

CONNECTED TO RISK

Cisco Critical Infrastructure and the Case for Independent Human Rights Assessment

EKŌ

SUMMARY

At its 2026 annual meeting of stockholders, shareholders in Cisco Systems Inc (Cisco) will vote on shareholder proposal 5 requesting that Board of Directors commission and oversee an independent third-party Human Rights Impact Assessment ("HRIA") evaluating severe and foreseeable human rights risks and impacts associated with high-risk customers, end users, and business relationships, including whether the use of Cisco products and services does or can contribute to adverse human rights impacts, at reasonable cost and omitting proprietary or legally privileged information. The HRIA should include surveillance, military, intelligence, immigration enforcement, and other sensitive government or security-related end uses.

This briefing outlines the various issues which raise questions about the Company's human rights due diligence (HRDD) practices and why supporting the resolution is necessary to protect shareholder value.

KEY ISSUES

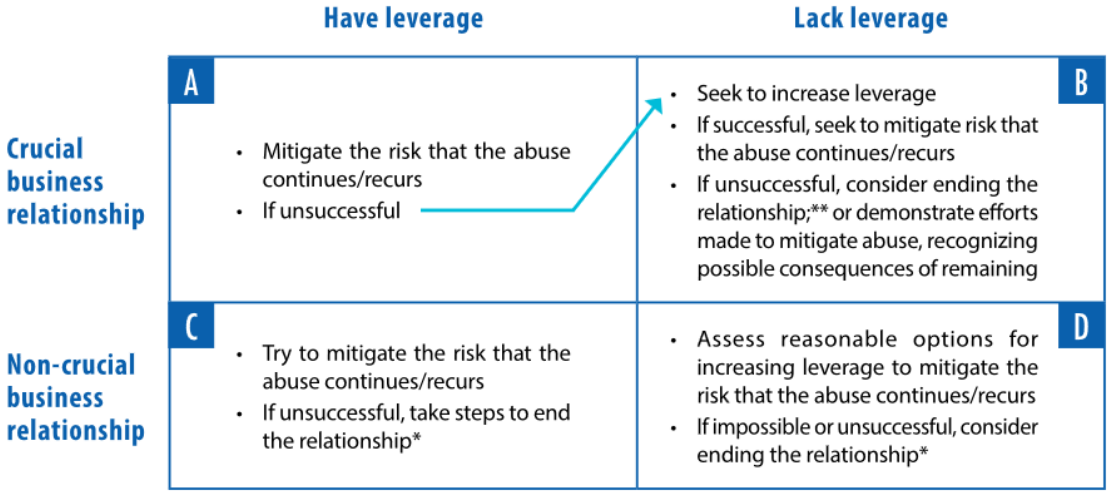
- Insufficient information on how Cisco identifies and addresses severe and foreseeable risks associated with high-risk customers, end users, and business relationships such as governments, military and security actors, immigration enforcement agencies and law enforcement entities.
  - No details of any independent third-party human rights assessments such as the name and specific expertise of those carrying them out, their terms of reference, findings, and/or recommendations.
  - Cisco provides products and services to high risk end users via partners. No visibility on how such partners are evaluated and audited on an ongoing basis.
  - Unclear whether in each case Cisco retains the ability to suspend service or end its agreements with customers or partners that violate its human rights policies.

- Recent reporting, civil society research, investor engagement, and employee organizing raise concerns about the adequacy of Cisco's human rights impact assessment practices:
  - Leaked internal documents reported by The Guardian in November 2026 show Cisco mobilized senior staff and multiple teams, including on-site visits "under extreme security due to ongoing war," to repair failing networks for Israeli military intelligence during the Gaza war, then billed the effort internally as a "customer success story."[1] Importantly, this occurred after the International Court of Justice imposed binding provisional measures and amid credible reporting and UN expert findings concerning severe human rights and international humanitarian law violations.
  - Cisco's reported provision of communications, networking, cybersecurity, and surveillance capabilities to Israeli government, military and intelligence institutions amid allegations of serious violations of international humanitarian and human rights law.
  - Cisco's Digital Hub partnerships operating in Israeli settlements in the occupied West Bank and Syrian Golan Heights, which international bodies, including the International Court of Justice, have found unlawful.
  - Allegations, denied by Cisco, that it customized China's Golden Shield surveillance system to help identify and target Falun Gong practitioners. The Supreme Court ended the case in June 2026 on statutory grounds without deciding whether the conduct occurred.
  - Department of Homeland Security agencies, including Immigration and Customs Enforcement (ICE), have procured Cisco network and communications products amid documented constitutional and human rights concerns involving agency practices.
  - Cisco software is reportedly used by Mytel, a telecommunications company partly owned by the Burmese military. Cisco has not disclosed how the software was obtained or whether it has taken steps to prevent its continued use.

[1] Alice Speri, "*A 'customer success story': leaked documents show Cisco doubled down on Israeli military deals during Gaza war*". The Guardian. November 7, 2026. https://www.theguardian.com/world/2026/nov/07/israel-intelligence-cisco-gaza-palestine

CISCO'S HRDD IS INADEQUATE

The UN Guiding Principles on Business and Human Rights ("UNGPs")[1] constitute the global authoritative framework outlining human rights responsibilities of states and businesses, and expectations are heightened for companies with business activities in conflict-affected and high-risk areas. Companies are expected to take all reasonable steps to ensure their products and services - including the deployment of such technologies by customers - are not used to violate human rights. To meet these obligations, companies should conduct HRDD to identify, prevent, mitigate, and account for adverse human rights impacts, and transparently report on the effectiveness of such HRDD.



