Filed scanned BBB

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

Curling, et al.
Plaintiff
v.
Raffensperger, et al.
Defendant

Civil Action No. 17-cv-02989

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Nwakaego Nkumeh, Vice President and Chief Legal Affairs Officer, Kennesaw State University, Town Point, Suite 3400, 3391 Town Point Dr. NW, Kennesaw, GA 30144 Phone (470) 578-3562

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: SEE ATTACHED EXHIBIT A

Place:	Date and Time:
Ichter Davis LLC, 3340 Peachtree Rd NE, Suite 1530, Atlanta, Georgia 30326, or email to bbrown@brucepbrownlaw.com	07/18/2019 11:00 am

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 07/09/2019

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* COALITION FOR GOOD GOVERNANCE, who issues or requests this subpoena, are:

BRUCE P. BROWN,1123 ZONOLITE RD. NE, ATLANTA GEORGIA 30306 (404) 881-0700

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 17-cv-02989

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

INSTRUCTIONS

1. Prior to answering the following, you are requested to make due and diligent search of your books, records, and papers, with a view to eliciting all information available in this action.

2. If you object to any request, please identify the basis for the objection and identify each document that is being withheld on the basis of that objection. Please also state if, notwithstanding the objection, all responsive documents are being produced.

3. The requests set forth below are deemed to be continuing, so as to require the supplementation of your original production of documents in response to such requests promptly after any additional documents are located.

4. If any document responsive to this request was, but no longer is in your possession, state whether it is missing or lost; if it has been destroyed; if it has been transferred, voluntarily or involuntarily, to others; or if it has otherwise been disposed of. In each instance, identify the document fully, explain the circumstances, and identify the people having knowledge of such circumstances.

5. If you contend that any documents covered in these requests are not reasonably accessible or would be unduly burdensome to locate or produce, identify such documents by category and source and provide detailed information regarding the burden or cost you claim is associated with the search for or production of such documents.

6. To the extent documents produced in response to this request include electronic documents, such as spreadsheets or databases, you shall produce all such documents in native form, insuring that all formulae and metadata embedded in such documents are produced.

DEFINITIONS

1. The term "communications" means any oral, written, or electronic transmission of information, including without limitation any face-to-face meetings, letters, emails, text messages, social media messaging, or telephone calls, chat rooms, or group list serves.

2. The term "document" is intended to be as comprehensive as the meaning provided in Rule 34 of the Federal Rules of Civil Procedure, and includes, without limitation, all originals of any nature whatsoever, and all non-identical copies thereof, pertaining to any medium upon which intelligence or information is recorded, including electronic storage, in your possession,

custody or control, regardless of where located; including, without limiting the generality of the foregoing, emails, spreadsheets, databases, papers, punch cards, printout sheets, movie film, slides, phonograph records, photographs, microfilm, notes, letters, memoranda, ledgers, work sheets, books, magazines, notebooks, diaries, calendars, appointment books, registers, charts, tables, papers, agreements, contracts, purchase orders, acknowledgments, invoices, order confirmations, authorizations, budgets, analyses, projections, transcripts, minutes of meetings of any kind, correspondence, telegrams, drafts, data processing discs or tapes, and computer produced interpretations thereof, x-rays, instructions, announcements, schedules, price lists, and mechanical or electric sound records and transcripts thereof. In all cases, where originals are not available, document also means identical copies of original documents.

3. The term "GEMS Database" means the Diebold system Microsoft Access database used for programming, recording and reporting the referenced election. It shall have the same meaning as "GEMS database" as used in the Rules and Regulations of the State of Georgia, including Rule 183-1-12.07(5) and (6).

4. The term "person" means any individual, corporation, partnership, proprietorship, association, organization, governmental entity, group of persons or any other entity of whatever nature.

5. The terms "relate to" or "relating to" means consisting of, referring to, regarding, reflecting, supporting, prepared in connection with, used in preparation of, or being in any way logically or factually connected with the matter discussed.

