

INVESTOR MEMO

The Risk Multiplier: Product Integration, ICE Contracts, and the Case for Disclosure at Thomson Reuters

AGM June 10, 2026

Supporting the Shareholder Proposal for an Independent Human Rights Impact Assessment on Products used for Law and Immigration Enforcement

Submitted by the B.C. General Employees' Union (BCGEU)

Proposal	Independent Human Rights Impact Assessment (HRIA) on law enforcement & immigration use of TRI products
Proponent	B.C. General Employees' Union (BCGEU), long-term shareholder
Meeting Date	June 10, 2026 — Annual General Meeting
TRI Ticker	TRI (TSX / NYSE)
Contracts at Issue	Active contracts potentially worth US\$60M as of April 2026 to provide products such as CLEAR®, LPR technology, CALR LEIDS to Department of Homeland Security (DHS) and Immigration and Customs Enforcement (ICE).
BCGEU Recommendation	VOTE FOR the proposal

Executive Summary

Thomson Reuters (TRI), an AI and technology company, delivers software and data solutions to the U.S. government. The focus of this proposal is the solutions TRI offers to law enforcement and immigration enforcement including products such as its flagship CLEAR® (Consolidated Lead Evaluation and Reporting) product and related CLEAR Batch Services, CLEAR System-to-System, CLEAR ID Inform, CLEAR for Law Enforcement, CLEAR LPR, and services through Thomson Reuters Special Services (TRSS). CLEAR® software aggregates billions of data points from public and non-public sources, and in aggregate it can build comprehensive pictures of people's lives including understanding where they have been and where they may go. In contract documents from Department of Homeland Security (DHS), CLEAR® is described as “the most comprehensive investigative database platform available.”¹

TRI and its investors are materially exposed to compounding legal, reputational, and governance risks that its current disclosure of controls and enforcement does not specifically or adequately address. TRI's Board has recommended shareholders vote against the proposal, arguing its existing human rights impact assessment (HRIA) and process already addresses the concerns raised. We disagree for reasons detailed in this memo and believe investor support for the proposal is both warranted and consistent with shareholders' fiduciary and stewardship obligations.

¹ <https://www.highergov.com/document/sole-source-justification-clear-renewal-redacted-pdf-eb2cfa/>

Risk Summary

Risk Category	Assessment
Legal & litigation exposure (e.g. ICE lawsuits, product liability, whistleblower suit)	HIGH
Reputational risk due to adverse media coverage and employee dissent	HIGH
Technology integration and interoperability risk: TR's (e.g. Palantir, PenLink, LPR create potentially compounded harms)	HIGH
Disclosure gap: HRIA disclosure inadequate for investor oversight; enterprise HRIA insufficient for concentrated product-level risk	HIGH
Counterparty risk: U.S. government procurement changes limiting guardrail enforcement	HIGH
UNGP compliance	ELEVATED
Workforce / talent risk: whistleblower suit, retaliation allegations	ELEVATED
GenAI uninsured liability from AI-enhanced data products	ELEVATED

A Changing Risk Landscape

TRI products reportedly help the DHS and ICE target undocumented immigrants for detention and deportation. TRI's technologies have been directly linked to deportations and raids across the U.S., potentially involving family separation and the detention of immigrants in conditions that violate human rights.

Operation Metro Surge brought the conduct of U.S. federal immigration enforcement into sharp international focus, with credible, widely reported evidence of civilian deaths, warrantless arrests, racial profiling, due process violations, and systemic human rights abuses condemned by United Nations experts as gross violations of international human rights law.² ICE's activities are now the subject of a significant number of lawsuits, and the products used these operations, potentially including TRI's products, may feature in legal proceedings as evidence.

As noted in the proposal, both Capgemini and Stantec divested or terminated contracts with ICE/DHS in response to the same escalating risks.

Despite considerable reporting and documentation, TRI has maintained that its products are not used for deportations. In a deleted page on its website, it writes that CLEAR® is “not designed for use for mass illegal immigration inquiries or for deporting non-criminal undocumented persons and non-citizens.”³

² <https://www.ohchr.org/en/press-releases/2026/02/minneapolis-fatal-shootings-may-amoun-extrajudicial-killing-warn-un-experts>

³ <https://www.npr.org/2026/04/21/nx-s1-5786915/ice-immigration-enforcement-data-thomson-reuters>

Microsoft was forced to correct public statements regarding allegations its Azure cloud and AI technologies were used by the Israeli military for mass surveillance and target identification in Gaza after initially refuting the reporting. That company conducted a review, published information on its website, and subsequently ceased and disabled certain services.⁴

The Compounding Risk of Integrated Surveillance Technologies

The single most distinctive feature of BCGEU's proposal, and the area where TRI's enterprise-level HRIA is most obviously inadequate, is the question of integrated surveillance risk. TRI's products are no longer being used in isolation. They are being woven into a multi-platform surveillance ecosystem.

