



NEWS RELEASE

# Inotiv Provides Notice Regarding Cybersecurity Incident

2026-02-13

WEST LAFAYETTE, Ind., Feb. 13, 2026 (GLOBE NEWSWIRE) -- Inotiv, Inc. (NASDAQ: NOTV) (the "Company", or "Inotiv"), a leading contract research organization specializing in nonclinical and analytical drug discovery and development services and research models and related products and services, is providing public notice regarding its cybersecurity incident that it became aware of on August 8, 2025.

As previously described in the Company's Current Report on Form 8-K filed with the Securities and Exchange Commission (the "SEC") on **August 18, 2025** and its subsequent SEC filings, Inotiv experienced a cybersecurity incident in early August 2025. While Inotiv currently has no indication that personal information has been misused, it has provided notice via mail and email, and via this release and an accompanying posting on its **website**, to inform individuals whose personal information was potentially involved. This notification provides details of the incident and Inotiv's response, the resources it is making available to individuals whose personal information has been identified as potentially involved, and additional steps individuals can take if they believe their personal information was potentially involved.

On August 5, 2025, Inotiv detected unusual activity on certain of its systems and promptly initiated an investigation. On August 8, 2025, Inotiv determined that this unusual activity was due to unauthorized actions by a threat actor. Inotiv's investigation determined that between approximately August 5-8, 2025, a threat actor gained unauthorized access to Inotiv's systems and may have acquired certain data.

Upon learning of the potential data acquisition, Inotiv took prompt action to identify and review the data and

identify individuals whose personal information may have been involved. Inotiv subsequently determined that certain data may have been acquired by the threat actor during this incident, including personal information.

Inotiv maintains certain data related to current and former employees of Inotiv and their family members, as well as certain data related to other individuals who have interacted with Inotiv or companies it has acquired. Inotiv's review determined that the personal information potentially involved included names, Social Security numbers, tax identification numbers, driver's license numbers, other government-issued identification numbers or details, dates of birth, financial account information, payment card information, health insurance information, medical information, biometric data, passport information, digital signatures, and contact information, among other types of information.

Upon detecting the unusual activity, Inotiv promptly took steps to contain it and launched an investigation with the support of external cybersecurity specialists. Inotiv also notified regulators and U.S. law enforcement. Notification was not delayed as a result of a law enforcement investigation.

Inotiv has notified individuals whose personal information was potentially involved via mail and email where such contact information was available and has offered complimentary credit monitoring to these individuals. Inotiv is further posting substitute notice on its website and issuing this release for the limited number of individuals whose information was potentially involved but for whom Inotiv could not locate valid contact information.

Inotiv recommends that individuals remain vigilant for incidents of fraud and identity theft, including by regularly reviewing and monitoring their credit history and credit reports to detect any errors and guard against any unauthorized transactions or activity. Inotiv also recommends that individuals closely monitor their account statements and notify their financial institution if they suspect any unauthorized activity.

Please be assured that Inotiv has taken steps to address the incident and to further enhance its security measures to protect individuals' data. If you have any questions about this notice or the incident and believe your information may have been potentially involved, please contact (833) 918-5956 (U.S. residents, toll-free) or (214) 393-3323 (individuals outside the U.S.) Monday through Friday, from 8 am to 8 pm Central Time (excluding major U.S. holidays) or [dataprivacymanager@inotiv.com](mailto:dataprivacymanager@inotiv.com). Please be prepared to provide engagement number B158971.

#### About Inotiv

Inotiv, Inc. is a leading contract research organization dedicated to providing non-clinical and analytical drug discovery and development services and research models and related products and services. The Company's products and services focus on bringing new drugs and medical devices through the discovery and preclinical phases of development, all while increasing efficiency, improving data, and reducing the cost of taking new drugs and medical devices to market. Inotiv is committed to supporting discovery and development objectives as well as

helping researchers realize the full potential of their critical research and development projects, all while working together to build a healthier and safer world. Further information about Inotiv can be found here:

<https://www.inotiv.com/>.

This release contains statements that constitute “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995. Such statements include statements regarding the Company's assessment of the cybersecurity incident, ongoing or potential impacts, and efforts of the Company related to the incident. Actual results may vary materially from those expressed or implied by forward-looking statements based on a number of factors, including, without limitation: the results of further analyses of the scope and details of the data that the threat actor accessed; release by the threat actor of any of the Company's data, including third party data held by the Company, or the use of any such data for any fraudulent purposes; potential adverse impact of the incident on the Company's results of operations, including revenue, operating income and cash flows from operations, and on its financial condition, including liquidity; diversion of management's attention from operations of the Company to addressing the cybersecurity incident; potential litigation related to the cybersecurity incident; potential adverse effects on relationships with customers, suppliers and other third parties as a result of the cybersecurity incident; reputational risk related to the cybersecurity incident; regulatory scrutiny of the cybersecurity incident; and various other risks, including those detailed in the Company's filings with the SEC.

---

Company Contact  
Inotiv, Inc.  
Beth A. Taylor, Chief Financial Officer  
(765) 497-8381  
[beth.taylor@inotiv.com](mailto:beth.taylor@inotiv.com)

Investor Relations  
LifeSci Advisors  
Steve Halper  
(646) 876-6455  
[shalper@lifesciadvisors.com](mailto:shalper@lifesciadvisors.com)

Source: Inotiv, Inc.