Directives and their application. Applicable to CAT Boeing Aircraft: FAA AD 2024-26-02 FAA AD 2025-04-01 FAA AD 2025-04-02 FAA AD 2025-04-03 FAA AD 2025-07-03 FAA AD 2025-15-01 FAA AD 2025-19-12 Applicable to CAT Embraer Aircraft ANAC AD BR-2025-09-01 EASA_AD_2025-0222 Note: In relation to military products, and any airworthiness notifications from the relevant military airworthiness authorities, we do not put this information in the public domain due to confidentiality and security reasons.	**RT-AE-250a.3**
	Total amount of monetary losses as a result of legal proceedings associated with product safety	We do not ordinarily put this information in the public domain.	**RT-AE-250a.4**

Fuel economy and emissions in use-phase	Revenue from alternative energy-related products	£150,000,000	**RT-AE-410a.1**
	Description of approach and discussion of strategy to address fuel economy and greenhouse gas (GHG) emissions of products	We recognise that our value chain contributes to our total GHG emission footprint beyond that of our Scope 1 and 2 emissions. We acknowledge the importance of continuing to partner and collaborate with our customers and suppliers to reduce emissions by 2050. According to external studies, approximately 65%[1] of defence industry emissions come from downstream customer use of products/platforms. To address this requires collaboration with our customers and across the wider defence sector while recognising that operational performance and capability must always take precedence. In Australia, the Kingdom of Saudi Arabia and the UK, we have undertaken a programme of work to understand the GHG profile of material products. This helps us understand how to decarbonise our products and identify how we can support future customer decisions and investment in product upgrades and development to support their decarbonisation. We are innovating to drive decarbonisation of products and services, and reduce the dependency on fossil fuels. This will be achieved by: • Energy optimisation • Alternate fuels • Developing electrification programmes Although the continued progression to lower and zero emissions products and technologies for the defence sector will require a significant transition it is anticipated it may lead to revenue opportunities for the Group over the long-term. 1. Roland Berger – Defence Zero Volume 1: Military emissions and potential solutions.	**RT-AE-410a.2**

Materials sourcing	Description of the management of risks associated with the use of critical materials	We conduct supply chain risk assessments and work with suppliers to address any identified key risks to their businesses and supply to our programmes which would include risk associated with the supply of critical materials. Therefore, critical materials are considered as part of a broader corporate approach to monitoring supply chain risk. The challenge of limited or sole source supplies of raw materials remains, due to the nature of some of the products manufactured by the Group, which are often of a unique specification, and frequently supplied at low volumes. To address this, we have a multi-faceted risk management programme that seeks to: aggregate risk across the enterprise using proactive intelligence; manage continuity of supply; and illuminate lower-level supply chain tiers to help us to understand the relationships within our supply chain. We pay specific attention to single and sole source critical goods and services procured through the supply chain, to ensure that the risk is fully understood and adequate contingency and risk mitigation plans are in place and can be enacted if required to manage programme delivery. Where the Group has long-term programmes in place, it seeks to leverage the benefit of a more stable forward visibility of long-lead requirements to allow the Group to better manage supplier deliverables against programme requirements. • The Group seeks to manage its supplier cost inflation risk through contracting arrangements, supplier cost management activity, long-term supplier agreements and leverage of category volumes.	**RT-AE-440a.1**
Business ethics	Total amount of monetary losses as a result of legal proceedings associated with incidents of corruption, bribery, and / or illicit international trade	We do not put this information in the public domain due to commercial confidentiality.	**RT-AE-510a.1**