6. The term "Secretary" means the Secretary of State of Georgia and the Office of Secretary of State and all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on behalf of the Secretary.

7. The term "you" means the University System of Georgia unit Kennesaw State University ("KSU") and its former unit Center for Election Systems ("CES") while located on the KSU campus and all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf.

8. The term "DRE" means a direct recording electronic voting device which is a computer driven unit for casting and counting votes on which a voter casts

his or her votes through the use of a touch screen. The term shall include both state supplied devices and devices purchased by counties.

DOCUMENTS TO BE PRODUCED

1. Documents and all communications that relate to the decision, or implementation of the plan to destroy the electronic data on the elections.kennesaw.edu server.

2. Documents and all communications that relate to the decision, or implementation of the plan to destroy the electronic data on the Unicoi.edu server.

3. Communications concerning the retention, preservation, alteration or destruction of data on the elections.kennesaw.edu server that include in the distribution list any staff, employees, or officials of the Georgia Secretary of State's office.

4. Logging records for the elections.kennesaw.edu and the unicoi servers beginning January 1, 2016.

5. Documents related to the server scans and the 40+ "critical vulnerabilities" found on the elections.kennesaw.edu server and "critical vulnerability"

discovered on the Unicoi server referenced on Exhibit A p. CGG 00000164-165 and 00000171.

6. A complete image of the "fully working clone" for the elections.kennesaw.edu server referenced on Exhibit A p. CGG00000169

7. The documents referenced as cached on search engines on Exhibit A p. 000000171.

8. Documents reflecting or regarding the scans referenced on Exhibit A p. 00000171-175.

9. The electronic records obtained in the "data recovery" referenced on Exhibit A p. 00000005

10. Images of electronic files on the elections.kennesaw.edu server prior to its delivery to the FBI, and after its return.

11. Images of the electronic files on the unicoi. edu server prior to the destruction of its hard drive in 2017.

12. Documents showing all communications and distribution lists referencing or related to the "DBAN" of the hard drives referenced on Exhibit A p. 00000006.

13. All communications with any employees, official or representatives of the Secretary of State's office concerning the preservation of electronic records on the elections.kennesaw.edu servers after January 1, 2016.

14. All communications after January 1, 2016 with any representative of Election Systems & Software ("ES&S") concerning the topics of location or security of electronic files files or servers under the control of Center for Election Systems.

15. Communications indicating that the date of the deletion of the electronic data on the elections.kennesaw.edu server was done on or about March 17, 2017.

16. All communications and documents indicating or referencing all advice, orders, suggestions, recommendations or decisions to destroy the electronic records on the elections. Kennesaw. edu server and the uncoi.edu server.

17. All documents that indicate the deletion or removal of logging records from the elections.kennesaw.edu server between January 1, 2016 and March 15, 2017.

18. All documents related to the instruction to installation or reimageing or DBAN the hard drives referenced in Exhibit A 00000043

19. The document referenced at Attachment March 03 0258 v1 on Exhibit A 00000105

20. All documents including telephone call notes referencing or related to the documents and the transmission to counties referenced on Exhibit A 00000106.

21. All communications beginning January 1, 2016 between ES&S and CES staff related to GEMS databases.

22. All documents and evidence supporting the statement in the Kennesaw State University press release on Exhibit A p. 00000110 that "no person information was compromised."

EXHIBIT A

October 11, 2017

Jeff Milsteen
Chief Legal Affairs Officer
Kennesaw State University
Via email jmilstee@kennesaw.edu

Dear Mr. Milsteen:

Under the Georgia Open Records Act § 50.18.70 et seq., Coalition for Good Governance is requesting the following records supplied in electronic format:

1. All communications regarding or related to the preservation, back-up, deletion, copying, and/or destruction of data on the server "elections.kennesaw.edu" This request relates to communications during the period March 1, 2017 through October 8, 2017.
2. All communications regarding or related to the preservation, back-up, deletion, copying, and/or destruction of data on the server "unicoi.kennesaw.edu." This request relates to communications during the period March 1, 2017 through October 8, 2017.
3. All communications indicating the physical location, custody and status of each server named above, and whether the servers are currently in use in any location.
4. All agreements, contracts, instructions for review or analysis of the data associated with the above-mentioned servers. The date of this request relates to documents created after July 1, 2016.
5. All communications created after July 1, 2016 concerning the existence, preservation, deletion, back-up, copying and/or analysis of the web logs associated with each of the above-mentioned servers.