** Decisions on ending the relationship should take into account credible assessments of any potential adverse human rights impact of doing so.*
*** If the relationship is deemed crucial, the severity of the impact should also be considered when assessing the appropriate course of action.*

Source: https://www.undp.org/sites/g/files/zskgke326/files/2022-10/HRDD%20Interpretive%20Guide_ENG_Sep%202021.pdf#page=18

Cisco's formal response to the shareholder proposal[2] states that the company conducts human rights due diligence and commissions independent third party human rights impact assessments which "consider the geopolitical context and human rights landscape in a particular market[…] and risks […] relating to end users or partners in high-risk sectors; and product features or capabilities, including the risk of product misuse, surveillance, lawful intercept and other capabilities that may impact human rights". These assessments, their details, their recommendations, or the Company's steps to integrate them into practice, however, are not publically available. Additionally, potential misuse of its products has been revealed by investigative journalism[3], calling into question the efficacy of the company's policies and practices and bolstering the need for a HRIA.

[1] United Nations Office of the High Commissioner for Human Rights, *"Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework"*. (New York / Geneva: United Nations, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
[2] Cisco Systems, Inc., *"2026 Proxy Statement and Notice of Annual Meeting of Stockholders"*. October 29, 2026. https://www.cisco.com/c/dam/en_us/about/annual-report/2026-cisco-proxy.pdf
[3] Murtaza Hussain, *"Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State"*. Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza

In May 2026, Drop Site News reported that internal documents leaked to it by a whistleblower "shows Cisco's deep and growing collaboration with the Israeli military and intelligence establishment in its regional wars and the genocide in Gaza"[1]. The story reports that in 2025, an Israeli Air Force officer publicly "referenced Cisco infrastructure being used by air force intelligence personnel for communications and managing high volumes of operational data—including the use of networking tools by drone operators and ground forces to store and analyze videos and share coordinates for strikes." Internal Cisco documents indicate that Cisco's Israeli Ministry of Defense revenue nearly doubled between the first half of 2023 and the first half of 2024, from $52 million to $98 million. An internal presentation highlights the importance of "capturing defense opportunities", and identifies AI computing and military AI integration as growth areas. Reported customers include the Israeli Air Force, the Prime Minister's Office, the Israel Prison Service, and Elbit Systems. Investors need to understand whether Cisco's due diligence framework was applied to these contracts as they grew, whether the Board was informed, and whether the process included ongoing end-use monitoring and clear thresholds for restricting, suspending, or ending relationships where severe risks could not be mitigated.

Public reporting also identifies Cisco Digital Hub partnerships in settlements in the occupied West Bank and occupied Syrian Golan which carry additional legal and regulatory risks.[2] Yet, Cisco doesn't disclose:

- Each hub's current status or location
- What services Cisco or its partners provide
- Whether any hub supports a settlement's operation or growth
- What if any human rights risk assessment has been carried out in relation to each hub
- What if any assessment has been done regarding the company's potential legal and regulatory exposure especially in light of countries such as Spain[3], Norway[4] and the UK[5] announcing plans to place restrictions on providing services in and sanctions exposure for companies that facilitate or profit from settlement activity and whether the company has considered suspension, relocation, or disengagement from any settlement-based partnership.

[1] Murtaza Hussain, "Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State". Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza
[2] Meir Orbach, "Cisco Launched a Technology Hub Network in Israel" [Hebrew: "סיסקו וקישה תשר מיזכרמ מייגולונכט לארשיב"]. Calcalist. March 6, 2018. https://www.calcalist.co.il/internet/articles/0,7340,L-3733440,00.html
[3] Moncloa Palace, "The Government of Spain strengthens the arms embargo on Israel, and bans imports from illegal settlements in Palestinian territories". September 23, 2025. https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2025/20250923-council-press-conference.aspx
[4] Norwegian Ministry of Foreign Affairs, "Proposal for a bill banning trade with Israeli settlements in Palestine announced for public consultation".June 19, 2026. https://www.regjeringen.no/en/whats-new/proposal-for-a-bill-banning-trade-with-israeli-settlements-in-palestine-announced-for-public-consultation/id3166860/
[5] Foreign, Commonwealth & Development Office, "UK to bring forward new powers to respond to moral emergency in Palestine, and target illegal settlement activity in the West Bank to protect the viability of a two-state solution". September 8, 2026. https://www.gov.uk/government/news/ukto-bring-forward-new-powers-to-respond-to-moral-emergency-in-palestine-and-targetillegal-settlement-activity-in-the-west-bank-to-protect-the-viabili

In November 2026, The Guardian reported on a further trove of internal documents leaked by Cisco workers.[1] According to the reporting, repeated outages in late 2024 to networks used by an Israeli military intelligence client, which the documents describe as delivering "critical network infrastructure for various intelligence departments within the Israeli Ministry of Defense," led the client to threaten to cancel its business. A September 2025 draft memo warned that "during a period of national conflict, these repeated outages severely impacted critical operations." Cisco responded by activating senior staff, mobilizing multiple internal teams over several months, and sending staff to meet a secretive military intelligence unit on site "under extreme security due to ongoing war." Once the client returned to "business as usual," Cisco described the effort internally as a "customer success story." This conduct took place while the company was facing internal objections from employees and as international bodies documented mass civilian harm in Gaza. The International Court of Justice had ordered provisional measures under the Genocide Convention, and in September 2025 a UN Commission of Inquiry concluded that Israel had committed genocide in Gaza.[2]

The reporting raises direct questions about Cisco's claim that its existing due diligence is sufficient. Investors need to understand whether Cisco's due diligence framework was applied to these contracts as they grew, whether it was applied when Cisco chose to restore and deepen a military intelligence relationship in wartime, and whether the Board was informed.

[1] Alice Speri, "A 'customer success story': leaked documents show Cisco doubled down on Israeli military deals during Gaza war". The Guardian. November 7, 2026. https://www.theguardian.com/world/2026/nov/07/israel-intelligence-cisco-gaza-palestine

[2] Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel, "Legal analysis of the conduct of Israel in Gaza pursuant to the Convention on the Prevention and Punishment of the Crime of Genocide". A/HRC/60/CRP.3, United Nations. September 16, 2025. https://www.un.org/unispal/document/commission-of-inquiry-report-genocide-in-gaza-a-hrc-60-crp-3/

Cisco's own due diligence should have flagged human rights risks from Israeli military contracts. It won't say whether it did.

