State of South Carolina
Office of the Inspector General

MEMORANDUM REPORT

DATE: 1/29/2016

The Office of the State Inspector General (SIG) reviewed the potential misuse of state assets by state employees using state email addresses or state Internet Protocol (IP) addresses to access an "Ashley Madison" account.

Ashley Madison is a commercial "adult" website designed to enable extramarital affairs. This review was initiated based on August, 2015 public media reports that South Carolina state government email addresses were contained in leaked stolen information from the Ashley Madison website. The leaked stolen information contained approximately 32 million users and approximately 10 gigabytes of data, which was publicly posted on the Internet by the hackers of the Ashley Madison website.

Below table sets forth summary of leads sent to 36 State agencies receiving referenced communications:

Lead Data	Higher Ed (HESS)	Non Higher Ed (NHESA)	Totals
Agencies Involved	11	25	36
State Email Accounts Used	526	8	534
Private Email Accounts Used	27	58	85
State IP Address Used	8	36	44

All 36 State agencies provided the SIG the results of their respective administrative investigations. A summary of these agencies' ability to identify a State employee associated with each investigative lead is as follows:

Investigative Lead Result	Higher Ed (HESS)	Non Higher Ed (NHESA)	Totals
Not Identified or Student	460	47	507
Former Employee, Contractor, or Public	57	6	63
Employee Identified	35	14	49
Total	**552**	**67**	**619**

Of the 49 State employees identified as associated with an investigative lead, their respective agency's administrative actions were as follows:

Administrative Action	Higher Ed (HESS)	Non Higher Ed (NHESA)	Totals
No Action Taken	16	4	20
Counseling	17	5	22
Oral Reprimand	2	2	4
Written Reprimand	0	2	2
Oral Reprimand and Leave of Absence	0	1	1
Total Employees Identified	**35**	**14**	**49**

(See the SIG's cover email to Agency Heads, dated 10/23/2015, and letter to Agency Heads, dated 10/22/2015 attached to this memo.)

Observations based on reviewing State agencies' investigative results:

1. As of June 30, 2015, SC State Office of Human Resources reported having 59,285 employees in the Executive Branch, excluding non-regulatory agencies. Of those employees, 49 (0.082%) were associated with potentially misusing State resources to access the Ashley Madison website.

2. Many of the IP addresses could not be linked to a specific user. Rather, the IP addresses were forward-facing IP addresses of agencies' routers. Others used agencies' public Wi-Fi IP addresses, wherein guests or the general public were allowed Internet access.

3. The vast majority of email addresses belonged to students at State universities which were not included in the scope of this review as set forth in referenced communications.

4. There were several instances where employees were victims of identity theft, to include their credentials being inappropriately used to gain email access.

5. The organizational controls to protect against this type of misconduct are enhanced specificity in codes of conduct/policy on appropriate Internet use and employee Internet awareness training.

6. It should be noted public media has reported scammers exploiting this open Internet data for extortion purposes. This Executive Branch-wide effort has mitigated the risk of an extortion of a State employee, both individually and any derivative impact on State government.

The SIG considers the data owner of the initial lead information to be the Division of Technology, Department of Administration (DOA), therefore any FOIA request for this data will be referred to the DOA. All 36 State agency results responses to the SIG are directly connected to a personnel misconduct investigation, therefore any FOIA request for this data will be referred to those agencies.

Patrick J. Maley
State Inspector General

From: Maley, Patrick
Sent: Friday, October 23, 2015 4:53 PM
To: [Agency Director]
Cc: xxxxxx
Subject: State Inspector General Request re Potential Misuse of State Assets Within Your Agency
[SECURE]

Dear Director xxxxxx:

Attached to this email is a PDF file containing a self-explanatory letter from the State Inspector General to the Agency Head. An original hard copy letter is being sent as well through the mail service.

The attached letter requests Agency Heads to initiate administrative inquiries based on lead information that employees within your agency used a state email account or state Internet IP address to access open Ashley Madison accounts on an "adult" website designed to facilitate extramarital affairs. As you may recall, national public media reports raised this issue in August 2015.

The SIG organized and analyzed data developed by the Division of Technology, DOA, which identified 36 state agencies having 534 state email accounts (526 Higher Ed; 8 Non-Higher Ed) accessing open Ashley Madison accounts. Additionally, 85 private email addresses (27 Higher Ed; 58 Non-Higher Ed) used 44 state IP addresses to access open Ashley Madison accounts. The data was stratified between Higher Ed and Non-Higher Ed inasmuch as the SIG is requesting administrative inquiries on **state employees only and not students** for obvious reasons. All data on students is left to the discretion of the higher education Agency Head for any action deemed appropriate. The data developed of lead value pertaining to your agency will be sent via a separate encrypted email to your Human Resource Director.

Inasmuch as these administrative inquiries & likely agency adjudications are personnel matters involving potential misconduct, agencies are to return investigative results to the SIG in an established non-attributable summary format to allow the SIG to summarize final results of this effort, as well as ensure agencies conducted adequate follow-up to leads provided.

As distasteful as this effort may be to execute by those involved and to be involved, it is necessary to address this potential misconduct issue undermining the public's confidence in state government.

Thank you in advance for rigorously addressing this issue to maintain the high integrity workplace the public expects of South Carolina state government.

