Ethical Risk Assessment Report: Broadcom Inc.

Executive Summary

This report presents a comprehensive ethical risk assessment of Broadcom Inc. (NASDAQ: AVGO), conducted in accordance with the "Guidelines for observation and exclusion of companies from the Government Pension Fund Global" (the Fund), specifically criteria outlined in § 3 (product-based) and § 4 (conduct-based).[1] The purpose of this analysis is to provide the Council on Ethics and Norges Bank with a detailed, evidence-based evaluation to inform the status of the Fund's investment in the company.

The assessment concludes that while Broadcom's products do not meet the specific criteria for product-based exclusion, the company's conduct presents significant and multifaceted ethical risks. The key findings are as follows:

- **Product-Based Risk (§ 3):** The investigation found no evidence that Broadcom develops or produces "key components" designed or adapted *solely* for weapons that violate fundamental humanitarian principles, such as nuclear weapons, cluster munitions, or anti-personnel mines. While the company is an active supplier of military-grade components, its products are primarily dual-use and do not fall under the specific prohibitions of § 3(1)(a) of the guidelines. The risk in this category is assessed as **Low**.
- **Conduct-Based Risk (§ 4):** The company exhibits a pattern of conduct that raises serious concerns across multiple criteria:
    - **Gross Economic Crime (§ 4g):** There is extensive, multi-jurisdictional evidence of systemic anticompetitive and monopolistic practices. Formal investigations by the U.S. Federal Trade Commission (FTC) and the European Commission (EC) have resulted in consent orders and legally binding commitments to cease exclusionary conduct. This pattern appears to be continuing with the company's post-acquisition strategy for VMware, indicating a high and ongoing risk of gross economic crime. The risk in this category is assessed as **High**.
    - **Human Rights (§ 4a):** A significant discrepancy exists between Broadcom's comprehensive human rights policies and its poor performance in independent benchmarks. Allegations of exposure to Uyghur forced labor risk within its supply

chain, coupled with a lack of detailed public disclosure on mitigation efforts for this specific risk, present an unacceptable risk of contribution to human rights violations. The risk in this category is assessed as **Moderate**.
    - **Severe Environmental Damage (§ 4e):** Credible reports indicate that Broadcom's post-acquisition business model, which involves terminating support for older hardware and enforcing restrictive software licensing, leads to the premature obsolescence of functional equipment. This practice is a direct contributor to the growing global problem of electronic waste (e-waste). The risk in this category is assessed as **Moderate**.
- **Geopolitical Conflict Risk (§ 4b & § 4c):** There is credible, multi-source evidence that Broadcom-manufactured semiconductor components are being used in advanced Russian weapon systems, including cruise missiles and fighter jets, deployed in the full-scale invasion of Ukraine. These weapons have been used in attacks constituting serious violations of international law. While the components are likely diverted through indirect channels, Broadcom's repeated failure to publicly respond to inquiries on this matter demonstrates a lack of transparency and adequate due diligence concerning a severe and ongoing norm violation. This creates an unacceptable risk that the company is contributing to serious violations of individuals' rights in a war situation. The risk in this category is assessed as **High**.

The cumulative weight of these findings, particularly the high risks associated with systemic economic misconduct and the documented link to an active armed conflict, indicates significant ethical failings. The company's mitigating actions are insufficient, and its responsiveness to allegations is inconsistent and inadequate.

Summary of Findings against Oljefondet Ethical Guidelines

Guideline Clause	Risk Area	Summary of Findings for Broadcom Inc.	Assessed Risk Level
§ 3(1)(a)	Prohibited Weapons Components	Produces military-grade, dual-use components but no evidence of producing "key components" designed or	Low

		adapted solely for weapons that violate fundamental humanitarian principles.	
§ 4(a)	Gross or Systematic Human Rights Violations	Strong corporate policies are contradicted by very low external benchmark scores and a lack of transparency regarding specific Uyghur forced labor risks in the supply chain.	Moderate
§ 4(b) & § 4(c)	Violations in War / Sale of Weapons to States in Conflict	Widespread, documented presence of components in advanced Russian weapon systems used in Ukraine, obtained via indirect supply chains. The company has not publicly responded to inquiries on this issue.	High
§ 4(e)	Severe Environmental Damage	Business practices following acquisitions are credibly linked to forced hardware obsolescence and the generation of significant e-waste,	Moderate

		contributing to severe environmental harm.	
§ 4(g)	Gross Economic Crime	A systemic, multi-year pattern of monopolistic and anticompetitive conduct confirmed by consent orders and legally binding commitments with both U.S. and EU regulators.	High

Final Recommendation: Based on the comprehensive analysis of the available evidence, and after consideration of mitigating factors, this report assigns Broadcom Inc. a final risk categorization of **3 - Moderate Risk**. While the company presents high risk in two distinct areas, the "generous assessment" principle allows for a period of observation and engagement. However, should the company fail to demonstrate significant improvement in its antitrust conduct, supply chain due diligence related to conflict zones, and transparency on human rights, a re-evaluation toward a higher risk category would be warranted.

Introduction and Corporate Profile of Broadcom Inc.

Corporate Overview

Broadcom Inc. (NASDAQ: AVGO) is an American multinational technology company headquartered in San Jose, California, positioned as a global leader in the design, development, and supply of a wide range of semiconductor and infrastructure software products.[2] The company's lineage traces back to Hewlett-Packard's semiconductor division, established in 1961, which later became part of Agilent Technologies before being acquired by private equity firms to form Avago Technologies in 2005.[2] The modern Broadcom Inc. was

formed through the landmark acquisition of Broadcom Corporation by Avago Technologies in 2016.[5]

Broadcom's growth has been defined by a highly aggressive and successful strategy of large-scale acquisitions. Beyond the foundational merger, the company has integrated numerous major technology firms, including LSI Corporation (2013), Brocade Communication Systems (2017), CA Technologies (2018), and the enterprise security business of Symantec (2019).[2] Most recently, Broadcom completed its acquisition of VMware in late 2023, a move that significantly expanded its footprint in the enterprise software and private cloud markets.[7] This history is fundamental to understanding the company's business model, which often involves acquiring companies with dominant market positions in mission-critical technologies and subsequently restructuring their operations and licensing models to maximize profitability. This recurring post-acquisition playbook has become a defining characteristic of the company's corporate conduct and a primary source of ethical and regulatory risk.