The company identifies bodily security, access to remedy, freedom of expression, political participation, and land rights among its salient human rights issues[1], and recognizes that risks may become more likely or severe in conflict-affected areas. However, shareholders still lack sufficient information to evaluate whether Cisco treats Israel and the occupied Palestinian territory as a conflict-affected context; whether it has conducted enhanced, context-specific due diligence; or any criteria for suspending or exiting a relationship.

Cisco Human Rights Due Diligence policy[2] says its due diligence draws on "credible journalism and reports by human rights organizations, UN Special Procedures, academic institutions." Cisco's expansion of its contracts with Israeli military and government institutions appears to have taken place after the International Court of Justice ordered provisional measures under the Genocide Convention in January 2024.[3]

In addition, human rights organizations, credible journalists and UN Special Rapporteurs have documented issues which should flag with the company serious risks in Cisco's Israeli government/military contracts:

- The reports of UN Special Rapporteurs:
  - Anatomy of a Genocide. Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese.[4]
  - From economy of occupation to economy of genocide. Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese.[5]
  - Report of the Special Rapporteur on the right to development, Surya Deva Peace for development: road map for a peace economy.[6]
  - Non Profits The American Friends Service Committee and Who Profits publish details of Cisco's contracts with the Israeli military.[7]
  - Drop Site News reporting headlined "Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State."[8]

[1] Cisco, "*Human Rights at Cisco*". https://www.cisco.com/c/m/en_us/about/purpose/reporting-hub/responsible-innovation/human-rights.html

[2] Cisco, "Human Rights Due Diligence". https://www.cisco.com/c/dam/m/en_us/about/purpose/reporting-hub/_pdf/human-rights-due-diligence.pdf

[3] International Court of Justice, "*Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), Provisional Measures, Order of 26 January 2024, I.C.J. Reports 2024, p.3*" https://www.icj-cij.org/sites/default/files/case-related/192/192-20240126-ord-01-00-en.pdf
International Court of Justice, "*Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), Request for the Modification of the Order Indicating Provisional Measures of 26 January 2024, Order of 28 March 2024, I.C.J. Reports 2024, p. 513*". https://www.icj-cij.org/sites/default/files/case-related/192/192-20240328-ord-01-00-en.pdf
International Court of Justice, "*Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel), Request for the Modification of the Order of 28 March 2024, Order of 24 May 2024, I.C.J. Reports 2024, p. 649*". https://www.icj-cij.org/sites/default/files/case-related/192/192-20240524-ord-01-00-en.pdf

[4] Francesca Albanese, "*Anatomy of a genocide Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967*". A/HRC/55/73, United Nations, July 2024. https://docs.un.org/en/A/HRC/55/73

[5] Francesca Albanese, "*From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied Since 1967*". A/HRC/59/23, United Nations, July 2025. https://docs.un.org/en/A/HRC/59/23

[6] Surya Deva, "*Peace for development: road map for a peace economy*". A/81/187, United Nations, July 2026. https://docs.un.org/en/A/81/187

[7] Investigate, "*A US-based digital communications company that provides technologies to the Israeli military, police, and prisons, and to illegal Israeli settlements in the occupied Palestinian territory*". February 5, 2025. https://investigate.info/company/cisco. Who Profits Research Centre, "*Cisco Systems*". https://www.whoprofits.org/companies/company/6529?cisco-systems

[8] Murtaza Hussain. "*Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State*". Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza

Cisco has not published any details of any independent third-party human rights assessments such as the name and expertise of those carrying them out, their terms of reference, findings, and/or recommendations. Nor has the company published any information about actions it has taken pursuant to any such assessments. Cisco has not disclosed what criteria and escalation thresholds it uses to determine when enhanced human rights due diligence or an independent Human Rights Impact Assessment is warranted for a customer, end user, product deployment, market, or business relationship.

In opposing the shareholder proposal and attempting to demonstrate existing adequate board oversight, Cisco states that its Public Policy Committee[1] "reviews and discusses with management public policy matters, such as matters related to human rights which encompasses privacy, security, AI governance, and legislative and government policy, among other areas."[2] The Committee's charter (effective 28 May 2026) does not mention human rights, privacy or security despite the fact that Cisco identifies these as "salient issues". It does however explicitly mention government affairs and AI governance.

In opposition to the proposal, Cisco points to its stakeholder engagement as providing "stockholders with meaningful insights about our human rights commitments and approach". However, Cisco's published stakeholder list is primarily trade and standards bodies.[3] The human rights related entities are largely minerals and supply-chain initiatives. Access Now is the only digital rights group. There are no Palestinian, MENA or affected-community organizations listed, and no engagement outcomes are reported.

Cisco also highlights employee training and a whistleblowing line - EthicsLine - and a no retaliation policy as evidence of the adequacy of its existing policies and practices on human rights. However, the U.S. Equal Employment Opportunity Commission (EEOC) found reasonable cause that Cisco "subjected a class of individuals to a hostile work environment based on their national origin (Middle Eastern), religion (Muslim), and/or their association with Muslim and/or Middle Eastern individuals" to a hostile work environment in violation of Title VII of the Civil

[1] Cisco Systems Inc, "*CHARTER OF THE PUBLIC POLICY COMMITTEE*". https://s21.q4cdn.com/812015656/files/committee/2026/Cisco-s-Public-Policy-Committee-Charter-effective-5-28-26.pdf
[2] Cisco Systems, Inc., "*2026 Proxy Statement and Notice of Annual Meeting of Stockholders*". October 29, 2026. https://www.cisco.com/c/dam/en_us/about/annual-report/2026-cisco-proxy.pdf
[3] Cisco, "*Stakeholder Engagement*". https://www.cisco.com/c/m/en_us/about/purpose/reporting-hub/governance/stakeholders.html

Rights Act of 1964.[1] Cisco has publicly disagreed with the non-binding EEOC finding and says it investigated and took appropriate action. Nonetheless the finding raises questions about the mechanisms the company is relying upon and supports calls for an independent HRIA.

