Data Breach Information

Information and resources for current and previous employees

Alert: **Data breach information and resources for current and previous employees**

On Monday, Nov. 20, Idaho National Laboratory became aware of a cybersecurity data breach within Oracle HCM, a federally approved vendor system that resides outside the lab and supports certain INL Human Resources applications. Information was stolen for many current and previous employees of Battelle Energy Alliance (BEA), the contractor that manages Idaho National Laboratory (INL), and some Idaho Cleanup Project (ICP) employees.

The laboratory is working with DOE, the FBI, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and other national labs to investigate the breach.

Impacted individuals will receive a joint notification letter from Experian and INL soon.

We are committed to continuing transparent communication on this incident. Current employees should refer to the internal resource center available on Nucleus that will be updated with information and resources as they become available. Email **databreach@inl.gov (mailto:databreach@inl.gov)** if you have questions.

Who is affected by the data breach?

Current INL employees, spouses and dependents:

We can confirm the release of information for many current INL employees (including postdocs, graduate fellows and interns), dependents and spouses in the data breach. Multiple forms of sensitive personally identifiable information (PII) were impacted. Affected employees will receive a joint notification letter from Experian and INL soon.

Those who were actively employed on June 1, 2023:

These individuals have information, including multiple forms of sensitive PII, in the data set impacted in the breach.

Dependents and spouses of employees who were actively employed on June 1, 2023:

These individuals have information, including names and dates of birth, in the data set impacted in the breach.

Employees who began active employment after June 1, 2023:

These individuals **did not** have any data impacted by the breach.

Previous INL employees, interns, postdocs and their dependents and spouses:

The laboratory continues to determine full impacts to previous INL employees, including interns and postdocs, in addition to spouses and dependents. Names and dates of birth for these individuals were impacted. For many previous employees, we know that other sensitive PII also may have been exposed. Impacted individuals will receive a joint notification letter from Experian and INL soon.

Employees who left INL after June 1, 2023:

Individuals who left INL for any reason after June 1, 2023, (e.g., voluntary or involuntary separation, etc.) have information, including multiple forms of sensitive PII, impacted by the breach.

Dependents and spouses of employees who left INL after June 1, 2023:

These individuals have information, including names and dates of birth, in the data set impacted in the breach.

INL retirees and their dependents and spouses:

INL continues to determine full impacts to retirees in addition to spouses and dependents. Names and dates of birth for these individuals were impacted. For some retirees, we know that other sensitive PII also may have been exposed. Impacted individuals will receive a joint notification letter from Experian and INL soon.

Employees who retired from INL after June 1, 2023:

Individuals who retired from INL for any reason after June 1, 2023 have information, including multiple forms of sensitive PII, impacted by the breach.

Employees who retired from INL before June 1, 2023:

INL continues to determine full impacts to previous employees, including retirees. Names and dates of birth for these individuals were impacted. For many previous employees, we know that other sensitive PII also may have been exposed. Impacted individuals will receive a joint notification letter from Experian and INL soon.

Dependents and spouses of employees who retired from INL after June 1, 2023:

These individuals have information, including names and dates of birth, in the data set impacted in the breach.

Individuals employed by the Idaho Cleanup Project between 2005 and 2006:

Anyone employed by the Idaho Cleanup Project (ICP) between 2005 until mid-2006 may have information impacted by the breach. During that time frame, ICP used BEA's Peoplesoft HR system and they were loaded into the Oracle HCM system as former employees. At this point, there is no evidence that dependent or beneficiary information is impacted by the breach.

Who is not affected by the data breach?

The event did not impact INL's own network, or other networks or databases.

INL employees who began active employment after June 1, 2023:

These individuals **did not** have any data impacted by the breach.

Experian Credit Monitoring

Impacted Individuals will receive a joint notification letter from Experian and INL at their home address. This letter will include activation codes to enroll in no-cost identity protection and credit monitoring services for all individuals, including employees, spouses and dependents who were impacted by the data breach. All individuals 18 and over will receive their own token to enroll in services. Dependents under 18 will receive coverage under the employee's code.

Identity monitoring services will include:

- **Tri-Bureau Credit Report and Monitoring**.
- **Experian 1 Bureau Credit Report**.
- **VantageScore Tracker**, which provides a monthly Experian credit score.
- **Score Simulator** to help individuals see how certain actions will impact their credit.
- **Experian Real-Time Credit Inquiry Notifications**.
- **Credit Limit, Utilization and Balance Notifications**.
- **Change of Address**, which monitors if an individual's mail has been rerouted.