Business Segments and Revenue

Broadcom operates through two primary business segments: Semiconductor Solutions and Infrastructure Software. For fiscal year 2024, the company reported total net revenue of $51.6 billion.[8]

1. **Semiconductor Solutions:** This segment constitutes the larger portion of the business, accounting for approximately 58% of fiscal 2024 revenue.[2] It encompasses a vast portfolio of products serving critical markets, including networking, broadband, wireless, storage, and industrial applications. Key products include Ethernet switches and routers for data centers, modem chips for broadband access, Wi-Fi and Bluetooth chipsets for mobile devices, and storage controllers for enterprise systems.[3] The company holds a dominant market position in many of these categories, driven by a broad intellectual property portfolio of approximately 20,000 patents and significant investment in research and development.[9]
2. **Infrastructure Software:** This segment has grown substantially through acquisitions and represented approximately 42% of fiscal 2024 revenue.[2] It provides mission-critical software for enterprise clients, focusing on areas such as mainframe computing (from CA Technologies), cybersecurity (from Symantec), and, most significantly, private and hybrid cloud virtualization (from VMware).[3] The strategy in this segment is to provide comprehensive, integrated solutions that are deeply embedded in the IT infrastructure of large organizations.[5]

Global Footprint and Market Position

Broadcom operates on a global scale, with a highly diversified geographic revenue base. For the twelve months ended in 2024, the Asia Pacific region was the largest market, accounting for 55.1% of total sales, followed by the Americas at 29.0% and Europe, the Middle East, and Africa (EMEA) at 15.9%.[11] Within Asia, China (including Hong Kong) and Singapore are particularly significant markets, representing 20.3% and 18.5% of total sales, respectively.[11]

The company's products are integral to the supply chains of many of the world's largest technology and telecommunications firms. Its leading customers include major original equipment manufacturers (OEMs) and service providers such as Apple, Samsung, Cisco, and Huawei.[5] Sales are highly concentrated, with the five largest customers accounting for 48.3% of net revenue in one recent period, with Samsung and Apple representing 21.3% and 13.3%, respectively.[12] This deep integration with key global players underscores the systemic importance of Broadcom's technology while also highlighting the complexity of its multi-tiered supply chains. The company competes with other semiconductor giants like Qualcomm, Intel, and NVIDIA, but has maintained its market leadership through its strategic acquisitions and technological innovation.[3]

Part 1: Product-Based Risk Assessment (Guidelines § 3)

This section assesses Broadcom Inc.'s product portfolio against the criteria for product-based observation and exclusion outlined in § 3 of the Fund's ethical guidelines. The analysis focuses specifically on § 3(1)(a), which prohibits investment in companies that develop or produce "weapons or central components to weapons which by normal application violate fundamental humanitarian principles".[1] The assessment finds no grounds for exclusion under this section.

Analysis of Military and Dual-Use Product Lines

Broadcom is an established and active supplier to the military and aerospace sectors. The company designs, manufactures, and markets a specific product line of "hermetic optocouplers" that are explicitly intended for high-reliability applications, including "military

and aerospace," "transportation, medical, and life-critical systems".[13] These components are designed to operate under extreme conditions, with a guaranteed performance range from -55°C to 125°C.[15]

Significantly, these products are manufactured and tested on a MIL-PRF-38534 certified line, a U.S. military performance specification for microcircuits. Furthermore, Broadcom is listed on the Defense Supply Center Columbus (DSCC) Qualified Manufacturers List (QML-38534) for Hybrid Microcircuits.[15] This demonstrates that Broadcom knowingly and deliberately participates in the regulated U.S. military and defense supply chain, producing components that meet stringent military standards. Beyond these specific hardware components, Broadcom's software divisions also provide solutions to government and defense clients. The company's federal solutions portfolio includes cybersecurity software (Symantec) and modern private cloud platforms (VMware) designed to help government agencies "execute your mission" and "protect critical resources and confidential data".[16] This indicates a deep and ongoing business relationship with government and defense entities, extending beyond just the supply of discrete electronic components.[17]

Assessment of Involvement in Prohibited Weapons (§ 3(1)(a))

While Broadcom's role as a military supplier is clearly established, the critical test under § 3(1)(a) is whether its products constitute "key components" for weapons that are themselves prohibited. Prohibited weapon categories include nuclear weapons, chemical and biological weapons, anti-personnel mines, and cluster munitions.[1] A "key component" is generally understood to be an item specifically designed, developed, or adapted for sole use in a prohibited weapon, and which is critical for that weapon's functioning.[18] General-purpose or "dual-use" components, which can be used in a wide range of both civilian and military applications, typically do not meet this threshold.

A thorough review of Broadcom's product lines and available evidence reveals no direct involvement in the production of such key components for prohibited weapons:

- **Nuclear Weapons:** There is no evidence to suggest that Broadcom manufactures components, such as guidance or fissile material systems, that are designed or adapted exclusively for use in nuclear weapons or their specific delivery platforms.[19] The components it supplies to the military are general-purpose electronics valued for their reliability, not for a function unique to a nuclear warhead.
- **Cluster Munitions & Anti-Personnel Mines:** These weapons, particularly less sophisticated variants, often rely on relatively simple mechanical fuzes and casings rather than advanced microelectronics.[22] While modern "smart" submunitions may use more advanced sensors, there is no public information linking Broadcom to the production of

components specifically and solely designed for the fuzing, guidance, or dispersal mechanisms of cluster munitions or anti-personnel mines.

The components Broadcom supplies to the military sector, such as its hermetic optocouplers, are fundamentally dual-use. They are designed for high performance in harsh environments, making them suitable for a wide array of applications from aerospace and industrial automation to various defense systems.[13] Their utility is not specific to any single type of weapon, let alone one that violates fundamental humanitarian principles.

This assessment is corroborated by external, third-party evaluations. Broadcom Inc. is a constituent of the "MSCI World ex Controversial Weapons Index," which explicitly screens out companies involved in such weapons.[27] Similarly, a factsheet from the investment management firm Invesco for one of its funds shows Broadcom as having 0% of its revenue derived from controversial weapons.[28]

In conclusion, the distinction between being a general supplier to the military and being a producer of components for prohibited weapons is critical. Based on the available evidence and the strict definitions within the guidelines, Broadcom falls into the former category but not the latter. Therefore, its products do not meet the criteria for exclusion under § 3(1)(a).

Part 2: Conduct-Based Risk Assessment (Guidelines § 4)

This section evaluates Broadcom's corporate conduct against the criteria for observation or exclusion detailed in § 4 of the guidelines. The analysis reveals a pattern of behavior that presents an unacceptable risk of contribution to "gross economic crime" (§ 4g), "severe environmental damage" (§ 4e), and "gross or systematic violations of human rights" (§ 4a). The risks identified are not isolated incidents but appear to be systemic outcomes of the company's core business strategy.

