State of South Carolina
Office of the Inspector General

MEMORANDUM

DATE: 1/29/2016

TO: Inspector General Patrick J. Maley

FROM: Investigator Caroline Overcash

RE: Closing File 2015-1414-I (Ashley Madison)

Reference is made to State Inspector General (SIG) Maley's cover email to Agency Heads, dated 10/23/2015, and SIG Maley's letter to Agency Heads, dated 10/22/2015.

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**

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.

It is recommended this matter be closed.