RiskD3M

Materiality Determination Support

Meridian Defense Systems, Inc. · Ransomware encryption of ERP and CAD environments; suspected exfiltration of CUI

Prepared 2026-07-22 · Data-Driven Decision-Making for cyber financial risk

Recommendation (for human decision)

MATERIAL (confidence: clear)

Recommend treating as MATERIAL, the following factor(s) independently meet a materiality threshold: Estimated financial impact; Records affected; Sustained operational downtime; and contributing factors also weigh toward materiality: Sensitivity of data involved; Regulated data involved; Reputational / brand exposure; Legal / regulatory exposure; Operational criticality of affected systems; Competitive / IP harm; Third-party / supply-chain dimension; Incident ongoing / scope unresolved.

Disclosure clock

Determination date: 2026-07-22. Four-business-day Form 8-K Item 1.05 deadline: 2026-07-28. Basis: If materiality is determined on 2026-07-22, the Form 8-K Item 1.05 disclosure would be due by 2026-07-28 (4 US business days later, excluding weekends and observed federal holidays).

Factor analysis (every factor shown)

Factor	Observed	Threshold	Kind	Weight	Triggered
Estimated financial impact	$2,400,000	≥ $1,000,000 (lesser of 1% of revenue or $1,000,000 floor)	quantitative	sufficient	YES
Records affected	40,000	≥ 25,000	quantitative	sufficient	YES
Sustained operational downtime	96 h	≥ 24 h	quantitative	sufficient	YES
Sensitivity of data involved	high	≥ high	qualitative	contributing	YES
Regulated data involved	CUI (CMMC / DFARS 252.204-7012), ITAR-controlled technical data	any regulated data present	qualitative	contributing	YES
Reputational / brand exposure	high	≥ high	qualitative	contributing	YES
Legal / regulatory exposure	high	≥ high	qualitative	contributing	YES

Operational criticality of affected systems	high	≥ high	qualitative	contributing	YES
Competitive / IP harm	high	≥ high	qualitative	contributing	YES
Third-party / supply-chain dimension	yes	present	qualitative	contributing	YES
Incident ongoing / scope unresolved	yes	present	qualitative	contributing	YES

Methodology

Measured, not modeled. Each factor above is evaluated deterministically against the registrant's configured thresholds and the qualitative considerations the SEC directs registrants to weigh. Every input, threshold, and trigger is shown, so the same facts always produce the same reproducible recommendation and deadline. Quantitative analysis uses the registrant's own policy figures, not SEC thresholds; a low quantitative impact can still be material on qualitative grounds (SAB No. 99).

Important notices

Decision support only, not a legal determination and not legal advice. The SEC has no quantitative bright-line for cybersecurity materiality; the final determination is a facts-and-circumstances judgment reserved to the registrant's officers, board, and counsel. This tool never files anything and never starts the disclosure clock on its own.

Decision support only. This analysis assists management and the board in making their own materiality determination. RiskD3M does not determine materiality and makes no securities filing. It is not legal, accounting, or actuarial advice. All outputs require review and approval by an authorized officer before use.

RiskD3M. Powered by ElasticD3M. Patent Pending.