Business ethics	Revenue from countries ranked in the 'E' or 'F' Band of Transparency International's Government Defence Anti-Corruption Index	As stated on page 151 of our 2025 Annual Report, our revenues from Saudi Arabia and Qatar (which constitute substantially all of our revenues from countries in Bands "E" and "F") are as follows: • Kingdom of Saudi Arabia: £2,838m • Qatar: £252m We do not put revenues from other countries in these Bands in the public domain due to commercial confidentiality.	**RT-AE-510a.2**
	Discussion of processes to manage business ethics risks throughout the value chain	Our industry is among the most highly regulated of any sector. Our global Operational Framework sets out our approach and the mandated policies and processes which apply across all wholly-owned entities. **Anti-corruption programme** Our customers, shareholders, partners and employees expect the highest standards when it comes to anti-corruption. We support our employees in understanding the vital role they have in helping the business to meet those standards and in respect of business conduct compliance more generally. We do not tolerate corruption in any of its forms. Our anti-corruption programme is designed to identify, manage and mitigate corruption risks and enable the company to adhere to all relevant legal and regulatory requirements recognising the bribery and corruption risks the Group faces (see legal risk on page 71). The programme provides our employees with practical guidance, helps them to understand what is expected of them and creates an environment where they feel they can confidently and, anonymously if needed, ask questions and raise concerns. **Our ethics programme** Our global Code of Conduct lays out the standards and behaviours that we expect of all employees and outlines the ways in which anyone can seek help and guidance. Our Code is supported by a training and engagement programme. All of our employees are required to complete live, manager-	**RT-AE-510a.3**

Business ethics		led ethics training annually alongside e-learning programmes of role-specific training, for example on trade controls. We value openness and strive to create a culture where people feel they can speak up freely and report issues and concerns without fear of retaliation. Employees can raise a concern through four primary channels: via our Ethics Officers; by email; on the telephone; and online reporting to our externally run Ethics Helpline service. Our Ethics Helpline permits anonymous reporting and is also open to third parties. Our Ethics Officers receive training to equip them with the skills to provide guidance to employees raising a concern. During 2025, we received 2,099 reports, reflecting a 22% increase globally from 2024; an increase driven across all businesses. The growth reflects our expanding operations and continued efforts to promote a speak up culture. During 2025, 56% of reports were resolved and closed through guidance, compared to 49% in 2024. Reporters seeking guidance has increased, with the substantiation rate of allegations at 31%. Our anonymity rate remained at 27% for the second consecutive year, remaining below the global benchmark rate of 54%. 35% of reports were made directly to Ethics Officers in 2025 – we encourage this route for raising reports, as it allows for an immediate response by someone familiar with the local situation. We interpret these metrics as positive indicators of reporters, including our employees, showing trust in the business and in speaking up. **Working with our supply chain** It is important that we collaborate and partner with our suppliers and the steps we are taking are detailed below. In 2025, we spent £16bn with more than 22,000 directly contracted suppliers worldwide. These relationships are often long-lasting due to the complexity of our products and their long lifecycles, so it is critical that our suppliers adhere to our Supplier Code of Conduct. We communicate our expectations of our supply chain through our Supplier Code of Conduct, which we share with all our directly contracted suppliers.	**RT-AE-510a.3**

Business ethics		Our Supplier Code of Conduct covers supplier workplace, labour standards, employee business practices and wider topics of focus. We are keen to continue to build our networks with companies, particularly small businesses, both within and external to our current supply chain, seeking to strengthen existing relationships, build new and novel ones, where appropriate, and continue to take actions that support businesses both within local communities and the broader defence sector. During 2025, we undertook an annual risk-based assurance activity to assess our suppliers' adoption of our Supplier Code of Conduct and to identify any areas that required investigation and/or mitigation. We completed this assurance activity with directly contracted suppliers representing more than 31% of our global spend. Additionally, our standard terms and conditions require suppliers to comply with all applicable laws and regulations, including those related to human rights, anti-slavery, anti-corruption and the environment.	**RT-AE-510a.3**
Production by reportable segment		At BAE Systems, we provide some of the world's most advanced, technology-led defence, aerospace and security solutions. We focus our operations across five key sectors: **Electronic Systems** Electronic Systems comprises the Group's US- and UK-based electronics business and the US-based Space & Mission Systems business. Key capabilities span electronic warfare systems, navigation systems, electro-optical sensors, military and commercial avionics, precision guidance solutions and communications systems, as well as space electronics, spacecraft, ground and tactical systems. **Platforms & Services** Platforms & Services, with operations in the US, Sweden and the UK, manufactures and upgrades combat vehicles, weapons and munitions, and delivers services and sustainment activities, including	**RT-AE-000.A**