Systematic Economic Crime: A History of Antitrust and Monopolistic Conduct (§ 4g)

The guideline for § 4g allows for exclusion where there is an unacceptable risk that a company is responsible for "gross corruption or other gross economic crime".[1] Broadcom's history of

leveraging its market dominance through anticompetitive practices, which has prompted formal enforcement actions by regulators in both the United States and Europe, constitutes a clear and ongoing risk under this criterion. This conduct is not ancillary to its business but appears to be a central pillar of its strategy for extracting value from acquired companies.

U.S. Federal Trade Commission (FTC) Investigation (Docket C-4750)

In July 2021, the U.S. Federal Trade Commission issued a formal complaint charging Broadcom with illegally monopolizing markets for semiconductor components used in set-top boxes and broadband internet devices.[29] The FTC's investigation found that Broadcom possessed monopoly power in three specific chip markets and used this power to maintain its dominance through anticompetitive means.[29]

The core of the FTC's complaint was that Broadcom entered into long-term, exclusive, or near-exclusive supply agreements with at least ten major Original Equipment Manufacturers (OEMs) and key service providers.[29] These agreements allegedly prevented customers from purchasing chips from Broadcom's competitors. The FTC alleged that Broadcom secured these terms by threatening to withhold its essential, monopolized products or charge significantly higher prices to customers who did not grant Broadcom exclusivity for other, related components where it faced more competition.[30] This conduct was found to have created "insurmountable barriers" for competitors, foreclosing them from a substantial share of the market and harming competition.[29]

The matter was settled via a consent order (C-4750), finalized in November 2021.[31] Under the terms of the order, Broadcom is legally prohibited from entering into certain types of exclusivity or loyalty agreements with its customers for these key chips. The order also explicitly forbids Broadcom from conditioning the supply or pricing of its monopolized chips on a customer's commitment to source other chips exclusively from Broadcom, and it prohibits retaliating against customers for doing business with competitors.[29]

European Commission (EC) Investigation (Case AT.40608)

Parallel to the FTC's action, the European Commission launched its own formal antitrust investigation in June 2019 into Broadcom's practices in the markets for TV and modem chipsets.[34] The EC's concerns mirrored those of the FTC, focusing on contractual clauses that imposed exclusive or quasi-exclusive purchasing obligations on customers, as well as product

bundling and other leveraging strategies.[34]

The EC determined that the risk of harm to competition was so immediate and significant that it took the rare step of imposing "interim measures" in October 2019—the first such action in an antitrust case in 18 years.[35] These measures legally required Broadcom to suspend the application of the contentious exclusivity clauses while the full investigation proceeded, with the EC arguing that without such intervention, Broadcom's conduct could result in the "elimination or marginalisation of competitors" and cause "serious and irreparable harm to competition".[34]

The investigation was ultimately closed in October 2020 after Broadcom offered legally binding commitments to address the EC's concerns.[35] For a period of seven years, Broadcom committed to not apply exclusivity provisions in its agreements with TV and modem manufacturers in the European Economic Area (EEA) and to not condition the supply of certain chips on the customer buying other Broadcom products.[35] The acceptance of these commitments resolved the case without a formal finding of infringement, but it underscored the severity of the anticompetitive conduct alleged.

Post-Acquisition Conduct and Ongoing Concerns (VMware)

Despite the regulatory actions in the U.S. and EU, there is substantial evidence that Broadcom continues to employ a similar playbook. Following its acquisition of VMware, Broadcom has implemented sweeping changes to VMware's licensing and sales models that have drawn widespread condemnation from customers and partners, and which are now the subject of new legal and regulatory challenges.

In early 2024, Broadcom announced the discontinuation of all perpetual licenses for VMware software, forcing all customers onto a subscription-based model.[6] It also eliminated the ability to purchase products à la carte, bundling numerous services into two large, expensive packages.[6] This has resulted in dramatic price increases for many customers, with reports of costs rising by 800% to 1,500%.[41]

This conduct has been characterized by critics and customers as a coercive strategy to leverage VMware's dominance in server virtualization software. In April 2025, United Health Group filed a lawsuit against Broadcom, alleging that the company was refusing to honor its existing contractual commitments and was attempting to "coerce United into paying hundreds of millions of dollars more" for access to mission-critical software.[42] The lawsuit explicitly links Broadcom's current actions with its history of leveraging market power acquired through acquisitions like CA Technologies.[42]

Furthermore, the European cloud provider association CISPE has filed a formal appeal with the European General Court, seeking to annul the EC's approval of the VMware acquisition.[43] CISPE alleges that the EC failed to impose adequate conditions to prevent Broadcom from abusing its newly strengthened dominant position, and that Broadcom's subsequent actions—including terminating contracts and imposing "exorbitant costs"—are harming competition in the European cloud market.[41]

The consistency of this behavior across different acquisitions, markets, and jurisdictions demonstrates a systemic corporate strategy. This pattern of leveraging market dominance through exclusionary and coercive tactics, which has been repeatedly identified and sanctioned by major global regulators, constitutes a high risk of ongoing involvement in "gross economic crime" as defined by § 4g of the guidelines.

History of Antitrust Investigations and Regulatory Actions

Regulatory Body	Case/Docket No.	Key Allegations	Resolution	Date
U.S. Federal Trade Commission (FTC)	C-4750	Illegal monopolization of semiconductor markets through exclusive dealing, loyalty agreements, and coercive tactics.	Consent Order prohibiting exclusivity and retaliation.	2021
European Commission (EC)	AT.40608	Abuse of dominant position through exclusivity provisions, rebates, and product	Legally binding commitments to cease practices for 7 years.	2020

		bundling in TV/modem chipset markets.		
European General Court	(Appeal Filed)	Appeal by CISPE challenging EC's approval of the VMware acquisition, citing subsequent abuse of dominance.	Pending	2025
U.S. District Court	0:25-cv-01189	Lawsuit by United Health Group alleging breach of contract and coercive pricing for CA software post-acquisitio n.	Pending	2025

Human Rights in the Supply Chain (§ 4a)

Under § 4a, a company may be excluded if there is an unacceptable risk of contribution to "gross or systematic violations of human rights".[1] While Broadcom has established comprehensive policies on human rights, there is a notable gap between these commitments and the company's performance as assessed by independent organizations, particularly concerning transparency in its complex global supply chain.