If there are any fees for searching or copying these records, please inform me if the cost will exceed $50. However, Coalition for Good Governance, a non-partisan 501(c) (3) organization, with members who are residents of Georgia, requests a waiver of all fees because the disclosure of the requested information is in the public interest and will contribute significantly to the public's understanding of the operations of electronic voting equipment and reporting of results. This information is not being sought for commercial purposes.

The Georgia Open Records Act requires a response time to produce those records within three business days. If production of the records I am requesting will take longer than three days, please contact me with information about when I might expect copies or the ability to inspect the requested records.

If you deny any or all of this request, please cite each specific exemption on which you base your denial of the election information and notify me of the appeal procedures available to me under the law.

Thank you for your consideration. Please contact me at the email or phone number below with any questions.

Sincerely,

Marilyn Marks
Exec. Director
Coalition for Good Governance
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1618
Marilyn@USCGG.org

From: Jeff Milsteen <jmilstee@kennesaw.edu>
Date: Friday, October 20, 2017 at 10:15 AM
To: Marilyn Marks <marilyn@aspenoffice.com>
Cc: asklegal <asklegal@kennesaw.edu>, Cristina Correia <ccorreia@law.ga.gov>
Subject: Fw: ORR for data retrieval from elections.kennesaw.edu

Ms. Marks,

Attached please find the records responsive to your open records request. All records have been produced except documents that would be exempt pursuant to OCGA 50-18-72(a)(41), which excepts privileged attorney-client communications from the disclosure requirements of the Open Records Act. To be clear, the record that has been withheld involves communications between the Office of the Attorney General and employees of Kennesaw State University, and not internally between the Legal Affairs Division and employees of the Center for Elections Systems or UITS.

Sincerely,

Jeff Milsteen

Chief Legal Affairs Officer

Kennesaw State University

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 15, 2017 10:51 AM
To: Michael L. Barnes; Merle Steven King
Subject: Request for data retrieval from elections.kennesaw.edu

We would like to retrieve certain records from elections.kennesaw.edu, including equipment inventory records and workflow databases used during ballot building. These data are located in the *cesuser* user directory at /home/cesuser. We would like to retrieve the entire *cesuser* directory.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: Stephen Craig Gay
To: Lectra Lawhorne
Subject: CES Investigative update
Date: Friday, March 17, 2017 5:11:58 PM

Lectra,

Good afternoon. I wanted to take a moment and provide you with an update on the Center for Election Systems Incident Response process:

- We met with CES Staff today to review the architecture of their internal network, review physical access controls, and understand the services running on the internal network. We validated that an air gap exists between the internal and external network and further validated via arp tables that no routes were available from the intranet servers to an external network. Several opportunities for improvement were identified and CES staff are working on documentation for the system. An executive summary with recommendations is forthcoming

- All external-facing servers associated with the Center are isolated to elections.kennesaw.edu which is hosted in the Enterprise instance of OmniUpdate and contains only public information.

- UITS WinServ, in partnership with the ISO and CES, is provisioning a dedicated Virtual Server which will be used for internal file storage for CES. The server will be locked down via AD group memberships and will use verbose logging and monitoring tied to our splunk instance. The logs will specifically audit for file access and alert on any modifications to the authorizing AD group. Furthermore a local firewall will be in place and all traffic outside the CES IP range blocked.

- I met with FBI Agent Ware at 4:30pm to receive the elections server - Dell PowerEdge R610 Tag Number 96J2F21. The ISO team will be performing a data recovery for data requested by the CES (Business Operations) on Monday. We have confirmed that the FBI is maintaining a forensic image and changes to the server can occur. Agent Ware shared that "the investigation is wrapping up" and mentioned being in attendance at the March 29th meeting with AUSA Grimberg.