A 2023 sole-source contract review comparing CLEAR[®] against competitor platforms identified TRI as the superior choice specifically because of capabilities competitors lacked: namely the integration of Motorola/Vigilant's license plate reading (LPR) technology, and with PenLink.

CLEAR[®] & Palantir

In an April 2026 blog post, TRI writes that "Palantir is not a customer of CLEAR". However, as Robert Ambrogi writes, TRI's surveillance infrastructure does not operate in isolation. Government contracting documents, reporting by Oakland Privacy, *The New York Times*, and the national research project American Dagnet "have documented how Thomson Reuters' CLEAR can be used to work with Palantir's analytical platform in a system-to-system configuration."⁵

DHS contractually required TRI's products to be interoperable with Palantir's FALCON system.⁶ According to a TRI contract with ICE's Homeland Security Investigations division, CLEAR data was fed directly into Palantir's controversial automated analysis system, determining whom to target for investigation. According to Sarah Lamdan, "[t]he contract specifies that TRI will provide the data and the technology firm Palantir will conduct the real-time analysis to determine who to target through system-to-system communication."⁷

A newer app developed by Palantir, Enhanced Lead Identification and Targeting (ELITE), integrates TRI's data with Palantir's analytics platform to enable the mapping of targets for detention across geographic areas.^{8,9} ELITE has faced allegations of misuse, including the indiscriminate targeting of individuals without criminal records.

Palantir, co-founded by Peter Thiel, has for years been described as instrumental in enabling ICE to consolidate and operationalize millions of data points, from social media posts to location history and, more recently, tax information, to identify and track targets.¹⁰ TRI provides the data that powers this system. The Company has described itself as a 'data processor' that does not control how clients use its information; documented evidence suggests these assurances do not prevent or mitigate harm and should not be treated as risk controls.

A 2025 Securities and Exchange Commission (SEC) privacy impact assessment indicates that Penlink PLX links

⁴ <https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/#:~:text=Sep%2025%2C%202025%20%7C%20Microsoft%20Corporate,privacy%20as%20a%20fundamental%20right.>

⁵ <https://www.lawnext.com/2026/04/the-legal-tech-giants-powering-ice-part-1-how-thomson-reuters-and-lexisnexis-helped-support-americas-immigration-surveillance-machine.html>

⁶ https://oaklandprivacy.org/wp-content/uploads/2017/10/LSJ_Final.pdf

⁷ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3231431

⁸ <https://www.ft.com/content/fe3d1ad7-ffd3-40f3-a35a-4d00a351687d?segmentId=2c1df321-36a4-1206-2c08-112c059dd69d&syn-25a6b1a6=1>

⁹ <https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/>

¹⁰ <https://prismreports.org/2026/04/29/dhs-surveillance-location-data-penlink-plx/>

the data it collects to a verified personal profile in CLEAR. The assessment noted the risk that “personal information may be collected without a clear purpose or legal authority.”¹¹

CLEAR® & PenLink: Warrantless Phone Tracking

Since at least 2022, CLEAR® has sourced real-time location data with time stamps from PenLink, a surveillance technology provider.¹² PenLink has faced persistent allegations of violating privacy and constitutional rights, enabling real-time location tracking, wiretapping and the ability to perimeter tracking, and allegedly the tracking of entire neighbourhoods.¹³

A 2025 privacy impact assessment (PIA) issued by the Security and Exchange Commission (SEC) indicates that PenLink PLX links the data it collects to a verified personal profile in CLEAR®¹⁴ creating “a comprehensive, real-time portrayal of a person’s digital and physical life”. PenLink PLX captures live communications and web activity, conducts geospatial tracking using real-time location pings from mobile phones and commercial app data, and has geofencing capabilities, the ability to identify every phone in a geographic area during a specific timeframe.¹⁵

CLEAR® & Vigilant’s Mobile Companion and LEARN

In 2017 TRI brought Vigilant’s (owned by Motorola) license plate recognition data to the CLEAR® investigation platform, offering “a potent new solution in CLEAR LPR to augment investigations.¹⁶ CLEAR® is also reportedly integrated into Vigilant LEARN (Law Enforcement Archival & Reporting Network) platform, which has two applications, Vigilant PlateSearch™ and Vigilant FaceSearch™. Motorola Solutions’ licence plate reading technology has collected over 20 billion licence plate and vehicle scans and reportedly includes facial recognition technology. According to a 2020 DHS synopsis/solicitation document for LPR technology, TRI was expected to make at least 30 million new unique LPR data records available each month.¹⁷ When a licence plate is photographed, it is not only a plate that is captured. People, children, and bystanders are caught in the dragnet as well as lawn signs and other data. The risk potential of this technology and its additional facial recognition and geofencing capabilities are considerable.

