



Sustainability Accounting Standards Board (SASB) Disclosure 2021

BAE Systems plc
Industry: Aerospace and Defence

BAE SYSTEMS

Topic	Metric	BAE Systems Response	Code
Energy management	(1) Total energy consumed (2) Percentage grid electricity (3) Percentage renewable	<p>(1) 5,848,565 gigajoules Total energy consumed – Scope 1 and 2. This disclosure is consistent with the corresponding disclosure in our 2021 Annual Report (which reports in kilowatt hours rather than gigajoules). See page 46 of our 2021 Annual Report.</p> <p>(2) 51.21% (3) 16.03%</p> <p>Notes: (2) (3) These figures are different from the corresponding figures on page 45 of our 2021 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 REGO backed renewable energy purchased by the Company.</p>	RT-AE-130a.1
	Amount of hazardous waste generated, percentage recycled	<p>(1) 8,690 tons (2) 83%</p> <p>Hazardous waste is defined by reference to relevant local laws and regulations. The reported percentage recycled includes non-hazardous, hazardous and construction waste recycled as the Company does not distinguish between the types of waste in its data collection. See page 45 of our 2021 Annual Report.</p>	RT-AE-150a.1
	Number and aggregate quantity of reportable spills, quantity recovered	<p>0 reportable spills (following CERCLA requirements) in respect of US facilities where we have operational control. In respect of a US facility where we do not have operational control, 2 spills were reported under CERCLA the volume released during both of these events was limited, however the exact volume is unknown.</p> <p>CERCLA only applies in the US. We can confirm that in other jurisdictions in which we operate, zero spills occurred in 2021 thus no enforcement action by regulatory authorities resulted under relevant local environmental legislation.</p>	RT-AE-150a.2
Data security	(1) Number of data breaches (2) Percentage involving confidential information	We do not put this information in the public domain due to confidentiality and security reasons.	RT-AE-230a.1

Data security
(continued)

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, it is critical that not only our own intellectual property and confidential information, but also that which we hold, collect, generate and process on behalf of our customers, partners, suppliers and employees around the world is properly protected and secure.

We do this by efficiently leveraging our core specialist internal capabilities in information security, and combining it with our external market and intelligence knowledge, to ensure continued protection, and constant re-evaluation of our security posture against targeted attacks and other evolving threats. Our internal Cyber Security Standards are aligned to NIST SP 800-53 for the plc business, and NIST SP 800-171 for the Inc. business. NIST SP 800-171 is derived from NIST SP 800-53, (Protecting Controlled Unclassified Information in Non-federal Systems and Organisations), and both are intended to mitigate cyber security risks. We are required to ensure our computing facilities and networks are configured and operated to meet or exceed the relevant Company, customer and contractual requirements. For customer-mandated requirements, this will include compliance with national regulations for the storing, managing and processing of government security classified information. Our Cyber Security Standards contain the baseline controls we wish to see for any computing device or network infrastructure, mapped to appropriate external customer requirements. Where requirements of the standards cannot be met, a formal multi-tiered security exceptions process is used to review any mitigating controls and assess whether the exception falls within risk tolerance.

A formal assurance programme is operated to check adherence to Company standards or customer requirements, which is audited both internally and externally. Additionally, many of our networks are formally accredited by our customers.

To complement the threat and data security risk activity, we perform continual protective monitoring of our networks locally and by our Global Security Operations Centre (GSOC) for centralised analysis to protect the enterprise infrastructure.

As well as monitoring for signs of external attack our protective monitoring also operates against Insider Threat activity, where user violations of security policy are detected and investigated, primarily to stop information exfiltration - whether accidental or deliberate.

RT-AE-230a.2

Employees and staff are subject to mandatory training, which depending on role covers IT security, physical security, document marking, security of export controlled information, and personal data protection. As many of our security threats can be delivered by email, we run a programme of phishing susceptibility testing for all email users across the enterprise.

For information belonging to the organisation that is processed by the Company on platforms outside of our network boundaries, a formal assurance process is in place that requires a minimum level of protective controls to be implemented, depending on information classification. This covers not only security considerations, but also other aspects such as compliance with customer and personal data protection requirements.

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 are the foundation of how we work with our customers and supply chain partners where contracted to design, develop, manufacture and support our products and services throughout the product lifecycle, to ensure the product can, in line with our contractual obligations, address the continually evolving threat of cyber-attack.

BAE Systems Digital Intelligence provides a Technology Focussed Threat Intelligence service. This information can be used to help evaluate product exposure to threat actors and vulnerabilities, which can be mitigated by putting appropriate safeguards in place.

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 are potentially able to support analysis and mitigation as required.