Please let me know if you have any questions or if I can provide any additional information.

In service,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

Milestone	Due Date	Status	Lead	Notes
Private Network Assessment Meeting	26-Jun	Complete	S. Gay	
Spec UPS	13-Jul	Complete	C. Dehner	
Order UPS	13-Jul	Complete	C. Dehner	
DBAN R610 Hard Drives	7-Jul	Complete	C. Dehner	
Deliver R610 to Networking	7-Jul	Complete	C. Dehner	
Image Dell PowerEdge R630s (101614 & 101613)	26-Jul	Complete	C. Darrow	
Rack Dell PowerEdge R630 and migrate DC and NAS	28-Jul	In progress	C. Darrow	
Install UPS	4-Aug	Complete	C. Darrow	Due data dependant on delivery of UPS from CDW-G.

192.168.3.135	Linux 2.6.8	•M6600M85		IMI Card Duplicator	
192.168.3.119	Linux 2.6.8	•M6600M73		IMI Card Duplicator	
192.168.3.81	Linux 2.6.8	•M6600M80		IMI Card Duplicator	
192.168.3.73	Linux 2.6.8	•M6600M72		IMI Card Duplicator	
192.168.3.116	Linux 2.6.8	•M6600M82		IMI Card Duplicator	
192.168.3.104	Linux 2.6.8	•M6600M70		IMI Card Duplicator	
192.168.3.115	Linux 2.6.8	•M6600M71		IMI Card Duplicator	
192.168.3.130	Linux 2.6.12	•M6600M81		IMI Card Duplicator	
192.168.3.76	Linux 2.6.8	•M6600M69		IMI Card Duplicator	
192.168.3.123	Linux 2.6.8	•M6600M26		IMI Card Duplicator	
192.168.3.128	Linux 2.6.8	•M6600M79		IMI Card Duplicator	
192.168.3.131	Linux 2.6.8	•M6600M84		IMI Card Duplicator	
192.168.3.71	Linux 2.6.8	•M6600M83		IMI Card Duplicator	
192.168.3.132	Linux 2.6.8	•M6600M86		IMI Card Duplicator	
192.168.3.69	Linux 2.6.8	•M6600M417		IMI Card Duplicator	
192.168.3.66	Linux 2.6.8	•M6600M74		IMI Card Duplicator	
192.168.3.2	Microsoft Windows Server 2003 R2 SP2	•SEMINOLE			
192.168.3.53	HP P2055 Series	•Fax-Printer •FAX-PRINTER			
192.168.3.55	Microsoft Windows XP	•SDEAN-GEMS-2			
192.168.3.57	Microsoft Windows XP	•CALLCENTER			
192.168.3.50	Microsoft Windows Server 2008 R2, Standard Edition	•EPIC			
192.168.3.4	Microsoft Windows Server 2008 R2, Enterprise Edition	•CES-DC1			
192.168.3.3	Microsoft Windows Server 2008 R2, Standard Edition	•CES-NAS			
192.168.3.1	Microsoft Windows Server 2008	•CES-DC.CES.KENNESAW.EDU			
192.168.3.54	Microsoft Windows XP	•MPEARSO9-980			
192.168.3.56	Microsoft Windows XP	•GEMS-DDESSERT			
192.168.3.60	Microsoft Windows 7 Home, Premium Edition SP1	•STEVEN7-GEMS		Audio recording	
192.168.3.70	Windows XP	h57-marie.CES.KENNESAW.EDU			
192.168.3.65	Windows XP	GEMS-mking.CES.KENNESAW.EDU			
192.168.3.51	Microsoft Windows 7.5	•KSLICES-2HALL		Audio recording	
192.168.3.61	Unknown				
192.168.3.52	Windows XP	seminole-termin.CES.KENNESAW.EDU			

From: Christopher Dehner
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus
Date: Wednesday, August 9, 2017 11:24:58 AM