AI INFRASTRUCTURE AND GROWTH

AI infrastructure has become central to Cisco's growth strategy. In fiscal 2026, Cisco took $9.3 billion in AI infrastructure orders and delivered approximately $4 billion in AI infrastructure.[2] It expects $7.5 billion in fiscal 2027. Part of this expansion runs through government and state-linked customers. Internal documents reported by Drop Site identify AI computing and "military AI integration" as growth areas in Cisco's Israeli defense business.[3] Leaked documents reported by The Guardian detail dozens of deals Cisco pursued in 2026 with Israeli government clients, including the intelligence community, air force and navy, many tagged as "AI" deals. They also show that executives for Cisco's Splunk data-analytics subsidiary pitched to join Project Nimbus, the Israeli government's controversial cloud contract with Google and Amazon.[4]

Cisco is positioning itself to capture AI demand "however or wherever"[5] customers choose to deploy it. Its disclosed safeguards have not kept up to the same pace. Although Cisco's Responsible AI Framework covers AI that Cisco builds and uses and its due diligence triggers cover new products, markets and acquisitions, neither addresses the due diligence tied to high-risk government and military customers deploying AI on Cisco infrastructure. The concerns raised above suggest this gap is meaningful in practice, despite the Company's other policies and standards.

Human rights risk is a defining issue in this sector. Responsible AI researchers have documented how militaries chain together AI systems for intelligence and targeting.[6] This growth in military AI runs on data centers and computing infrastructure,[7] including, according to reporting, Israeli military facilities built with Cisco products and services.[8] These systems are used to automate at speed

[1] Noam Scheiber, "*Cisco Likely Allowed Harassment of Pro-Palestinian Workers, Agency Says*". New York Times. September 14 2026. https://www.nytimes.com/2026/09/14/business/cisco-eeoc-palestinian-harassment.html
[2] Cisco, "*Cisco Reports Fourth Quarter and Fiscal Year 2026 Earnings*". August 12, 2026. https://www.sec.gov/Archives/edgar/data/858877/000085887726000106/exhibit991pressrelease-q4f.htm
[3] Murtaza Hussain, "*Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State*". Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza
[4] Alice Speri, "*A 'customer success story': leaked documents show Cisco doubled down on Israeli military deals during Gaza war*". The Guardian. November 7, 2026. https://www.theguardian.com/world/2026/nov/07/israel-intelligence-cisco-gaza-palestine
[5] Cisco, "*Cisco Reports Fourth Quarter and Fiscal Year 2026 Earnings*". August 12, 2026. https://www.sec.gov/Archives/edgar/data/858877/000085887726000106/exhibit991pressrelease-q4f.htm
[6] AI Now Institute and Airwars, "*Anatomy of an AI Kill Chain*" 28 July 2026. https://ai-killchain.airwars.org/
[7] Harry Davies and Yuval Abraham, "*Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war*," The Guardian, 23 January 2025. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft
[8] Murtaza Hussain, "*Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State*". Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza

tasks previously carried out by human analysts, such as generating targets.[1] The networking, compute and security infrastructure underneath them is what makes this AI kill chain possible.

As Cisco's AI business grows, so does the share of its revenue exposed to high-risk end uses. Investors have no disclosure on how Cisco assesses AI infrastructure sales to military, government, or intelligence customers, or whether its Responsible AI Framework, which governs AI that Cisco itself develops and uses, applies to how customers deploy that infrastructure.[2]

HIGH RISK CUSTOMERS AND SENSITIVE END USES

The risks are not restricted to contracts with Israeli entities or activity in the settlements. Cisco products and services are used by government, military, intelligence, immigration enforcement and law-enforcement entities in contexts that may present heightened risks.

Public contracting records indicate that the U.S. Department of Homeland Security ("DHS") agencies, including Immigration and Customs Enforcement, have procured Cisco products and services, including network infrastructure, licenses, support, and video-teleconferencing equipment,[3] amid documented constitutional and human rights concerns involving DHS practices.[4] These records show that in 2026 U.S. Customs and Border Protection awarded a Cisco Enterprise Agreement support-services contract valued at approximately $22 million, with a potential value of nearly $66 million. ICE separately purchased approximately $1.66 million in Cisco Catalyst wireless access points to support its network infrastructure as staffing and joint operations expanded.[5] These procurements place Cisco technology within core DHS operations amid documented constitutional and

[1] Yuval Abraham, "'*Lavender*': *The AI machine directing Israel's bombing spree in Gaza*" +972 Magazine, 3 April 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/

[2] Cisco, "*Cisco Principles for Responsible Artificial Intelligence*", https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-principles.pdf?CCID=cc000742&DTID=odicdc000016

[3] USA Spending.gov, "*Contract Summary: Delivery Order (DO) PIID 70B04C26F00000120*". https://www.usaspending.gov/award/CONT_AWD_70B04C26F00000120_7014_NNG15SD22B_8000 ; HigherGov.com, "*NNG15SD07B-70CTD025FR0000023, Delivery Order*". https://www.highergov.com/contract/NNG15SD07B-70CTD025FR0000023/ ; Cisco, "*Partner Profile: Regency Consulting Inc. (RCI)*". https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/pf/index.jsp#/NDk4NzE0@MTM2NTYwOD-cy@RU4= ; Sam.gov, "*Cisco & Poly Virtual Teleconferencing (VTC) Equipment Blanket Purchase Agreement*". https://sam.gov/opp/5fc4c404d1d2423b945711fadd8d742a/view ; U.S. Immigration and Customs Enforcement, "*Virtual Attorney Visitation Program*". https://www.ice.gov/detain/detention-facilities/vav

[4] The Robert & Ethel Kennedy Human Rights Center et al., "*Update to Joint Submission of Coalition of Immigrant Rights Organizations to the United Nations Universal Periodic Review of the United States of America*". April 10, 2026. https://kennedyhumanrights.org/wp-content/uploads/2026/04/UPR-2026-Final-Joint-Submission-Update_4.10.26.pdf ; American Immigration Council, "*How ICE Went Rogue*". February 11, 2026. https://www.americanimmigrationcouncil.org/fact-sheet/ice-cbp-legal-analysis/ ; United Nations, "*UN rights chief decries US treatment of migrants, as deaths in ICE custody rise*". January 23, 2026. https://news.un.org/en/story/2026/01/1166816