Broadcom has a robust set of public-facing policies, including its Human Rights Principles, a Supplier Environmental and Social Responsibility Code of Conduct based on the Responsible Business Alliance (RBA) Code, and annual Statements Against Modern Slavery and Human

Trafficking.[45] These documents affirm the company's commitment to freely chosen employment, non-discrimination, and the elimination of forced and child labor.[46] The company states it conducts supplier surveys, audits, and human rights impact assessments, and has found no instances of forced labor in its operations or among surveyed suppliers.[48]

However, external evaluations paint a different picture. The 2022 Corporate Human Rights Benchmark (CHRB) awarded Broadcom a score of just 13.3 out of 100, indicating very weak performance on human rights due diligence and transparency.[51] Similarly, KnowTheChain, an initiative that benchmarks corporate efforts to address forced labor, noted in a 2018 report that Broadcom had "reduced its public disclosure dramatically," leading to an 81% decrease in its score.[52] More recently, KnowTheChain's 2025 scorecard identified one allegation of forced labor in Broadcom's supply chains related to alleged Uyghur forced labor.[54]

This specific allegation is of high concern. The use of state-sponsored forced labor of Uyghurs and other ethnic minorities in China is a well-documented and severe human rights crisis, with particular risks in the electronics supply chain.[55] While Broadcom's general policies prohibit forced labor, the company does not provide specific public disclosure on the steps it has taken to trace its supply chain and address the particular risks of Uyghur forced labor, especially in lower tiers beyond its direct suppliers.[54] This lack of transparency on a salient, severe, and systematic human rights issue is a significant deficiency. The discrepancy between the company's extensive policy framework and its poor external ratings and lack of disclosure on a critical risk creates a moderate, yet unacceptable, risk of contribution to human rights violations under § 4a.

Severe Environmental Damage: The E-Waste Controversy (§ 4e)

The guideline for § 4e addresses acts or omissions that lead to "severe environmental damage".[1] Broadcom maintains a formal environmental program, including a commitment to reduce its Scope 1 and 2 GHG emissions by 38% by 2030, alignment with the ISO 14001 environmental management standard, and an EcoVadis Silver Medal for its sustainability efforts.[7]

However, there are credible and serious allegations that the company's core business practices directly contribute to severe environmental damage through the generation of electronic waste (e-waste). This issue stems from the same post-acquisition strategy that drives its anticompetitive conduct. Critics and industry groups argue that by unilaterally ending support for older but still functional hardware (such as Brocade network switches) and by forcing customers to abandon perpetual software licenses (as with VMware), Broadcom renders vast quantities of serviceable IT equipment obsolete by policy, not by technical

necessity.[6]

This forced obsolescence pushes customers to discard hardware that would otherwise have a much longer useful life, directly fueling the global e-waste crisis, which the United Nations has identified as the world's fastest-growing domestic waste stream.[62] Discarded electronic hardware often releases toxic materials like lead, mercury, and cadmium into the environment.[62] This conduct is particularly concerning given that Broadcom's own policy statement regarding the European WEEE (Waste from Electrical and Electronic Equipment) Directive explicitly disclaims legal responsibility for the take-back and management of its products at their end of life, shifting the burden onto its partners.[63] This stance is problematic, especially as the company is headquartered in California, a state with stringent laws classifying e-waste as hazardous and regulating its disposal.[64]

The connection between Broadcom's profit-driven business model and the resulting environmental harm is direct. The practice of forcing hardware upgrades through software policy changes is not an incidental byproduct of its operations but a central element of its strategy to maximize revenue from its acquired assets. This conduct, which limits reuse and promotes premature disposal of hardware on a potentially massive scale, represents a significant contribution to a severe environmental problem, creating a moderate risk under § 4e.

Part 3: Geopolitical Conflict Risk Exposure (Guidelines § 4c & § 4b)

This section assesses the unacceptable risk that Broadcom contributes to "serious violations of individuals' rights in war or conflict situations" (§ 4b) and the "sale of weapons to states in armed conflicts which benytter våpnene [use the weapons] on måter [in ways] that constitute serious and systematic breaches of international law's rules for hostilities" (§ 4c).[1] The analysis finds a high risk of contribution, not through direct sales, but through the persistent and documented presence of its components in Russian weapon systems used in Ukraine, combined with an inadequate corporate response to this known risk.

Documented Presence of Broadcom Components in the Ukraine Conflict

Since Russia's full-scale invasion of Ukraine in February 2022, a substantial body of evidence has emerged from multiple independent and credible sources identifying Broadcom-manufactured components in a variety of advanced Russian weapon systems. These are not isolated findings but represent a consistent pattern across different types of munitions and platforms used in attacks that have resulted in widespread civilian casualties and destruction of civilian infrastructure, in violation of international humanitarian law.

- **Cruise Missiles:** A report by the Royal United Services Institute (RUSI), a highly respected UK defense think-tank, found that a Russian 9M727 Iskander cruise missile contained multiple foreign components, including some from Broadcom.[65] These advanced weapons have been used extensively to strike targets deep inside Ukraine.
- **North Korean Missiles:** An investigation by Ukraine's Independent Anti-Corruption Commission (NAKO) analyzed a North Korean KN-23/24 ballistic missile, supplied to and used by Russia against Ukraine, and found that it contained microelectronics from Western manufacturers, including Broadcom.[67] Some of the components were produced as recently as 2023, long after comprehensive sanctions were in place.[69]
- **General Findings:** Broader investigations have repeatedly named Broadcom as one of the key Western companies whose components are found in Russian military equipment. A RUSI analysis of 27 different Russian systems found that US-made components were predominant, and Broadcom was among the companies identified.[65] The Ukrainian government has also published a database of Western components found in Russian armaments which includes Broadcom parts.[71] A U.S. Senate investigation into the presence of American technology in Russian weapons also highlighted the issue, noting that such components are essential for Russia's ability to produce and operate these systems.[73]

The presence of these components is critical for Russia's war effort. As one expert noted, "They can't build missiles without it".[76] The components are not incidental; they are integral to the guidance, communication, and control systems of the weapons being used to commit systematic violations of international law.

Analysis of Culpability and Supply Chain Integrity

It is highly unlikely that Broadcom is selling these components directly to the Russian military or its suppliers. The components are overwhelmingly dual-use, meaning they have legitimate civilian applications and are not typically subject to the strictest export controls prior to the 2022 invasion.[65] The established route for these components into Russia is through a complex network of distributors and intermediaries in third countries, including China, Hong Kong, Turkey, and Serbia, which serve to obfuscate the true end-user.[65] This is a widespread

challenge affecting the entire semiconductor industry.

However, under the Fund's guidelines, the assessment hinges on whether there is an "unacceptable risk" of *contribution* and whether the company is doing what can be reasonably expected to reduce that risk [§ 4, § 6].[1] In this context, Broadcom's response to these public revelations is a critical factor.

