DAVID Y. IGE
GOVERNOR

DR. CHRISTINA M. KISHIMOTO
SUPERINTENDENT

STATE OF HAWAI'I
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI'I 96804

OFFICE OF THE SUPERINTENDENT

April 2, 2019

The Honorable Ronald D. Kouchi, President
and Members of the Senate
State Capitol, Room 409
Honolulu, Hawaii 96813

The Honorable Scott Saiki, Speaker
and Members of the House of Representatives
State Capitol, Room 431

Dear President Kouchi, Speaker Saiki, and Members of the Legislature:

For your information and consideration, I am transmitting a copy of the Department of Education's report, pursuant to Hawaii Revised Statutes (H.R.S.) § 487 N (2006). In accordance with H.R.S. Section 93-16, I am also informing you that the report may be viewed electronically at: http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/StateReports/Pages/Legislative-reports.aspx

Sincerely,

Dr. Christina M. Kishimoto
Superintendent

CMK:cs
Enclosures

c: Legislative Reference Bureau
Office of Fiscal Services
Office of Information Technology Services

HAWAII DEPARTMENT OF EDUCATION REPORT

REPORT TO THE 2019 LEGISLATURE

Report on the Security Breach at The Department of Education March 2019

Discovery Date of Exposure:	March 14, 2019
Location of Data Exposure:	Department of Education Procurement and Contracts Branch Office Waipahu Civic Center 94-275 Mokuola St, Waipahu, HI 96797
Nature of Data Exposure:	Devices containing sensitive information were stolen

Incident Description

The Hawaii Department of Education's (HIDOE) Procurement and Contracts Branch, located at the Waipahu Civic Center, was broken into overnight between Wednesday, March 13, 2019 and Thursday, March 14, 2019. Devices, including laptops and external drives, were stolen from the location.

HIDOE filed a Police report of the break-in and theft, as well as notified the Department of Accounting and General Services (DAGS), who manages the Waipahu Civic Center facilities.
After interviewing staff and reviewing the server files it was determined that the stolen devices contained personally identifiable information (PII).
Approximately 135 individuals have been identified as having their personal information exposed. Notification letters are being mailed to the last known address on file and all affected individuals have the option to purchase one (1) year of credit monitoring services that we will reimburse them for. Attachment A contains a sample of the letter that will be mailed to the individuals.

Remediation

To prevent this from happening again, files that include sensitive information which are not needed for business operations have been removed and remaining files have been redacted or encrypted. In addition, we have changed HIDOE's policy to require any stored personally identifiable information at rest to be encrypted. Lastly, we are increasing our staff cybersecurity training.

DAVID Y. IGE
GOVERNOR

DR. CHRISTINA M. KISHIMOTO
SUPERINTENDENT

STATE OF HAWAI'I
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI'I 96804

OFFICE OF INFORMATION TECHNOLOGY SERVICES

Attachment A

<< First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>>(Format: Month Day, Year)

Notice of Data Breach

Dear << First Name>> <<Last Name>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

The Hawaii Department of Education's (HIDOE) Procurement and Contracts Branch, located at the Waipahu Civic Center, 94-275 Mokuola St, Waipahu, HI 96797, was broken into sometime in the early morning of March 14, 2019. Devices containing personally identifiable information (PII) were stolen during the break in. HIDOE has filed a Police report of the break-in and theft.

What information was exposed?

The sensitive information that was exposed, included your name and Social Security Number.

What are we doing?

Files that include sensitive information which are not needed for business operations have been removed and remaining files have been redacted or encrypted. In addition, we are increasing our security measures by requiring any stored personally identifiable information at rest to be encrypted as well as increase staff cybersecurity training to prevent this from happening again.

To help relieve concerns and restore confidence following this incident, you may opt to purchase credit monitoring services. If you do so by July 15, 2019, you may send the invoice showing the amount, your name, and a copy of your driver's license or State ID to the department for reimbursement of up to $250.00 for up to one year of monitoring. Invoices must be received by August 15, 2019 in order to be reimbursed.

You may mail the documents to:

Office of Information Technology Services
Attn: Enterprise Architecture Branch
650 Iwilei Road Ste 332
Honolulu, Hi 96817

If you do not know of any credit monitoring companies we have listed a few that provide credit monitoring services. If you have a preferred credit monitoring service please feel free to use them.

Experian
https://www.experian.com/consumer-products/compare-identity-theft-products.html?v=c01

Identity Force
https://secure.identityforce.com/sales_landing/step2?offer=sasuspc&SSAID=514792&asid=50050

Identity Guard
https://www.identityguard.com/compare-plans.html

What you can do?

We also urge you to carefully monitor your credit card statements and to take heightened protective measures including:

- Obtain and carefully review your credit reports. You can order free credit reports from all three credit agencies at https://www.annualcreditreport.com
- Review your bank and credit card statements regularly and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately if you notice any irregularity in your credit report or any account. If your accounts or identity have been compromised, you may take immediate actions such as requesting refunds, closing accounts, placing your credit reports in a state of "fraud alert" or "freeze", and filing a police report.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information

If you have questions, please call Jonathan Chee at (808) 564-9448, Monday through Friday 8:00 am to 5:00 pm Hawaii Standard Time (HST)

Protecting your information is important to us. We trust that the service we are offering to you demonstrates our continued commitment to your security.

Sincerely,

Brook Conner
Assistant Superintendent and CIO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, Tx 75013, www.experian.com, 1-888-397-3742
Transunion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-888-909-8872

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order you annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228.**

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes: (2)Social Security Number: (3) date of birth (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your stat's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission,** Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

IdentityTheft.gov Offers Free Personal Recovery Plans

Visit IdentityTheft.gov if you believe you have been the victim of identity theft, or if your personal information has been lost or exposed. IdentityTheft.gov is the federal government's free, one-stop resource for reporting and recovering from identity theft. The website, available in Spanish at RobodeIdentidad.gov, will provide you with a personal, interactive recovery plan tailored to your individual identity theft needs. It will:

- Walk you through each recovery step
- Generate an Identity Theft Report and pre-filled letters and forms for you to send to credit bureaus, businesses, debt collectors, and the IRS
- Adapt to your changing needs, provide you with follow-up reminders, and help you track your progress
- Give advice about what to do if you're affected by specific data breaches

IdentityTheft.gov has recovery plans for more than 30 types of identity theft, including tax-related identity theft and identity theft involving a child's information.