Identity protection services will include:

- **Experian Real-Time Authorization Notifications** when personal information is used for new applications or identity validations.
- **Experian Internet Surveillance** to monitor internet activity for trading or selling of personal information.
- **Court Records** searches criminal and court records to determine if an individual's identity has been used by an unauthorized user.
- **Lost Wallet** provides protection for all personally identifiable information that has been compromised.
- **Non-Credit or Pay-Day Loans** alerts individuals when no credit check or payday loans have been acquired using their Social Security number.
- **Social Security Number Trace** provides a report of all names, aliases and addresses associated with an individual's Social Security number.
- **Financial Account Takeover** monitors activity in deposit accounts, including new deposit account applications, new deposit accounts opened, changes made to deposit account holder's personal information and new signers added to account.

Impacted individuals can reach Experian identity protection agents 24/7 via a dedicated, toll-free customer assistance line. These agents can explain identity theft risks and remediation options, and help with enrollment, identity restoration and product-related questions.

Individuals who need identity restoration will arrange a call back from a highly trained fraud resolution agent, who is certified under the federal Fair Credit Reporting Act.

INL's service with Experian also includes identify theft insurance for enrolled individuals. This service provides reimbursement for U.S. residents for certain ancillary expenses associated with restoring their identity should they become a victim of identity theft.

How should affected individuals protect their information?

INL has finalized a contract with Experian to provide no-cost credit monitoring to all individuals (including employees, spouses and dependents) impacted by the data breach. Impacted individuals will receive a joint letter from Experian and INL soon with details on how to enroll in this service, as well as the types of personal information impacted by the data breach. Individuals should also review their credit reports using sources like **Annual Credit Report.com (https://www.annualcreditreport.com/index.action)**.

In addition, all affected individuals should follow best cybersecurity practices to keep their information safe, including:

Freezing your credit

Place a free **credit freeze (https://www.annualcreditreport.com/securityFreezeBasics.action)** on your credit report. This will prevent unauthorized access to your credit history and credit score and prevent an unauthorized individual from taking out a loan or opening new lines of credit in your name.

Individuals must establish an online account at each of the U.S. Credit Reporting Agencies:

- **Equifax (https://www.equifax.com/personal/credit-report-services/credit-freeze/)**
- **Transunion (https://www.transunion.com/credit-freeze)**
- **Experian (https://www.experian.com/freeze/center.html)**
- **Innovis (https://www.innovis.com/securityFreeze/index)**

Contact your financial institutions

Contact financial institutions listed in your Oracle HCM profile on June 1, 2023, and follow their recommendations for account safety. Keep an eye on your financial accounts (bank, credit card, shopping) for suspicious activity. Consider updating passwords or implementing multifactor authentication if you don't already have it in place.

Other recommendations

Be on guard for identity theft. More information on this topic is available from the **Federal Trade Commission (https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft)** and **usa.gov (https://www.usa.gov/identity-theft)**.

Watch your email, text messaging, social media and phone calls for highly targeted phishing attempts that take advantage of this information. Many cybercriminals prefer to launch attacks on weekends and around the holidays.

Frequently Asked Questions

When did we first learn about the incident?

The laboratory was alerted to the breach in the early morning hours of Nov. 20, 2023.

How did we learn about the incident?

How did this data breach happen?

What is INL doing to protect impacted individuals' information?

Should I update or change my bank account information?

Were other systems or critical infrastructure at INL impacted?

Who is responsible for the breach?

What is INL doing now?

Who was impacted, and what information was impacted?

Is INL working with authorities on investigating the cyber breach?

What can I do to protect my information?

Was my retirement account impacted?

What should I do if my address or the address of one of my dependents has changed?

Alert: Data breach information and resources for current and previous employees (https://inl.gov/)

Data Breach Questions

Send a Message (mailto:databreach@inl.gov)

Additional Links

Identity Theft Recovery Plan(https://www.identitytheft.gov/#/)

Taxpayer Guide to Identity Theft (https://inl.gov/integrated-energy/all-research/)

Credit Feeze Basics (https://www.annualcreditreport.com/securityFreezeBasics.action)

Annual Credit Report.com (https://www.annualcreditreport.com/index.action)

U.S. DEPARTMENT OF ENERGY

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

- DOE Office of Nuclear Energy(https://www.energy.gov/ne/office-nuclear-energy)
- DOE Idaho Operations Office(https://www.id.energy.gov/)
- Battelle(https://www.battelle.org/)

(https://www.facebook.com/) (https://twi (https://www.youtube (https://www.instagra (https://www.linkedin.com/com (https://www.pinterest.com/i (https://www.flickr.co

Alert: **Data breach information and resources for current and previous employees (https://inl.gov/)**

Idaho National Laboratory
1955 N. Fremont Ave.
Idaho Falls, ID 83415
866-495-7440

- Equal Opportunity Employer(https://inl.gov/eeo/)
- Privacy and Accessibility(https://inl.gov/privacy-and-accessibility/)
- Vulnerability Disclosure Program(https://doe.responsibledisclosure.com/hc/)