ICE's most recent Privacy Impact Assessment (PIA) governing the use of the mobile LPR from 2021 placed restrictions on use of the technology for immigration enforcement, in sensitive areas, and did not permit geographic or geofenced searches for enforcement activities.¹⁸ The vast majority of Homeland Security Investigation (HSI) staff have been redirected to work on enforcement activities¹⁹, and it is unclear how this technology is being deployed in ways that differ from this assessment.

Vigilant and parent company Motorola have previously been criticized for circumventing sanctuary laws to enable information sharing with ICE.²⁰

¹¹ <https://www.sec.gov/files/pia-penlink.pdf>

¹² <https://sam.gov/workspace/contract/opp/7030ebced0ef45a5b6e6d9489a45ec32/view>

¹³ <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/>

¹⁴ <https://www.sec.gov/files/pia-penlink.pdf>

¹⁵ <https://prismreports.org/2026/04/29/dhs-surveillance-location-data-penlink-plx/>

¹⁶ <https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-brings-vigilant-license-plate-recognition-data-to-clear-investigation-platform>

¹⁷ https://assets.nationbuilder.com/bcgeu/pages/19571/attachments/original/1778003868/3_DHS_ICE_LEIDS_RFP_PWS.pdf?1778003868

¹⁸ https://www.dhs.gov/sites/default/files/publications/privacy-pia30b-ice-acquisitionanduseoflprdatafromacommercialservice-june2021_0.pdf

¹⁹ <https://www.cato.org/blog/ice-has-diverted-over-25000-officers-their-jobs>

²⁰ <https://jisis.washington.edu/humanrights/2022/12/07/whos-watching-washington/>

AI Risk

TRI has made significant investments in artificial intelligence (AI) and claims to be at the forefront of generative AI (GenAI), offering Risk Analysis Summary (RAS) which works within its Consolidated Lead Evaluation and Reporting (CLEAR) investigative software.

A 2025 Stanford study reviewed two of TRI legal AI models, Westlaw Precision and Ask Practical Law, which use retrieval-augmented generation (RAG). According to the analysis, one third of Westlaw's responses contained a hallucination.²¹ And TRI's Ask Practical Law AI provides incomplete answers (refusals or ungrounded responses) on more than 60 per cent of queries, the highest rate among the systems tested.²²

The company contested the findings, however, according to Legal AI World, "the vendors' response ... was not to publish their own independent benchmarks proving otherwise. It was to dispute the methodology and point to internal data they have not made public." The blog goes on to say that "in the absence of transparent, third-party benchmarking — which the Stanford researchers explicitly called for — lawyers are being asked to trust marketing claims that have not been independently verified. That is a professional responsibility problem, not just a product quality question."²³

Workforce and Governance Concerns

Workers Speak Out

As media scrutiny on ICE contracts intensified, TRI employees became aware of the company's involvement with ICE, many for the first time. This prompted internal organizing, culminating in a letter to company leadership requesting non-renewal of ICE contracts. These efforts received media attention, including in *The Minnesota Star Tribune*²⁴ and *The New York Times*²⁵. The company has since renewed and expanded contracts with the agencies.²⁶

TRI's response to internal dissent has itself become a governance concern. Internal discussion of ICE contracts was reportedly shut down, and one employee, Billie Little, alleges she was investigated and ultimately fired for her role in organizing. She has since filed a whistleblower lawsuit, which received widespread media coverage.²⁷ If that suit proceeds to discovery, the resulting record could be material to investors.