Broadcom maintains a formal export control policy, stating its intent to comply with international trade regulations and providing a system for classifying its products with export control codes (ECCNs).[79] Following the invasion, VMware (now a Broadcom division) issued a clear statement suspending all business operations in Russia and Belarus.[81]

Despite these policies, Broadcom Inc.'s response regarding its semiconductor components has been notably deficient. The Business & Human Rights Resource Centre, a respected NGO, has reached out to numerous companies whose components were identified in Russian or North Korean weapons. On multiple occasions, their records indicate that while other companies like Analog Devices, NXP, and STMicroelectronics provided responses detailing their compliance efforts, Broadcom and its subsidiary Avago did not respond.[68]

This persistent silence in the face of specific, credible, and severe allegations is a significant failure of corporate responsibility and due diligence. While stopping all diversion is impossible, a responsible company is expected to publicly acknowledge the issue, detail the steps it is taking to investigate its supply chains, and engage with governments and civil society to strengthen controls. Broadcom's lack of a public response suggests an unwillingness to transparently address its role in a supply chain that is directly enabling systematic violations of international humanitarian law. This failure to act and communicate elevates the situation from a general industry problem to a specific company-level risk of an unacceptable nature, thereby meeting the threshold for a high-risk assessment under § 4b and § 4c.

Part 4: Evaluation of Mitigating Factors and Forward-Looking Assessment (Guidelines § 6)

According to § 6 of the guidelines, the assessment of whether to exclude a company must consider forward-looking factors, including the probability of future norm violations and whether the company is doing what can be reasonably expected to reduce that risk.[1] This includes evaluating the company's governance, policies, and responsiveness to past violations. An analysis of Broadcom's mitigating factors reveals a compliance framework that appears more reactive than proactive and whose effectiveness is questionable given the

recurring nature of the identified risks.

Effectiveness of Corporate Governance and Compliance Programs

Broadcom has established formal governance structures for overseeing ethical issues. Its Board of Directors includes a Nominating, Environmental, Social and Governance (NESG) Committee responsible for overseeing the company's ESG programs, including environmental sustainability and human rights.[60] This is supported by an ESG Steering Committee composed of senior leaders, including the CFO and Chief Legal Officer, which meets quarterly.[7] The company publishes annual Corporate Responsibility Reports and has a Code of Ethics and Business Conduct that all employees are required to follow.[7]

However, the effectiveness of these programs is undermined by the company's actual conduct. The repeated and systemic nature of the anticompetitive practices across multiple jurisdictions and acquisitions suggests that the compliance programs have failed to prevent "gross economic crime." Similarly, the significant gap between the company's human rights policies and its low scores in independent benchmarks indicates that the governance structures are not translating into effective due diligence and transparent reporting in the supply chain.[51] The governance framework appears sufficient for documenting policies and reporting on favorable metrics (like GHG emissions) but is demonstrably ineffective at preventing or mitigating the most severe conduct-based risks identified in this report.

Company Responsiveness to Norm Violations

Broadcom's responsiveness to norm violations is highly inconsistent and appears to be dictated by legal and regulatory pressure rather than a consistent ethical commitment.

- **On Antitrust and Economic Conduct:** When faced with formal investigations by powerful regulators like the FTC and EC, Broadcom engages, negotiates, and ultimately agrees to legally binding consent orders and commitments.[29] This demonstrates a capacity and willingness to alter its conduct when legally compelled to do so. However, the fact that the behavior persists until such formal action is taken, and then appears to re-emerge in new contexts like the VMware acquisition, suggests a strategy of pushing legal boundaries rather than proactively adhering to ethical norms of fair competition.
- **On Human Rights and Conflict Exposure:** In stark contrast, the company's response to credible reports about human rights risks in its supply chain and the use of its components in the Ukraine conflict has been one of public silence.[68] This lack of

engagement and transparency on issues of grave ethical concern, where the immediate legal liability may be less direct, is a significant negative factor. It indicates a failure to do what can be "expected to reduce the risk of future normbrudd".[1] A responsible company would proactively investigate, report on its findings, and detail its enhanced due diligence measures. Broadcom's failure to do so suggests that these issues are not prioritized by its governance and compliance functions in the absence of direct regulatory enforcement.

Probability of Future Norm Violations

The forward-looking assessment indicates a high probability of future norm violations.

1. **Economic Crime:** The company's business model is fundamentally reliant on acquiring companies with dominant market positions and aggressively restructuring them for profit. As long as this remains its core strategy, it is highly probable that it will continue to engage in conduct that attracts antitrust scrutiny from regulators and legal challenges from customers. The ongoing controversies surrounding VMware suggest this pattern is already repeating.
2. **Conflict Exposure:** The global semiconductor supply chain is notoriously complex and difficult to monitor. Without a significant and transparent enhancement of its due diligence, end-user verification, and distributor auditing processes, it is highly probable that Broadcom's dual-use components will continue to be diverted to sanctioned entities and conflict zones. The company's lack of public engagement on the issue provides no assurance that it is taking the necessary steps to mitigate this risk.

In summary, while Broadcom possesses the formal structures for ethical governance, their practical application is inconsistent and appears insufficient to prevent recurring, serious norm violations. The company's responsiveness is selective, and the probability of future violations in key risk areas remains high.

Conclusion and Final Risk Categorization

This comprehensive assessment of Broadcom Inc. has evaluated the company's products and conduct against the ethical guidelines of the Government Pension Fund Global. The analysis concludes that while the company is not in breach of the product-based criteria, its conduct presents a range of serious and systemic ethical risks that warrant a high level of concern.

The investigation confirms that Broadcom does not develop or produce key components for weapons prohibited under § 3 of the guidelines. Its involvement in the military sector is limited to the supply of dual-use components, which does not meet the threshold for exclusion on product-based grounds.

However, the company's conduct demonstrates a clear and persistent pattern of norm violations under § 4. The risk of involvement in **"gross economic crime" (§ 4g)** is assessed as **high**. This is not based on a single incident, but on a well-documented, multi-year history of monopolistic and anticompetitive practices that have been subject to formal enforcement actions by both U.S. and EU regulators. The continuation of this behavioral pattern in the context of the recent VMware acquisition indicates that this is a systemic and ongoing risk embedded in the company's core business strategy.

Furthermore, the risk of contribution to **"serious violations of individuals' rights in war or conflict situations" (§ 4b and § 4c)** is also assessed as **high**. This conclusion is based on extensive, credible evidence showing Broadcom components in advanced Russian weapon systems being used to commit violations of international humanitarian law in Ukraine. While the supply is indirect, the company's failure to adequately and transparently respond to these severe and repeated findings represents a significant failure of corporate responsibility and due diligence, creating an unacceptable risk of contribution to the conflict.