Product safety	<p>Number of recalls issued Total units recalled</p>	<p>We do not put this information in the public domain due to commercial confidentiality.</p> <p>BAE Systems' Engineering function actively addresses and monitors product safety issues across the business and works with customers and suppliers to address any issues raised or identified.</p>	RT-AE-250a.1
	<p>Number of counterfeit parts detected Percentage avoided</p>	<p>Our approach to counterfeit parts in the supply chain is one of prevention and assurance. We seek to prevent the use of counterfeit parts, through contractual requirements within our Standard Conditions of Purchase as well as through our Supplier Principles – Guidance for Responsible Business (Supplier Principles) which set out BAE Systems' expectations of its suppliers including in relation to counterfeit goods. https://www.baesystems.com/en/sustainability/responsible-supply-chain/suppliers/supplier-principles. We assure our global supply base using a risk based approach to confirm our suppliers' adoption of the Supplier Principles and identify any associated risks – in our 2021 assurance activity, we covered 25% of global spend. We also look to procure directly from Original Equipment Manufacturers where possible, or accredited distributors, to further reduce the risk.</p>	RT-AE-250a.2
	<p>Number of Airworthiness Directives received Total units affected</p>	<p>Civil Airworthiness Directives 7 Directives: AD References: G-2021-05, G-2021-06, G-2021-8, G-2021-11, G-2021-13, G-2021-15 and BR-2021-02-02 7 units affected (Platforms)</p> <p>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.</p>	RT-AE-250a.3
	<p>Total amount of monetary losses as a result of legal proceedings associated with product safety</p>	<p>We do not put this information in the public domain due to commercial confidentiality.</p>	RT-AE-250a.4

Fuel economy and emissions in use-phase	Revenue from alternative energy-related products	US\$253m This relates to Hybrid-electric, fully electric and other fuel alternative products.	RT-AE-410a.1
	Description of approach and discussion of strategy to address fuel economy and greenhouse gas (GHG) emissions of products	<p>Our goal is to develop and implement a long-term strategy that reduces the impact of our activities and products on the environment. We have set ourselves the target of:</p> <ul style="list-style-type: none"> • Achieving net zero greenhouse gas emissions across our operations (Scope 1 and 2) by 2030. We aim to do this by reducing our emissions as a minimum in line with the 1.5°C pathway; and • Working towards a net zero value chain by 2050 (see pages 38-47 of our 2021 Annual Report). <p>We also strengthened our net zero pathway by signing up to the UN Race to Zero via the Business Ambition for 1.5°C campaigns. Our UK business will be developing net zero milestones for the Science Based Targets initiative during 2022. We will look to extend this to other parts of the Group as we mature the development of our net zero roadmap and our related internal processes. We aim to improve energy efficiency, introduce cleaner technologies, collaborate across our value chain, and mitigate both physical and transitional climate related risk. BAE Systems has world-class engineering capabilities and high-end discriminating technologies, well aligned to the current and future requirements of our customers including advancing our proven electric drive technology to the maritime domain (see page 49 of our 2021 Annual Report). Our academic partnerships, including those with six leading UK universities (University of Birmingham, Cranfield University, the University of Manchester, the University of Nottingham, University of Southampton, and University of Strathclyde) enable BAE Systems to have access to research and development in key areas for future platforms such as electrification, alternative fuels and energy storage. Some of our partners also have capabilities spanning artificial intelligence and digital systems which we can draw upon to support our activities to drive energy efficiencies and optimisation through the design and support of our products.</p>	RT-AE-410a.2

<p>Materials sourcing</p>	<p>Description of the management of risks associated with the use of critical materials</p>	<p>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 issue of limited or sole source supplies of raw materials is familiar, due to the nature of some of the products produced by the Company which are often of a very high, specific and potentially unique specification, but which are required to be supplied in certain cases 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 suppliers to help us to understand the relationships within our supply chain.</p> <p>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.</p> <p>The external supply chain environment is very dynamic at this time, with both lead-time and availability issues, but also pricing pressures, including from inflationary increases in labour, energy and other key materials. We continue to monitor this risk. In many cases, the Group benefits from long-term programme positions and incumbencies with more stable forward visibility for long-lead items allowing the Group to continue to actively manage supplier lead times against demand requirements.</p>	<p>RT-AE-440a.1</p>
<p>Business ethics</p>	<p>Total amount of monetary losses as a result of legal proceedings associated with incidents of corruption, bribery, and/or illicit international trade</p>	<p>We do not put this information in the public domain due to commercial confidentiality.</p>	<p>RT-AE-510a.1</p>

<p>Business ethics (continued)</p>	<p>Revenue from countries ranked in the "E" or "F" Band of Transparency International's Government Defence Anti-Corruption Index</p>	<p>As stated on page 208 of our Annual Report 2021, our revenues from Saudi Arabia and Qatar (which constitute substantially all of our revenues from countries in Bands "E" and "F") are as follows: Saudi Arabia - £2,476m Qatar - £1,014m</p> <p>We do not put revenues from other countries in these Bands in the public domain due to commercial confidentiality.</p> <p>Our success depends on us being trusted by our stakeholders to uphold high standards of governance and business conduct. Robust governance remains at the core of our business and underpins the sustainability of the business. Our Operational Framework sets out our approach and the policies, processes and standards to which we adhere and apply everywhere we operate. For more information please see: https://www.baesystems.com/en/sustainability/governance/ethics-and-anti-corruption and our 2021 Annual Report.</p>	<p>RT-AE-510a.2</p>
	<p>Discussion of processes to manage business ethics risks throughout the value chain</p>	<p>Our success, as a Company, depends on our employees behaving ethically in everything they do. Each employee has a vital role to play in ensuring that we maintain the high standards of ethical conduct that our stakeholders expect. BAE Systems has a zero tolerance policy regarding corruption in all its forms. Our anti-corruption programme guides and supports our employees in making responsible decisions. It also helps employees understand what is expected of them and creates an environment in which employees feel they can ask questions and raise issues and concerns. Our programme is embedded through our key global policies and processes including thorough due diligence programmes. The programme receives both internal and external oversight and assurance. We drive improvements in the programme annually to ensure it continues to meet best practice.</p> <p>Our approach to how we manage business ethics risks throughout our value chain can be found in 'Our approach to ethics and anti-corruption' brochure found here - https://www.baesystems.com/en/sustainability/governance/ethics-and-anti-corruption.</p>	<p>RT-AE-510a.3</p>