[5] USAspending.gov, "*Cisco Enterprise Agreement Support Services 1.0*," Award No. 70B04C26F00000120. April 16, 2026. https://www.usaspending.gov/award/CONT_AWD_70B04C26F00000120_7014_NNG15SD22B_8000; USAspending.gov, "*Purchase of Cisco Catalyst WAPs to Support Immigration and Customs Enforcement Network Infrastructure*," Award No. 70CTD025FR0000113. September 30, 2025. https://www.usaspending.gov/award/CONT_AWD_70CTD025FR0000113_7012_NNG15SD49B_8000

human rights concerns involving immigration enforcement and detention, raising questions about whether Cisco applies heightened human rights due diligence to these government customers and end uses.

Cisco also faced allegations that the company helped customize China's Golden Shield surveillance system in ways used to identify and target Falun Gong practitioners. Although the Supreme Court decision in June 2026 means the case will not proceed no finding was made on the underlying factual allegations, which have been denied by the company.[1]

In July 2026 Cisco was added by Burma Campaign UK to its 'Dirty List', for alleged links to the Burmese military or human rights violations and environmental destruction in Burma.[2] The listing followed reports that job advertisements posted by Mytel, a telecommunications company linked to Burma's military, indicated that it may use Cisco technology obtained directly or indirectly.[3] Cisco stated that its sales comply with U.S. export controls and that it conducts human rights due diligence on transactions presenting heightened risks, but it did not confirm or deny Mytel's use of its technology or explain whether it had investigated the reported connection.[4] In January 2025, the U.S. Commerce Department added Mytel to its Entity List, which identifies foreign organizations whose activities are considered contrary to U.S. national-security or foreign-policy interests.[5] The designation requires a government license, subject to a presumption of denial, to export, reexport, or transfer covered U.S. hardware, software, or technology to Mytel. Although the listing does not establish that Cisco violated these restrictions, investors need to understand whether Cisco has traced the source of any technology used by Mytel and prevented unauthorized transfers, support, or software updates, including through channel partners.

Cisco does not adequately publicly disclose how it assesses potential impacts before entering into or continuing high-risk customer relationships; whether leverage (including acceptable-use requirements or audit rights) is used to prevent or mitigate harms; or how identified risks and impacts are addressed.

[1] Jan Wolfe, "*US supreme court ends lawsuit alleging Cisco helped China pursue Falun Gong*". The Guardian. Reuters. June 23, 2026. https://www.reuters.com/world/us-supreme-court-ends-suit-alleging-cisco-helped-china-pursue-falun-gong-2026-06-23/

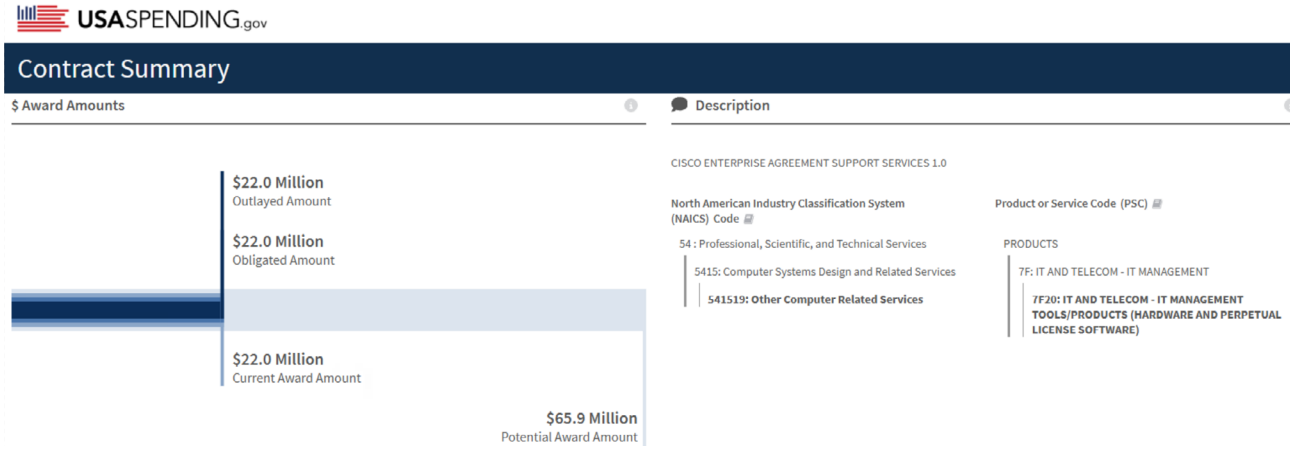
[2] Burma Campaign UK, "*Myanmar. 53 companies added to Burma Campaign UK 'Dirty List' for alleged involvement with the junta's operations or human rights violations*". Business and Human Rights Centre. July 20 2026. https://www.business-humanrights.org/en/latest-news/global-53-companies-added-to-dirty-list-for-involvement-with-the-myanmar-military-or-human-rights-violations-in-myanmar/

[3] Business & Human Rights Resource Centre, "*Myanmar. American tech firms urged to cut ties with Burmese military-linked telco*". January 30, 2025. https://www.business-humanrights.org/en/latest-news/myanmar-american-tech-firms-urged-to-cut-ties-with-burmese-military-tied-telco/

[4] Cisco Systems, "*Cisco's Response*". Published by the Business & Human Rights Resource Centre, January 29, 2025. https://www.business-humanrights.org/en/latest-news/cisco-did-not-respond-3/

[5] U.S. Department of Commerce, Bureau of Industry and Security, "*Revisions to the Entity List*". 90 Federal Register 559–563, January 6, 2025. https://www.federalregister.gov/documents/2025/01/06/2024-31468/revisions-to-the-entity-list

Investors therefore lack sufficient information to evaluate whether Cisco adequately addresses severe risks associated with high-risk customers.