In addition to these high-risk areas, the company presents **moderate risks** of contributing to **"gross or systematic violations of human rights" (§ 4a)** through a lack of transparency in its supply chain, particularly regarding Uyghur forced labor risks, and of causing **"severe environmental damage" (§ 4e)** through business practices that promote forced hardware obsolescence and generate e-waste.

The principle of a "generous assessment" requires a careful weighing of these risks against mitigating factors. Broadcom has formal governance and compliance policies in place. However, their effectiveness is severely undermined by the company's recurring misconduct. The company's responsiveness is inconsistent; it reacts to regulatory pressure but remains silent on other grave ethical issues. The confluence of two distinct, high-risk findings—one concerning systemic economic misconduct and the other concerning direct links to a major armed conflict—presents a compelling case that the company's conduct falls well below the ethical standards expected of investments by the Fund. The systemic nature of the antitrust violations and the severity of the components' use in Ukraine, combined with the company's inadequate response, are serious enough to warrant a significant risk rating.

Final Risk Category Recommendation

Based on the cumulative weight of the evidence, the systemic nature of the violations, and the high probability of future norm breaches, the final recommended risk category for Broadcom Inc. is:

3 - Moderate Risk

Justification: While the company's conduct presents high risk in two distinct and severe areas (§ 4g and § 4b/c), the "generous assessment" principle suggests that immediate exclusion may be premature. A classification of "Moderate Risk" allows the Fund to place the company under observation, engage in active ownership to demand specific and measurable improvements, and re-evaluate its status based on its response. Key areas for engagement should include demanding:

1. A transparent, third-party audit of its supply chain controls to prevent diversion of components to sanctioned entities and conflict zones.
2. Public reporting on specific due diligence measures taken to address Uyghur forced labor risks.
3. A commitment to reform post-acquisition business practices that lead to anticompetitive outcomes and generate excessive e-waste.

Failure to demonstrate substantial progress in these areas within a reasonable timeframe would provide strong grounds for escalating the risk category to "High Risk" or "Exclusion Candidate."

Works cited

1. etchical_guidelines.pdf
2. Broadcom - Wikipedia, accessed on August 18, 2025, https://en.wikipedia.org/wiki/Broadcom
3. Broadcom Inc. (AVGO) Business Profile - stockrow, accessed on August 18, 2025, https://stockrow.com/AVGO/business-profile
4. About Us, accessed on August 18, 2025, https://www.broadcom.com/company/about-us
5. Broadcom Inc.: A Deep Dive into Its Semiconductor Dominance | by Salman Aziz | Medium, accessed on August 18, 2025, https://medium.com/@armourstocks.com/broadcom-inc-a-deep-dive-into-its-semiconductor-dominance-f41c2a5e6518
6. The Environmental Ripple of Broadcom's Market Moves - Free ICT Europe, accessed on August 18, 2025, https://www.freeict.eu/news/the-environmental-ripple-of-broadcoms-market-moves
7. Broadcom® 2023 ESG Report - Responsibility Reports, accessed on August 18, 2025, https://www.responsibilityreports.com/HostedData/ResponsibilityReportArchive/b/NASDAQ_AVGO_2023.pdf

8. Broadcom Inc. Announces Fourth Quarter and Fiscal Year 2024 Financial Results and Quarterly Dividend, accessed on August 18, 2025, https://investors.broadcom.com/news-releases/news-release-details/broadcom-inc-announces-fourth-quarter-and-fiscal-year-2024
9. Broadcom Company Overview, accessed on August 18, 2025, https://investors.broadcom.com/static-files/602c2fd3-89a0-436f-b638-4890f20feda7
10. Broadcom Corporation - Wikipedia, accessed on August 18, 2025, https://en.wikipedia.org/wiki/Broadcom_Corporation
11. Description of Broadcom Inc's Business Segments - AVGO - CSIMarket, accessed on August 18, 2025, https://csimarket.com/stocks/segments.php?code=AVGO
12. Broadcom Inc Customers by Division and Industry - CSIMarket, accessed on August 18, 2025, https://csimarket.com/stocks/markets_glance.php?code=AVGO
13. HCPL-6630 - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/products/optocouplers/hermetic/ac-dc-to-logic-interface/hcpl-6630
14. Products - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/products
15. Hermetic Optocouplers - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/products/optocouplers/hermetic
16. Modernize infrastructure | Support mission-critical operations - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/solutions/industry/federal
17. [PDF]2024 Annual Report - Broadcom Inc., accessed on August 18, 2025, https://investors.broadcom.com/static-files/752e631c-b5f3-46af-9d67-bdeb658f5fa2
18. Decision to exclude companies that produce controversial weapons - KLP, accessed on August 18, 2025, https://www.klp.no/en/corporate-responsibility-and-responsible-investments/exclusion-and-dialogue/Decision%20to%20exclude%20companies%20that%20produce%20controversial%20weapons.pdf
19. Nuclear weapons delivery - Wikipedia, accessed on August 18, 2025, https://en.wikipedia.org/wiki/Nuclear_weapons_delivery
20. TRANSCRIPT: Remarks: Donald Trump Announces A Major Investment by Apple in Manufacturing - 08.06.2025 - Senate Democrats, accessed on August 18, 2025, https://www.democrats.senate.gov/newsroom/trump-transcripts/transcript-remarks-donald-trump-announces-a-major-investment-by-apple-in-manufacturing_-08062025
21. KHNP secures Czech nuclear project, commits to major equipment purchases and royalties, accessed on August 18, 2025, https://biz.chosun.com/en/en-industry/2025/08/18/LVRSKCSXHVCIXLVLEPYFDJZHB4/
22. Cluster munition - Wikipedia, accessed on August 18, 2025, https://en.wikipedia.org/wiki/Cluster_munition
23. PMN mine - Wikipedia, accessed on August 18, 2025,