Oversight, Procurement and Auditing Concerns

- Since March 2025, the Trump administration has dismantled key Department of Homeland Security (DHS) oversight offices, specifically targeting those responsible for civil rights and detention

²¹ https://dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf

²² https://dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf

²³ <https://legaliworld.com/westlaw-ai-and-lexis-ai-still-hallucinate-what-the-stanford-study-actually-found/>

²⁴ Mike Hughlett, *The Minnesota Star Tribune*, 'Thomson Reuters criticized by some Minnesota employees over its ICE contract', March 3, 2026. <https://www.startribune.com/ice-crackdown-thomson-reuters-eagan-license-plate-data-westlaw-clear/601583754>

²⁵ Kashmir Hill, *The New York Times*, 'They Don't Want Their Company's Surveillance Tool Used by ICE,' March 11, 2026 <https://www.nytimes.com/2026/03/11/technology/thomson-reuters-ice-minnesota.html>

²⁶ See https://www.usaspending.gov/award/CONT_AWD_70RTAC26FR0000018_7001_GS02F026DA_47 and https://www.usaspending.gov/award/CONT_AWD_70RTAC26FR0000018_7001_GS02F026DA_4732

²⁷ Jude Joffe-Block, NPR, 'She Raised Concerns About Her Company's Contracts with ICE. Then She Lost Her Job,' April 21, 2026 <https://www.npr.org/2026/04/21/nx-s1-5786915/ice-immigration-enforcement-data-thomson-reuters>

conditions.²⁸ The Office for Civil Rights and Civil Liberties (CRCL) and Citizenship and Immigration Services Ombudsman (CISOMB) were effectively gutted, with CRCL staffing reduced from 150 to just nine, halting over 550 investigations while hundreds of allegations of abuses remain pending.²⁹

- The Office of the Immigration Detention Ombudsman (OIDO) was also gutted, however in May 2026, it was shuttered entirely.³⁰ At least 18 deaths have been reported in ICE custody through the first four months of 2026, following 31 deaths last year, a two-decade high. With less oversight, companies and their investors are more exposed to risk.
- Changes in procurement federally landscape has also shifted in ways that may materially limit Thomson Reuters' ability to uphold its own stated policies and principles as a contractor. For example, the GSAS's draft AI Terms and Conditions include requirements that "AI System(s) must not refuse to produce data outputs or conduct analyses based on the Contractor's or Service Provider's discretionary policies." As the *Center for Democracy and Technology* (CDT) writes, "this will likely mean that vendors will be forced to have their systems provide outputs regardless of potential risk".³¹
- According to analysis from Lawfare, companies cannot rely on contractual guardrails to govern the use of their products when the U.S. government has the unilateral right to modify contract terms.³²
- Changes to contract language may further limit the ability of contractors to enforce internal policies. For example, some GSA contracts include specific provisions which explicitly reserve the right for the government to "unilaterally modify the contract to implement Executive Orders" and require contractors to accept mass modifications or face removal from the contract vehicle. Contractors who do not accept these modifications "may result in off-ramping."³³

Audits and Disclosure

TRI states that it conducts audits to ensure appropriate use of its products. It is contractually required to do so by agencies including DHS and committed to additional audits as a condition of the Brooks et al. v. Thomson Reuters Corporation class action settlement. Yet despite conducting these audits, the company provides no disclosure on how the process works in practice.

Audit disclosure is standard in analogous supply chain and client governance contexts. Companies routinely report the number of audits conducted, their findings, and outcomes. Given that TRI already conducts audits, this is not a question of capability. It is a question of transparency.

Basic questions remain unanswered:

- How many audits are conducted annually, and across which client categories?
- What do audits examine: user query logs, access controls, compliance with use restrictions? How is international human rights law applied?
- How does the company ensure that restricted data, such as Experian credit header data, is not used for immigration enforcement purposes, even inadvertently?
- How many audits have resulted in contract terminations, remedial action, or escalation?
- What happens when non-compliant use is identified? Does the company have the authority to act on that information?

²⁸ The Office for Civil Rights and Civil Liberties (CRCL), Office of the Immigration Detention Ombudsman (OIDO), and Citizenship and Immigration Services Ombudsman (CISOMB) were effectively gutted, with CRCL staffing reduced from 150 to just nine, halting over 550 investigations while hundreds of allegations of abuses remain pending <https://www.theguardian.com/us-news/2025/nov/30/us-watchdog-human-rights-department-homeland-security>

²⁹ <https://www.theguardian.com/us-news/2025/nov/30/us-watchdog-human-rights-department-homeland-security>

³⁰ <https://www.reuters.com/legal/government/us-close-watchdog-office-federal-immigration-detention-abuses-2026-05-05/>

³¹ https://cdt.org/wp-content/uploads/2026/04/CDTEFFPDEPIC_Comments-re-GSA-Draft-AI-Terms_4.3.2026.pdf

³² <https://www.lawfaremedia.org/article/military-ai-policy-by-contract--the-limits-of-procurement-as-governance>

³³ <https://govtribe.com/file/government-file/oasis-plus-sb-rfp-47qca23r0001-amendment-0008-1-dot-12-dot-26-dot-pdf>

The gap between what is known and what is disclosed is itself a risk. Strong policies matter, but without transparency, investors cannot assess whether they are working. This is about accountability and understanding how risk is managed in practice.