INCREASED RISK BY OPERATING THROUGH PARTNERS

A substantial portion of Cisco's products and services is sold through channel partners rather than directly to end users. This model can limit Cisco's visibility into ultimate customers and uses and complicate its ability to monitor deployments, enforce safeguards, or suspend support when severe risks emerge. These risks are particularly significant when partners serve military, intelligence, security, or other high-risk customers. Recent reporting concerning Cisco's partner relationships in Israel illustrates the concern. According to internal documents reported by Drop Site,[1] its Israeli partner Bynet handles recurring sales across Israel's security establishment, including military units, intelligence agencies and weapons manufacturers:

- The Israeli Air Force and Navy
- MAMRAM (the IDF's computing unit)
- The Prime Minister's Office, including Mossad and Shin Bet
- The Israel Prison Service
- Elbit, Rafael and Israel Aerospace Industries

Cisco's Human Rights Policy says that it "expect[s] our partners… to make commitments aligned to these standards."[2] And its due diligence page cites human rights "triggers: "For example, in recent years we have worked cross-functionally to incorporate triggers in the context of due diligence processes related to partner

[1] Murtaza Hussain, "*Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State*". Drop Site News. May 15, 2026. https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza
[2] Cisco, "*Global Human Rights Policy*". Last revised August 14, 2025. https://www.cisco.com/c/dam/assets/csr/pdf/Human-Rights-Policy.pdf

onboarding, high-risk products, artificial intelligence (AI) governance, and mergers and acquisitions, among others."[1] The UNGPs - which Cisco claims to adhere to - requires companies to "Seek to prevent or mitigate adverse human rights impacts that are [...] by their business relationships, even if they have not contributed to those impacts" and that its "business relationships" are understood to include relationships with business partners, entities in its value chain, and any other non-State or State entity directly linked to its business operations, products or services".[2]

However, Cisco does not confirm:

- The detail of the due diligence carried out when onboarding Bynet, or what was found.
- Whether such diligence looks beyond a partner's policies to which customers it serves and for what use.
- The nature and frequency of ongoing monitoring and auditing of partners after onboarding.
- The ongoing auditing and monitoring (if any) of end customers and whether this is carried out by the channel partner or Cisco.
- Whether Cisco has confirmed that Bynet explicitly passed Cisco's General Use Terms and Acceptable Use Policy on to end customers including Israeli military and government customers.
- Whether Cisco contractually has the ability to suspend service or end its agreements with customers or partners that it considers to have violated its human rights related policies upon the conclusion of internal or third party assessments.

On the supplier side, Cisco confirms that it checks compliance through "internal and external audits" and may terminate suppliers who don't comply. Cisco publicly discloses[3] limited information about its supply chain audits, including an overview of key nonconformances revealed on audit and Cisco's actions to mitigate. Significantly, Cisco does not disclose even this limited information in relation to its partners.

[1] Cisco, "*Human Rights Due Diligence*". https://www.cisco.com/c/dam/m/en_us/about/purpose/reporting-hub/_pdf/human-rights-due-diligence.pdf
[2] United Nations Office of the High Commissioner for Human Rights, "*Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*". (New York / Geneva: United Nations, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
[3] Cisco, "*Due Diligence and Supplier Code of Conduct*" https://www.cisco.com/c/m/en_us/about/purpose/reporting-hub/responsible-innovation/supply-chain/due-diligence.html

Beyond apparent failures of HRDD, Cisco's conduct also raises questions about compliance with its Acceptable Use Policy[1] and General Use Terms[2]. Continued contracts with state and non-state actors implicated in systematic human and civil rights abuses and violations, including those contravening international humanitarian law, potentially represent not only process failures in HRDD but also potentially negligence in enforcing the company's user policies and standards.

Cisco relies on its channel partners through which it primarily sells its products and services to pass on Cisco's contract terms to the end customer. If the partner should fail to do so it's unclear what contractual safeguards, acceptable-use requirements, monitoring rights and ultimately termination rights apply.

Microsoft's response to a comparable high-risk use illustrates the importance of retaining contractual control. Microsoft ceased and disabled specified cloud-storage and AI services provided to a unit within the Israeli Ministry of Defense after finding evidence supporting reports that Azure had been used to store mass-surveillance data. Microsoft enforced its standard terms of service, which prohibit use of its technology for mass surveillance of civilians.[3] It's unclear in the absence of disclosures on partner audit and monitoring what degree of leverage Cisco retains to suspend or terminate a high-risk business relationship established via a channel partner.

[1] Cisco, "*Cisco Acceptable Use Policy*". https://www.cisco.com/c/dam/en_us/about/legal/cisco-acceptable-use-policy.pdf
[2] Cisco, "*General Terms*". https://www.cisco.com/c/dam/en_us/about/doing_business/legal/Cisco_General_Terms.pdf
[3] Microsoft, Brad Smith, "*Update on Ongoing Microsoft Review*". September 25, 2025. https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/

MATERIAL RISKS FOR INVESTORS

Inadequate HRDD exposes Cisco to material, legal, operational, and reputational risks.

- **Legal and regulatory risk:**
  - Government measures addressing settlement-related activity create an evolving compliance risk for Cisco and its partners. Spain has restricted imports of settlement goods; the UK has announced measures addressing settlement goods, services and entities that support, facilitate or profit from settlement activity; and Norway has proposed restrictions covering goods, investment and specified property-related services. These measures differ in scope and implementation status. Their potential application to Cisco's settlement-based Digital Hub partnerships depends on the activities involved and the relevant jurisdictional connections. Investors need disclosure of which partnerships Cisco has assessed, what exposure it has identified, and whether suspension, relocation or disengagement is warranted.[1]

  - Military, intelligence and surveillance relationships create additional exposure to investigations and litigation concerning alleged contributions to human rights violations. Cisco's Golden Shield litigation illustrates the potential for technology deployments to generate prolonged legal scrutiny. The Supreme Court's June 2026 decision limited the available legal claims; it did not resolve the underlying factual allegations, which Cisco denies. A favorable legal outcome therefore does not substitute for assessing whether comparable risks persist in other customer relationships.[2] Even without an adverse judgment or settlement, prolonged litigation and regulatory scrutiny can impose substantial legal and compliance costs, consume management resources, and cause reputational harm.