An extremely broad range of products and components are produced by the Company annually in the various product categories. Products, and numbers of products produced, can be security classified and customer confidential, and so not disclosable. Therefore limited examples of units of key products, or subunits of key products which were produced in 2021 across the portfolio of ground vehicles, aircraft, maritime vehicles, aircraft components and space and weapons systems are set out below, by reference to the 2021 BAE Systems plc [Annual Report](#).

Ground vehicles

BAE Systems manufactures a broad range of ground vehicles, in the US and Sweden. Examples of key activities in this segment in 2021 include:

- In the US, Armoured Multi-Purpose Vehicle (AMPV) deliveries continued against the rebaselined customer schedule, and a sustainment and technical support services contract was also awarded for AMPV.
- In the US, the Amphibious Combat Vehicle deliveries against LRIP continued, and design development has begun on new mission variants.
- Contract received from Sweden for 127 Bvs10s.
- Contract received for mid-life upgrades of Dutch CV90s.

Aircraft

BAE Systems manufactures aircraft, as well as major subcomponents of such aircraft in international collaborations. Examples of product delivery activities in 2021, by aircraft type, include:

- Typhoon aircraft programme – final assembly and major subassembly work:
 - Qatar Typhoon programme is progressing well, with the first Qatar Typhoon flight achieved in November and deliveries on schedule to commence in 2022.
 - Production progressing to plan on the German Typhoon programme.
- F-35 aircraft programme:
 - F-35 rear fuselage production reached full rate levels, with 151 assemblies completed in the year.
- Tempest aircraft programme:
 - The Tempest next-generation Future Combat Air System programme continues to progress well, with the initial Concept & Assessment Phase contract secured.

	<p>Maritime vehicles BAE Systems manufactures and supports ships, and manufactures submarines, including in 2021:</p> <ul style="list-style-type: none"> • In the UK, construction of the first three City Class Type 26 frigates for the Royal Navy is now underway. • In the UK, the fifth Astute Class submarine, Anson, was launched in April 2021, with final installation and commissioning activities continuing to ready her for scheduled exit in 2022. • In the UK, construction of the first two Dreadnought Class submarines for the Royal Navy continues to advance. • Canadian Surface Combatant programme entered a key design milestone in December 2021, ahead of moving in to the next Functional Design phase. • Australian Hunter Class Frigate programme continues through prototyping, with good engagement with the Commonwealth to agree revised schedule for production to commence. <p>Vehicle and aircraft components A broad range of vehicle and aircraft components are supplied, including in relation to military and civil aircraft, as well as vehicles, including electric drive propulsion systems for urban bus fleets, maritime vessels, urban aircraft and military vehicles. By way of example, F-35 electronic warfare systems are supplied, of which the cumulative programme deliveries surpassed 1,000 electronic warfare systems as of year-end 2021.</p> <p>Weapon systems A broad range of gun systems, weapons systems and munitions are supplied to key government customers, including in the US, UK, India and Sweden. The Company operates the US Army’s Holston and Radford ammunition plants and has been awarded contracts for modernisation projects at the two facilities.</p>	
<p>Number of employees</p>	<p>90,500 as at 31 December 2021, including share of equity accounted investments.</p>	<p>RT-AE-000.B</p>

Dated: 30 March 2022

BAE Systems plc
Registered Office: 6 Carlton Gardens, London, SW1Y 5AD, UK
Registered in England & Wales No: 1470151

www.baesystems.com

©BAE Systems plc 2022. All rights reserved
BAE Systems is a registered trademark of BAE Systems plc.

Cautionary statement:

All statements other than statements of historical fact included in this report, including, without limitation, those regarding the strategy, plans and objectives of the BAE Systems Group, the markets and economies in which it operates and its financial condition, results, operations and businesses, are forward-looking statements. Such forward-looking statements which reflect management's assumptions made on the basis of information available to it at this time, involve known and unknown risks, uncertainties and other important factors which could cause the actual results, performance or achievements of the BAE Systems Group or the markets and economies in which it operates to be materially different from future results, performance or achievements expressed or implied by such forward-looking statements. BAE Systems plc and its directors accept no liability to third parties in respect of this report save as would arise under English law.