https://en.wikipedia.org/wiki/PMN_mine
24. Anti-personnel mine - Wikipedia, accessed on August 18, 2025, https://en.wikipedia.org/wiki/Anti-personnel_mine
25. Optocouplers and Opto-Isolators, accessed on August 18, 2025, https://www.broadcom.com/products/optocouplers
26. 5962-8957001, accessed on August 18, 2025, https://www.broadcom.com/products/optocouplers/hermetic/digital-optocouplers/20mbd/5962-8957001
27. MSCI World ex Controversial Weapons Index (USD), accessed on August 18, 2025, https://www.msci.com/documents/10199/84bf24dc-d9ce-4a2b-84fa-a12db8c46b41
28. Invesco Global Equity Income Advantage Fund C-Acc Shares, accessed on August 18, 2025, https://www.invesco.com/content/dam/invesco/ch/en/product-documents/gpr/share-class/factsheet/LU2471135173_factsheet_EN-CH.pdf
29. FTC Charges Broadcom with Illegal Monopolization and Orders the Semiconductor Supplier to Cease its Anticompetitive Conduct, accessed on August 18, 2025, https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-charges-broadcom-illegal-monopolization-orders-semiconductor-supplier-cease-its-anticompetitive
30. Broadcom Limited II: Complaint - Federal Trade Commission, accessed on August 18, 2025, https://www.ftc.gov/system/files/documents/cases/1810205c4750broadcomcomplaint.pdf
31. Broadcom Incorporated, In the Matter of | Federal Trade Commission, accessed on August 18, 2025, https://www.ftc.gov/legal-library/browse/cases-proceedings/181-0205-broadcom-incorporated-matter
32. Broadcom: Decision and Order (Public) - Federal Trade Commission, accessed on August 18, 2025, https://www.ftc.gov/system/files/documents/cases/1810205broadcomorder.pdf
33. Broadcom Limited II: Decision and Order - Federal Trade Commission, accessed on August 18, 2025, https://www.ftc.gov/system/files/documents/cases/1810205c4750broadcomfinalorder.pdf
34. Antitrust: Inquiry into Broadcom's exclusivity practices - European Commission, accessed on August 18, 2025, https://ec.europa.eu/commission/presscorner/detail/sv/ip_19_3410
35. Antitrust: Commission accepts commitments by Broadcom, accessed on August 18, 2025, https://ec.europa.eu/commission/presscorner/detail/sl/ip_20_1852
36. The Broadcom case: EU antitrust commitments and interim measures, accessed on August 18, 2025, https://www.nortonrosefulbright.com/es-es/knowledge/video/1d78cc56/the-broadcom-case-eu-antitrust-commitments-and-interim-measures

37. The EC announces interim measures in Broadcom investigation for the first time in 18 years, accessed on August 18, 2025, https://www.hausfeld.com/what-we-think/publications/the-ec-announces-interim-measures-in-broadcom-investigation-for-the-first-time-in-18-years
38. CASE AT.40608 - Broadcom ANTITRUST PROCEDURE Council Regulation (EC) 1/2003 Article 8 Regulation (EC) 1/2003 Date: 16/10/2019 - European Commission, accessed on August 18, 2025, https://ec.europa.eu/competition/antitrust/cases/dec_docs/40608/40608_2791_11.pdf
39. AT.40608 - Broadcom - Competition case search - European Union, accessed on August 18, 2025, https://competition-cases.ec.europa.eu/cases/AT.40608
40. Broadcom is Bullying Enterprises with VMware Audits - It's FOSS News, accessed on August 18, 2025, https://news.itsfoss.com/broadcom-bullying-enterprises/
41. Broadcom Faces EU Scrutiny Over Controversial VMware Licensing Practices, accessed on August 18, 2025, https://licenseware.io/broadcom-faces-eu-scrutiny-over-controversial-vmware-licensing-practices/
42. IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA UNITED HEALTHCARE SERVICES, INC., Plaintiff, v. BROADCOM INC., accessed on August 18, 2025, https://www.loeb.com/-/media/files/pdfs/2025-pdfs/client-alerts/uhcs-redacted-complaint.pdf?rev=56d997fb7f694d03939db01166c9995c&hash=DEBFC0807C008526210BC525B1D6CC99
43. CISPE Takes European Commission to Court to Annul Approval of Broadcom's Acquisition of VMware | CISPE - The Voice of Cloud Infrastructure Service Providers in Europe, accessed on August 18, 2025, https://cispe.cloud/cispe-takes-european-commission-to-court-to-annul-approval-of-broadcoms-acquisition-of-vmware/
44. EU Court examines Broadcom's dominant position after VMware deal (update) - Techzine, accessed on August 18, 2025, https://www.techzine.eu/news/privacy-compliance/133284/eu-court-examines-broadcoms-dominant-position-after-vmware-deal/
45. Workforce | Corporate Responsibility - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/company/corporate-responsibility/workforce
46. Supplier Responsibility | Corporate Responsibility - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/company/corporate-responsibility/supplier-responsibility
47. Human Rights Principles | Broadcom Inc., accessed on August 18, 2025, https://docs.broadcom.com/doc/human-rights-principles
48. Statement Against Modern Slavery and Human Trafficking - Support Documents and Downloads - Broadcom Inc., accessed on August 18, 2025, https://docs.broadcom.com/docs/Broadcom-Statement-Against-Modern-Slavery-and-Human-Trafficking
49. Broadcom Supplier Environmental and Social Responsibility Code of Conduct -

Support Documents and Downloads, accessed on August 18, 2025, https://docs.broadcom.com/docs/1234571
50. Norwegian Transparency Act Report 2024 - Support Documents and Downloads - Broadcom Inc., accessed on August 18, 2025, https://docs.broadcom.com/docs/norwegian-transparency-act-statement-english
51. Broadcom - Corporate Human Rights Benchmark WBA, accessed on August 18, 2025, https://www.worldbenchmarkingalliance.org/publication/chrb/2022/companies/broadcom-4/
52. KnowTheChain Ranks 40 Global Technology Companies on Action Taken to Address Forced Labor in their Supply Chains - PR Newswire, accessed on August 18, 2025, https://www.prnewswire.com/news-releases/knowthechain-ranks-40-global-technology-companies-on-action-taken-to-address-forced-labor-in-their-supply-chains-300667379.html
53. KnowTheChain Ranks 40 Global Technology Companies on Action Taken to Address Forced Labor in their Supply Chains - GoodElectronics, accessed on August 18, 2025, https://goodelectronics.org/knowthechain-ranks-40-global-technology-companies-action-taken-address-forced-labor-supply-chains/
54. Broadcom Inc. (Broadcom) - Business & Human Rights Resource Centre, accessed on August 18, 2025, https://www.business-humanrights.org/documents/41867/2025_KTC_ICT_Scorecard_Broadcom.pdf
55. Forced Labor | U.S. Customs and Border Protection, accessed on August 18, 2025, https://www.cbp.gov/trade/forced-labor
56. Uyghur Forced Labor Prevention Act (UFLPA) Fact Sheet - State Department, accessed on August 18, 2025, https://www.state.gov/office-to-monitor-and-combat-trafficking-in-persons/releases/2025/01/uyghur-forced-labor-prevention-act-uflpa-fact-sheet
57. Forced Labour in the UK's Supply Chains - Parliament UK, accessed on August 18, 2025, https://publications.parliament.uk/pa/jt5901/jtselect/jtrights/633/report.html
58. Xinjiang Supply Chain Business Advisory - United States Department of State, accessed on August 18, 2025, https://www.state.gov/bureau-of-economic-and-business-affairs/xinjiang-supply-chain-business-advisory
59. China's economy runs on Uyghur forced labour | TBIJ, accessed on August 18, 2025, https://www.thebureauinvestigates.com/stories/2025-05-29/chinas-economy-runs-on-uyghur-forced-labour
60. 2022 Environmental, Social & Governance Report - Support Documents and Downloads - Broadcom Inc., accessed on August 18, 2025, https://docs.broadcom.com/docs/environment-social-governance-report-2022
61. Environment | Corporate Responsibility - Broadcom Inc., accessed on August 18,