  - Potential financial consequences include legal defense and investigation costs, compliance and remediation expenditure, restrictions on particular transactions, and costs associated with restructuring or discontinuing affected relationships.

[1] Spain: President of the Government of Spain and the Council of Ministers, "*The Government of Spain strengthens the arms embargo on Israel, and bans imports from illegal settlements in Palestinian territories*". September 23, 2025. https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2025/20250923-council-press-conference.aspx
UK: Foreign, Commonwealth & Development Office, "*UK to bring forward new powers to respond to moral emergency in Palestine, and target illegal settlement activity in the West Bank to protect the viability of a two-state solution*". September 8, 2026. https://www.gov.uk/government/news/ukto-bring-forward-new-powers-to-respond-to-moral-emergency-in-palestine-and-targetillegal-settlement-activity-in-the-west-bank-to-protect-the-viabili
Norway: Norwegian Ministry of Foreign Affairs, "*Proposal for a bill banning trade with Israeli settlements in Palestine announced for public consultation*". June 19, 2026. https://www.regjeringen.no/en/whats-new/proposal-for-a-bill-banning-trade-with-israeli-settlements-in-palestine-announced-for-public-consultation/id3166860/

[2] Supreme Court of the United States, "*Cisco Systems, Inc. v. Doe*". June 23, 2026. https://www.supremecourt.gov/opinions/25pdf/24-856_kjfm.pdf

- **Financial Performance and Commercial Risk:**
  - Enterprises, governments, and other large customers may (or in the case of new laws relating to the settlements be obliged to) avoid association with companies under human-rights or surveillance controversy. The UN Human Rights Council has highlighted the business risks of corporate complicity in conflict-affected areas.[1]

  - Cisco's own FY2026 Form 10-K identifies uncertainty arising from human-rights-related laws and customer procurement requirements, alongside other regulatory exposures.[2] The commercial significance of a controversial relationship therefore extends beyond revenue from the customer directly involved: investors should also consider effects on other customers' confidence in Cisco as a trusted infrastructure and cybersecurity provider.

  - Unresolved involvement in severe human rights harms, without adequate mitigation, may expose Cisco to classification as a human rights norms-breach company of Business and Human Rights standard practices under institutional investor and ESG data-provider frameworks.[3] Such classifications can trigger enhanced engagement, investment restrictions, or portfolio exclusions among pension funds and other institutional investors applying norms-based screening criteria.

  - Although identified high-risk government and military relationships represent a relatively small share of Cisco's consolidated revenue, their growth underscores the importance of assessing these exposures before they become more commercially entrenched. According to internal documents reported by Drop Site News, Israeli Ministry of Defense revenue increased from $52 million in the first half of 2023 to $98 million in the first half of 2024, approximately 0.19% and 0.36%, respectively, of Cisco's consolidated revenue in the corresponding fiscal half-years.[4]

[1] Francesca Albanese, From Economy of Occupation to Economy of Genocide.
[2] Cisco's acknowledged business risks: Cisco Systems, Inc., "*Form 10-K for the fiscal year ended July 25, 2026*", Item 1A, Risk Factors. U.S. Securities and Exchange Commission. September 2, 2026. https://www.sec.gov/Archives/edgar/data/858877/000085887726000132/csco-20260725.htm
[3] Investor Initiative on Human Rights Data, "*Guidance for ESG Data Providers on Assessing Company Non-Compliance with, and Breaches of, International Human Rights Norms*". September 2025, pp. 5, 11–12. https://www.churchofengland.org/sites/default/files/2026-09/ii-hrd-report-september-2025.pdf
[4] Murtaza Hussain, "*Leaked Documents Show Cisco Systems' Deep Relationship with Israeli Security State*," Drop Site News, May 15, 2026. Reporting on leaked internal Cisco presentations showing Israeli MOD revenue of $52 million in H1 2023 and $98 million in H1 2024, total Cisco Israel revenue of $283 million in FY2024, and $111 million attributed internally to "conflict impact." https://www.dropsitenews.com/p/cisco-systems-israel-genocide-gaza ; Cisco Systems, Inc., "*Cisco Reports Second Quarter Earnings*," February 15, 2023, and February 14, 2024. Cisco reports consolidated revenue of $27.224 billion for the six months ended January 28, 2023, and $27.459 billion for the six months ended January 27, 2024. Estimated Israeli MOD revenue shares calculated as $52 million / $27.224 billion = 0.19% and $98 million / $27.459 billion = 0.36%. The Israeli and Cisco fiscal reporting periods may not align exactly. https://investor.cisco.com/news/news-details/2023/CISCO-REPORTS-SECOND-QUARTER-EARNINGS/default.aspx
https://investor.cisco.com/news/news-details/2024/CISCO-REPORTS-SECOND-QUARTER-EARNINGS/default.aspx

- These estimates suggest that Cisco has an opportunity to assess and mitigate severe and foreseeable human rights risks while the financial contribution from these relationships remains relatively limited and the company may retain flexibility to modify or discontinue problematic deployments.