Production by reportable segment		US naval ship repair and the management and operation of two government-owned, contractor-operated ammunition plants. **Air** Air comprises the Group's UK-based aircraft build and support activities for European and international markets, US programmes, development of our Future Combat Air System and FalconWorks®, alongside our business in the Kingdom of Saudi Arabia and interests in our joint ventures: Edgewing, Eurofighter and MBDA. **Maritime** Maritime comprises the Group's UK-based maritime and land activities, including ship build and support activities, major submarine build programmes, as well as our Australian business and interest in our RBSL joint venture. **Cyber & Intelligence** Cyber & Intelligence comprises the US-based Intelligence & Security business and UK-headquartered Digital Intelligence business and includes the Group's cyber security activities for national security, central government and government enterprises. **OUR KEY PROGRAMMES AND FRANCHISES** **Aircraft** Prime contracting, systems integration, rapid engineering, manufacturing, maintenance, repair and upgrade, and military training for advanced combat and trainer aircraft, including Typhoon and workshare of the F-35 Lightning II programme. **Combat Vehicles** Build and upgrade of tracked combat vehicles, including the Bradley fighting vehicles, M109 self-propelled howitzers, Armored Multi-Purpose Vehicles (AMPVs), CV90, BvS10, Beowulf and M88 recovery vehicles and Amphibious Combat Vehicles (ACVs). Through our interest in RBSL, design and manufacture of military vehicles.	**RT-AE-000.A**

Production by reportable segment		**Space** Leading capabilities in the design, build and operation of satellites and satellite systems, space electronics and instrument payloads. **Weapon systems and munitions** Design and manufacture of naval gun systems, munitions, energetics and propellants, torpedoes, radars, naval command and combat systems, artillery systems, missile launchers and, through our 37.5% interest in MBDA, missiles and missile systems. **Complex warships** Design and manufacture of eight Type 26 frigates for the Royal Navy and the first three (Batch 1) Hunter Class frigates for the Royal Australian Navy. Provider of the warship design for the Canadian Surface Combatant programme. **Submarines** Design and manufacture of seven Astute Class nuclear-powered attack submarines and four Dreadnought Class nuclear-powered submarines for the Royal Navy. Design and mobilisation activities on the SSN-AUKUS programme to deliver a replacement for the Astute Class. **Embedding environmental considerations** Provision of electric drive systems for low-and zero-emission propulsion systems with an extensive installed base on urban transit buses. **Intelligence and cyber security** Delivery of a broad range of intelligence, security and synthetic training services to enable military, intelligence and civilian branches of international governments to recognise, manage and defeat threats. **Naval ship repair and support** Provision of naval ship repair and modernisation services in the US and UK, together with support to the navies of the US, UK and Australia, at home and on deployment.	**RT-AE-000.A**

Production by reportable segment		**Uncrewed and future air system capabilities** Development of future air system capabilities, including joint investment with the UK Government and industry in a next-generation combat air system under the Tempest programme. Comprehensive portfolio of military uncrewed air systems UAS) and counter-UAS. **Commercial avionics equipment** Design, manufacture and support of avionics equipment across multiple commercial aircraft platforms, including engine and flight controls, and cabin and cockpit systems, as well as aftermarket support services. **Combat vehicles** Build and upgrade of tracked combat vehicles, including the Bradley fighting vehicles, M109 self-propelled howitzers, Armored Multi-Purpose Vehicles, CV90, BvS10, Beowulf and M88 recovery vehicles, and manufacture of Amphibious Combat Vehicles. **Air support and training** Provision of support to operational capability, including maintenance, upgrade, support and training for Typhoon, Tornado, Hawk and support for the F-35 Lightning II fleet around the globe. **Defence electronics** Design, manufacture and support of electronic systems across a range of military programmes, including a leadership position in the electronic warfare market.	**RT-AE-000.A**
Number of employees		**111,400** as at 31 December 2025 and including share of equity accounted investments.	**RT-AE-000.B**