2025, https://www.broadcom.com/company/corporate-responsibility/environment
62. The Environmental Ripple of Broadcom's Market Moves - Origina, accessed on August 18, 2025, https://www.origina.com/blog/the-environmental-ripple-of-broadcoms-market-moves
63. Broadcom Inc.'s Status under WEEE Directive, accessed on August 18, 2025, https://docs.broadcom.com/doc/1234568
64. Electronic Hazardous Waste (E-Waste) | Department of Toxic Substances Control, accessed on August 18, 2025, https://dtsc.ca.gov/electronic-hazardous-waste/
65. Interactive Summary: Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine | Royal United Services Institute - RUSI, accessed on August 18, 2025, https://www.rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine/interactive-summary
66. Russian weapons in Ukraine 'powered' by Western parts: Report - Al Jazeera, accessed on August 18, 2025, https://www.aljazeera.com/news/2022/8/8/russian-weapons-in-ukraine-powered-by-western-parts-rusi
67. Russia is using DPRK missiles with Western components: media on NAKO analysis, accessed on August 18, 2025, https://nako.org.ua/en/media/rosiya-vikoristovuje-raketi-kndr-iz-zaxidnimi-komponentami-media-pro-analiz-nako
68. North Korean missile used by Russia in attack on Ukraine contains recently made Western components, new investigation reveals; incl. cos. responses and non-responses - Business & Human Rights Resource Centre, accessed on August 18, 2025, https://www.business-humanrights.org/my/%E1%80%9E%E1%80%90%E1%80%84/north-korean-missiles-used-by-russia-in-recent-attacks-on-ukraine-contain-western-made-components-new-investigation-reveals-incl-cos-responses-and-non-responses/
69. Western-made parts found in North Korean missile downed over Ukraine, report shows, accessed on August 18, 2025, https://kyivindependent.com/western-made-parts-found-in-north-korean-missile-downed-over-ukraine-report-shows/
70. Hundreds of Western components found in Russian weapons in Ukraine - RUSI, accessed on August 18, 2025, https://www.rusi.org/news-and-comment/in-the-news/hundreds-western-components-found-russian-weapons-ukraine
71. Ukraine finds components from nine western companies in missiles fired by Russia — Analog Devices, Broadcom, NXP parts in the wreckage : r/UkrainianConflict - Reddit, accessed on August 18, 2025, https://www.reddit.com/r/UkrainianConflict/comments/1g9h18k/ukraine_finds_components_from_nine_western/
72. How Many Western ICs Are There In Russia's Weapons? - Hackaday, accessed on

August 18, 2025, https://hackaday.com/2024/06/08/how-many-western-ics-are-there-in-russias-weapons/
73. THE U.S. TECHNOLOGY FUELING RUSSIA'S WAR IN UKRAINE - Homeland Security and Governmental Affairs, accessed on August 18, 2025, https://www.hsgac.senate.gov/wp-content/uploads/09.10.2024-Majority-Staff-Report-The-U.S.-Technology-Fueling-Russias-War-in-Ukraine.pdf
74. How Western Tech Powers Russia's War Against Ukrainian Civilians - HUNTERBROOK, accessed on August 18, 2025, https://hntrbrk.com/jet-report/
75. US investigates domestic components in Russian weapons - Army Technology, accessed on August 18, 2025, https://www.army-technology.com/news/us-investigates-domestic-components-in-russian-weapons/
76. Investigation: We tried to buy American chips as a Russian defense manufacturer — and it worked - The Kyiv Independent, accessed on August 18, 2025, https://kyivindependent.com/investigation-we-tried-to-buy-american-chips-as-a-russian-defense-manufacturer-heres-why-its-possible/
77. Report: Enabling war crimes? Western-made components in Russia's war against Ukraine, accessed on August 18, 2025, https://www.business-humanrights.org/en/latest-news/report-enabling-war-crimes-western-made-components-in-russias-war-against-ukraine/
78. New Report Links Western-Made Components to the Weapons Used in Russia's Suspected Ukraine War Crimes - IPHR, accessed on August 18, 2025, https://iphronline.org/articles/western-made-components-in-russia-war-against-ukraine/
79. Home - goclass - Broadcom support portal, accessed on August 18, 2025, https://support.broadcom.com/web/goclass
80. Export Control Classification Number (ECCN) for Network Protection products, accessed on August 18, 2025, https://knowledge.broadcom.com/external/article/171241/export-control-classification-number-ecc.html
81. VMware Statement Regarding Ukraine - Broadcom News and Stories, accessed on August 18, 2025, https://news.broadcom.com/releases/vmware-statement-regarding-ukraine
82. Western-made components found in weapons used in Russia's suspected Ukraine war crimes, new investigation reveals, accessed on August 18, 2025, https://www.business-humanrights.org/en/latest-news/western-made-components-found-in-weapons-used-in-russias-suspected-ukraine-war-crimes-new-investigation-reveals-incl-cos-responses-non-responses/
83. Products of over 250 Western companies repeatedly found in Russian weapons on Ukraine's battlefield expose issues in export controls enforcement, according to new report, accessed on August 18, 2025, https://www.business-humanrights.org/en/latest-news/Products-of-over-Western-companies-repeatedly-found-in-Russian-weapons-on-Ukraines-battlefield-expose-issues-in-export-controls-enforcement-according-to-new-report-incl-cos

-responses-non-responses/
84. Broadcom Corporation did not respond - Business & Human Rights Resource Centre, accessed on August 18, 2025, https://www.business-humanrights.org/en/latest-news/broadcom-corporation-did-not-respond/
85. BRCM_codeofe.pdf, accessed on August 18, 2025, http://media.corporate-ir.net/media_files/irol/11/114961/cg/BRCM_codeofe.pdf
86. Corporate Responsibility - Broadcom Inc., accessed on August 18, 2025, https://www.broadcom.com/company/corporate-responsibility