The Disclosure Gap is a Governance Failure

TRI committed to the UN Guiding Principles on Business and Human Rights in 2022 and conducts human rights impact assessments and saliency assessments on a three-year cycle using a specialized external consultancy (Article One). The 2022 HRIA delivered a handful of high-level bullet points, with no meaningful discussion of law enforcement use cases, product integration risks, audit findings, or specific recommendations. The company indicated it could not share more. Its most recent assessment, in 2025, using the same consultancy has not been published yet, but the company has represented that it will release key findings of its most recent HRIA 'in line with previous assessments.' It further indicated that the 2025 assessment differs only marginally, except on AI risk.

2022	1 of 5	2025
UNGP commitment made Following BCGEU engagement	HRIA risks touched on harms to data subjects No law enforcement use cases disclosed	Latest HRIA completed Before Operation Metro Surge and major legal exposure

The 2025 HRIA was completed before Operation Metro Surge and the most significant wave of legal and reputational risk became apparent. There is no evidence the company evaluated the compounding risks created by integrating CLEAR® with Palantir, PenLink, and Motorola's LPR systems. Under the UNGPs, companies are required to evaluate impacts arising from the interaction of multiple technologies.

"Where certain design features of a product are well-known, or could have reasonably been foreseen, to increase the risk of adverse human rights impacts in the end-use phase, failure to address these will over time put the company in a position of contribution."³⁴
UN B-Tech Project

In BCGEU's view, investors do not have enough information to assess TRI's compliance with the UNGPs. The UNGPs also speak to leverage: where a company's product is linked to harm through a business relationship, the company has a responsibility to use its leverage to encourage the entity causing the harm to prevent or mitigate its recurrence. There is no publicly available evidence that TRI has exercised this leverage in any meaningful way as it relates to its contracts with ICE.

Conclusion: risks are documented, live, and escalating.

This proposal about whether TRI has the due diligence infrastructure to identify, assess, and mitigate risks from specific, high-risk product applications, and whether investors have the information to evaluate that question. In our view, TRI's disclosure has not kept pace with the changing risk environment it operates within, particularly when we consider the risks of data and software integration and interoperability. Further, in BCGEU's view, investors do not have enough information to assess TRI's compliance with the UNGPs.

³⁴ <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/taking-action-address-human-rights-risks.pdf>

<p>Legal</p> <p>Multiple active lawsuits tied to ICE data use, including a whistleblower suit. Concerns from Congress and states regarding conduct of data brokers.</p>	<p>Reputational</p> <p>Sustained international media coverage including the New York Times, NPR, Financial Times, and 404 Media.</p>
<p>Governance</p> <p>Workforce expressing concerns and internal dissent could undermine the Company's ability to deliver on its own commitments.</p>	<p>Integration</p> <p>Combined surveillance capabilities whose compounding effect has never been independently assessed.</p>

VOTE RECOMMENDATION

Responsible investors need this information.

Responsible investors need the information this proposal would provide to discharge their fiduciary and stewardship obligations.

BCGEU urges all shareholders to vote FOR this proposal.

Annual General Meeting: June 10, 2026

Further Reading

1. Kashmir Hill, The New York Times, 'They Don't Want Their Company's Surveillance Tool Used by ICE,' March 11, 2026
2. Joseph Cox, 404 Media, 'Thomson Reuters Shareholders Demand Investigation into ICE Contracts,' April 16, 2026
3. Peter Andringa, Financial Times, 'Thomson Reuters Faces Employee Backlash Over ICE Data Contracts,' April 15, 2026
4. Jude Joffe-Block, NPR, 'She Raised Concerns About Her Company's Contracts with ICE. Then She Lost Her Job,' April 21, 2026
5. Maurizio Guerrero, Prism, "DHS is buying access to real-time location data—the latest expansion of its “invasive” surveillance technology, April 29, 2026
6. Bob Ambrogi, LawNext, The Legal Tech Giants Powering ICE, Part 2 — The Pushback: Employees, Shareholders, Lawyers and the Fight Over May 31, April 29, 2026.

This memo was prepared by the B.C. General Employees' Union (BCGEU). It is intended for use by institutional investors in connection with the Thomson Reuters AGM on June 10, 2026. Nothing in this memo constitutes legal or financial advice. BCGEU is a minority shareholder in Thomson Reuters. For further information, contact BCGEU Investment and Pensions Department investor@bcgeu.ca . Additional materials and supporting documentation available on request.