- **Operational Risk:** Cisco's reliance on channel partners creates risks where it lacks visibility into ultimate end users or cannot enforce safeguards on sensitive deployments. Cisco's FY2026 Form 10-K acknowledges that partner compliance failures and distribution disruption could harm its business.[1]

- Employee protests and activism over controversial contracts can depress morale, productivity, erode trust in management, increase employee turnover, negatively impact recruitment pipelines, and slow delivery in mission-critical teams.[2] These risks are no longer hypothetical: in June 2026, the U.S. Equal Employment Opportunity Commission issued a reasonable-cause determination that Cisco subjected Middle Eastern and Muslim employees, and employees associated with those groups, to a hostile work environment in violation of Title VII. Cisco disputes the determination and maintains that it investigated the concerns and took appropriate action; the determination is not a final judicial finding of liability.[3] The matter is unresolved however the conflict and reports that agency-led conciliation was unsuccessful and employees were considering litigation illustrates how inadequate grievance, anti-harassment, and non-retaliation mechanisms can convert controversy over sensitive business relationships into regulatory scrutiny, potential legal costs, management distraction, and sustained human-capital risk.[4]

- **Reputational Risk:**
  - Repeated allegations that Cisco technology facilitates surveillance, repression or civilian harm can undermine confidence in the company's human rights commitments. This is particularly relevant to a business whose networking and cybersecurity offerings depend on customer trust.

[1] Cisco Systems, Inc., "*Form 10-K for the fiscal year ended July 25, 2026*", Item 1A, Risk Factors.
[2] Empirically, firms with higher employee satisfaction and perceived managerial trustworthiness deliver stronger long-run stock returns and profitability. See: Alex Edmans, "*Does the Stock Market Fully Value Intangibles? Employee Satisfaction and Equity Prices*". Journal of Financial Economics 101, no. 3 (2011): 621–640. https://doi.org/10.1016/j.jfineco.2011.03.021 ; More on employee organizing at Cisco: Paresh Dave, "*The Dissent at Cisco Over the War in Gaza*". October 30, 2024. WIRED. https://www.wired.com/story/cisco-dissent-gaza-israel-war/
[3] Alice Speri, "*Cisco probably violated Middle Eastern and Muslim employees' civil rights, US agency finds*". The Guardian. August 31, 2026. https://www.theguardian.com/technology/2026/aug/31/cisco-civil-rights-palestine-advocacy-violation
[4] Legal Aid at Work, "*Federal Government Finds Cisco Systems Failed to Protect Pro-Palestinian Employees*". August 31, 2026. https://legalaidatwork.org/federal-government-finds-cisco-systems-failed-to-protect-pro-palestinian-employees/

- The risk is amplified where Cisco states that reviews found no violations but provides insufficient information about their scope, evidence, findings and resulting safeguards. Without that information, customers, employees and investors cannot readily evaluate whether the company has addressed the concerns. Reputational damage may consequently translate into commercial or operational consequences through the mechanisms described above.

- **Portfolio-wide and systemic risk:** For diversified investors, corporate enablement of severe human rights harms and unrestrained conflict can transmit risk through weakened institutions and geopolitical instability into wider economic disruption and portfolio losses. This does not depend solely on a company's market capitalization or index weight; it is also relevant when the company has a meaningful nexus to severe harms and its products, services, or infrastructure can enable those harms to persist or escalate.
  - **Public harms and institutional destabilization.** Corporate products and services can enable surveillance, repression, civilian harm, and infrastructure destruction where companies fail to apply effective human rights safeguards. When violations of international humanitarian law proceed without accountability, they weaken governing institutions and the rules intended to restrain conflict. This can allow harm to persist and conflict to escalate, destroying productive capacity, displacing populations, and placing growing pressure on public systems and regional stability.
  - **Macroeconomic transmission and portfolio-wide losses.** Conflict and institutional deterioration can disrupt production, trade, energy markets, and supply chains, contributing to inflation, sovereign fiscal strain, and weaker economic growth. Rising uncertainty can produce broader asset repricing, credit deterioration, and defaults, while shared exposures and interconnected financial markets can amplify losses through contagion and cascading market disruption.

Cisco's relevance to this analysis arises from its provision of critical communications and digital infrastructure in conflict-affected and other high-risk settings. An independent HRIA would help investors assess whether Cisco's safeguards interrupt potential pathways from company involvement to wider harm by identifying severe impacts, evaluating the company's leverage, and producing meaningful changes in contracts, deployment decisions, and conduct.

CONCLUSION

Independent HRIAs have become an established governance tool, including at Microsoft[1] and Meta.[2] As Cisco expands its business relationships with high-risk customer categories and in the face of allegations which raise concern about human rights risk assessment combined with inadequate disclosure to shareholders on the specific processes and outcomes for human rights due diligence to date, it is prudent for the Board of Directors to commission and oversee an independent third-party Human Rights Impact Assessment evaluating severe and foreseeable human rights risks and impacts associated with such high-risk customers, end users, and business relationships.

Without a comprehensive HRIA, shareholders have limited ability to assess the company's exposure to material, financial, legal & regulatory, and reputational risks. Supporting the shareholder resolution is therefore prudent.

[1] Foley Hoag, "*Foley Hoag Conducts Independent Human Rights Impact Assessment Commissioned by Microsoft*". June 26, 2023. https://foleyhoag.com/news-and-insights/news/2023/june/foley-hoag-conducts-independent-human-rights-impact-assessment-commissioned-by-microsoft/

[2] Miranda Sissons, "*An Independent Due Diligence Exercise into Meta's Human Rights Impact in Israel and Palestine During the May 2021 Escalation*". Meta. September 22, 2022. https://about.fb.com/news/2022/09/human-rights-impact-meta-israel-palestine/









Disclaimer

None of Ekō, RJI, CMEI, or Azzad Asset Management are investment or financial advisors, and do not make any representation regarding the advisability of investing in any particular company or investment fund or vehicle. A decision to invest in any such investment fund or entity should not be made in reliance on any of the statements set forth in this briefing. While Ekō, RJI, CMEI, and Azzad Asset Management have obtained information believed to be reliable, they shall not be liable for any claims or losses of any nature in connection with information contained in this document, including but not limited to, lost profits or punitive or consequential damages. This publication should not be viewed as a comprehensive guide of all questions an investor should ask an institution, but rather as a starting point for questions specifically related to the issues presented in this publication. The opinions expressed in this publication are based on the documents specified in the endnotes. We encourage readers to read those documents.

Contact:

To connect with the authors of this report, please email press@eko.org