State of South Carolina
Office of the Inspector General

October 22, 2015 OIG File # 2015-1414-I

[Name of Agency Head]
[Agency Name]
[Address]
[City, State Zip]

Re: Potential Misuse of State Assets by State Employees Accessing Ashley Madison Accounts

Dear [Name of Agency Head],

The Office of the State Inspector General (SIG) is reviewing the potential misuse of state assets by state employees using state email addresses or state Internet Protocol (IP) addresses to access an "Ashley Madison" account. If you are an Agency Head recipient of this letter, then your agency has been identified as either having an agency email address, agency IP address, or both used to access an Ashley Madison account, which could potentially be a misuse of state assets violating your agency's policies or code of conduct. As a result, the SIG is requesting your agency conduct a logical administrative inquiry into the potential misuse of state assets or other potential misconduct issues using the background set forth in this letter and the Ashley Madison website data of lead value connected to your agency. This lead value data will be sent to your Human Resource Director via a separate encrypted email.

Ashley Madison is a commercial "adult" website designed to enable extramarital affairs. This review was initiated based on August, 2015 public media reports that South Carolina state government email addresses were contained in leaked stolen information from the Ashley Madison website. The leaked stolen information contained approximately 32 million users and approximately 10 gigabytes of data, which was publicly posted on the Internet by the hackers of the Ashley Madison website.

At the request of the State Inspector General, the Division of Technology, Department of Administration, analyzed the leaked Ashley Madison data. The data was analyzed in total and stratified into two categories: higher education state schools (HESS) and non-higher education state agencies (NHESA). These data categories clearly separated the HESS data inasmuch as this review focuses on state employees and not students.

The analysis of Ashley Madison records identified 36 state agencies (11 HESS; 25 NHESA) having 534 state agency email addresses (526 HESS; 8 NHESA) and 44 state agency IP addresses (8 HESS; 36 NHESA) used to access an Ashley Madison account. The 44 IP

addresses used 85 private email addresses (27 HESS; 58 NHESA) to access an Ashley Madison account.

The review identified 267 suspected state email addresses (260 HESS; 7 NHESA) which were used in unsuccessful attempts to open an Ashley Madison account. In order to complete the opening of an Ashley Madison account, Ashley Madison validated the account, such as sending an email to the application email address with a unique link to be clicked or a unique verification code to be entered. This validation control was likely intended to prevent the unauthorized use of someone else's email address. As a result of not accessing an Ashley Madison validated account and the risk, as well as likelihood, of misusing someone else's state email address, no further investigation on these 267 state email addresses was deemed necessary.

There are two streams of Ashley Madison data that generate potential leads to identify state employees potentially misusing state assets:

1. Ashley Madison Accounts Opened with a State Email Address

The Divisions of Technology's analysis identified 534 state email addresses (526 HESS; 8 NHESA) used to open Ashley Madison accounts. Only one state email address was used to make credit card payments.

2. State Agency IP Addresses Used to Access Ashley Madison Accounts with Private Email Addresses

The data analysis identified 85 entries from validated Ashley Madison accounts contained in the breached data originating from state IP addresses using private email addresses. Of these 85 entries, 27 entries used private email addresses at eight IP addresses at HESSs while 58 entries used private email addresses at 36 IP addresses at NHESAs. The recovered Ashley Madison data for each entry contained time of entry and the longitude/latitude of the device accessing the state IP address. Seventeen credit card transactions from six private email addresses were made through state IP addresses.

It should be noted the entries using IP addresses occurred predominately in 2013, but the agency location of the IP address was determined by the Division of Technology with an effective date of September 1, 2015. Another complicating factor is IP addresses may not go direct to a specific computer with one dedicated user, such as Wi-Fi access addresses; non-static IP addresses; public access or group terminals; IP addresses reconfigured or re-assigned since the Ashley Madison account transaction; non-state employee access allowed; and any other location with allowed access by more than one state employee.

A summary of data presented above is as follows:

	Higher Ed (HESS)	Non Higher Ed (NHESA)	Totals
Agencies Involved	11	25	36
State Email Accts Used	526	8	534
Private Email Accts Used	27	58	85
State IP Address Used	8	36	44

REQUEST OF THE STATE INSPECTOR GENERAL

Your agency is requested to conduct a logical administrative inquiry regarding your agency's email addresses and/or IP addresses used to access an Ashley Madison account or webpage, which could potentially be violations of your agency's policies or code of conduct. The Ashley Madison data pertinent to your agency has been sent to your agency's Human Resource Director via an encrypted email file. The Ashley Madison data is provided on spreadsheets with blank data fields [employee identified (yes/no); administrative action taken; and comments] for your agency to complete documenting resolution of your administrative inquiry into each agency email address or IP address used. The completed spreadsheets will be returned to the SIG to capture **non-attributable summary data** on this effort due to the personnel misconduct nature of this inquiry, as well as ensure agencies conducted adequate follow-up to leads provided.

For HESSs, the SIG only requests responses where administrative inquiry involves faculty and staff. All investigative leads involving students is completely left to the discretion of the Agency Head and should not be reported to the SIG. Only state employees are the subject of this review.

Please provide spreadsheets with resolution fields completed to the SIG via an encrypted email at oig@oig.sc.gov with a deadline of January 22, 2016. If you have any questions, please contact Investigator Caroline Overcash, telephone 803/896-4743 or email carolineovercash@oig.sc.gov.

The SIG thanks you in advance for rigorously addressing potential professional misconduct issues undermining the public's confidence in state government.

Sincerely,

Patrick J. Maley
State Inspector General

cc: [Agency Human Resource Director]