There is a massive amount of data to collect for use in an investigation of this type. This is just a summary of actions to assist.

Did the leaving person, actually depart the office yet? How are we sure? Has the person returned to the office to retrieve anything 'forgotten'?

The departing person is famous for deleting data. Did anyone verify this has not happened. If the data has been deleted or altered it would be a felony destruction of state property (data) on a state owned computer(s) to thwart an investigation. Did the departing person's computer get secured by DCI? Is there a full backup of the person's work PC in the State's archives? What is the procedure for securing a departing employee's digital footprint?

Are all the servers and the backup data touched by this office and the personnel secured? This includes the computers / servers of the exchange server data left by the departed person. There should be backups of this data available to restore emails and data from any moment in time needed. Exchange servers are used for e-mail processes and data synchronizing so users can log into data from multiple computers.

Midcontinent Communications serves most of Pierre, what IP addresses have Powers and Gant used from their Pierre homes since January 2011. This information will establish their home IP addresses and will set their private / home time internet activity versus State of South Dakota SOS

office computer use. On each email sent to customers or during website activity these IP addresses are attached for comparison as to time and place. The likely email sent to the vendor, purchaser or receiver should also have this information.

If Gant and Powers were doing their political work during office hours, using SD internet connectivity on their own personal computers and / or smart phones the IP addresses will also be saved with email correspondence timestamps.

Do not forget to have the Midphase.com servers in Utah subpoenaed for information on dakotawarcollege.com (DWC), dakotacampaignstore.com (DCS), postcardpro.com, jasongant.com and patpowers.com.

Needed information will include

1. How many websites does / did Pat Powers control during his state employment (was he hosting / controlling customer's sites and if he was, during SOS office time?)
2. Godaddy.com and Whois.com data for each site
3. date service started for each website on midpahse.com or other servers
4. directory structure of all folders with file names for each site
    a. January 1, 2011 (Gant / Power's employment date)
    b. January 1, 2012 (Gant / Power's one year

anniversary)

c. May 1, 2012 (the likely data available prior to the start of this investigation) On May 9, 2012 Powers was still operating Dakota Campaign Store with a direct link from Dakota War College

d. June 1, 2012 (or any other date close to verify if data has been destroyed)

e. A side note to this investigation, you may find a file structure being 'saved' under a different hidden link system. These may be the 'deleted' DWC and DCS files and pages. Powers is not the type of person to destroy years of work easily, it is likely hidden for his easy access when 'needed'. By now he may have backups at hidden at home or safe place.

5. The change logs for each server and website
6. Is the E-mail activity saved from SD state owned exchange server, dakotawarcollege.com, dakotacampaignstore.com, postcardpro.com, jasongant.com, patpowers.com and Pat Powers yahoo.com webmail account used for the website management as reported by whois.com. This would include the deleted emails. The sending of e-mails to customers or strategy
7. Website movements list documenting the different servers for each of the listed websites until they were up and running on Click Rain Servers based out of Sioux Falls, SD approximately June 27, 2012
8. Was Pat still using / participating in the political blog DWC, especially during the hours he was being paid

by the state as an employee? Examining the comment and access logs will help with this determination

9. As a state SOS office employee, Pat Powers was still listed as webmaster / contact for Jason Gant's campaign website in June 2012. What is the ethics of having your state employee still operating your campaign machinery?

SD Department of Revenue should have sales tax reports for Dakota Campaign Store for the time it was started through to the primary election of 2012. Sales were reported by on-line admission by at least one candidate. There should be a trail to follow as to when the orders were placed by customer, order placed with supplier and the delivery with payment by customer (what time where the orders placed and from what IP address?).

Purchase orders to / from suppliers, if these POs were called in to suppliers there would be artwork files to accompany. What phone#, time and IP address were attached to emails?

Cellphone logs should be examined, state and personal to determine whose phone actually was used to receive, place and track merchandise

Once the data and software code are secured, have forensic experts read the cryptic software code to look for holes or backdoors. This is a standard procedure in many

sensitive positions in sensitive offices, especially in potential criminal probes.

Please look at the code to verify if public access has been compromised. There could be a programmed or manual list of 'special' names, IP addresses, or webmail addresses / servers. These special programmed lists are often containing information on reporters, legislators, officials of agencies, political opponents or persons of personal interest webmasters / administrators want to follow.

Was there special consideration in transcribing and the posting of candidate financial reports prior to the June Primary election?

There are rules and laws governing the office of Secretary of State. There are programming rules to be followed for writing software. These software 'style' rules are followed by programmers so if one person leaves, another can come in and follow the code. No two people write exactly the same or accomplish the goal using the same thought process, so this can be time consuming and tedious. The state should have code standards to follow and others familiar with the style book should be able to see potential problems.

There should be data logs allowing investigators to see who has had access to SQL server based data. In our database controlled world there are transaction logs to be mined. With sensitive data, there should be controls on who and

what data can be accessed. With a terminated employee, a good manager or law enforcement (if called) would attempt to secure the computers and data including logs.

To do a forensic process like this, the investigators must consider multiple angles for each area of the office functions and how the code could be used. We have discussed many possibles in this and other threads.

In the past, ‘time bombs’ have been found where code has been written to erase itself after a job is done. We do not know Pat’s level of programming knowledge but with his history this is a concern

In ballot tabulating and voting equipment there are reports these processes being used in the past to erase ballot tabulating code loops once the changes have been made. Hackers around the world use forms of this to steal data.

There should be an email chain between the computers / exchange server account of Sec Gant and Pat Power’s multiple email accounts, was there a conspiracy between the two to collude, deceive and elude?