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

STATE OF GEORGIA

FULTON COUNTY

AGREEMENT BETWEEN THE SECRETARY OF STATE

AND

THE BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA

This AGREEMENT ("Agreement"), made this 6th day of June, 2016, by and between the OFFICE OF THE SECRETARY OF STATE OF THE STATE OF GEORGIA (hereinafter the "Secretary of State") and the BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA through KENNESAW STATE UNIVERSITY, a unit of the University System of Georgia, (hereinafter "University") for the consulting services of the Center for Election Systems of KENNESAW STATE UNIVERSITY (hereinafter "KSU").

WITNESSETH

WHEREAS, the Secretary of State desires to employ the services of KSU to assist the staff of the Elections Division of the Office of the Secretary of State (hereinafter "the Elections Division") with: technical support and training of State election officials in the use of the Statewide uniform electronic voting system (hereinafter "the voting system") in the State of Georgia; acceptance testing for the fiscal year 2017 of the GEMS software, the direct recording electronic voting devices (hereinafter "DREs"), and the electronic poll book/encoders "ExpressPoll" which constitute components of the voting system; ballot building and related activities for counties and municipalities in the State of Georgia ("State");

WHEREAS, the Secretary of State has the authority under the Laws of the State of Georgia to enter into this Agreement; and

WHEREAS, the University is both qualified to enter into this Agreement and has offered such services to the Secretary of State under the terms and conditions stated herein; and

WHEREAS, the parties wish to enter into this Agreement under the terms and conditions set forth herein;

NOW THEREFORE, in consideration of the mutual promises and agreements hereinafter set forth, the satisfactory consideration each for the other hereby expressly recognized and agreed, the parties hereby contract for services in accordance with the following provisions.

ARTICLE I. SCOPE OF SERVICES

KSU will assist the staff of the Elections Division under the direction of and as directed by the Director of the Elections Division or his/her designee, in the following areas:

A. KSU shall maintain a "Center for Election Systems" (hereinafter "the Center") that will primarily provide technical and training support on the statewide uniform system to the Elections Division, Georgia election officials, county election board members and election superintendents;

B. KSU shall test the voting system for compliance with the Georgia Elections Code, as required under Article 9 of Chapter 21 of the Official Code of Georgia and under the Rules of the State Election Board and the Rules of the Secretary of State, as these laws and rules presently exist and may hereafter be amended. This testing to be conducted during Fiscal Year 2017 shall include, but is not limited to, the physical examination of software and voting equipment acquired by the Secretary of State or any County in the State of Georgia in connection with deployment of the voting system, and the preparation and submission of reports of such evaluations to the staff of the Elections Division;

C. KSU shall work with the vendor and the Elections Division to define the next versions of all components of the voting system;

D. KSU shall implement classes and training modules, using electronic media where possible, for the instruction of Election Superintendents and Voter Registrars in the use of the voting system;

E. KSU shall provide ballot building support for county election officials. KSU will provide office space and appropriate technical support for these services. KSU will coordinate the printing of paper absentee ballots;

F. KSU shall support the deployment of the ExpressPoll electronic pollbook, including preparation of compact flash memory cards with voter lists for each election and extraction of credit-for-voting data, post-election;

G. KSU shall support all State certification testing of voting systems and will provide acceptance testing for the State's voting system

H. KSU shall provide technical support for the State's election servers installed in the county election offices throughout the State;

I. KSU shall provide consultation and advice to local governments on the purchase, testing, and utilization of the software, voting equipment and other components which comprise the voting system;

J. KSU shall maintain a website that will provide an initial point of contact for election officials wishing to utilize the services of the Center. The website shall describe the various services available through the Center, provide directions for obtaining these services from the Center, and facilitate answers to "frequently asked questions";

K. KSU shall maintain a Help Desk designed for immediate response to problems encountered with any component of the voting system during the conduct of an election in any precinct. The Help Desk shall be staffed from 8:00 a.m. to 5:00 p.m. on all business days throughout the year, and from 6:00 a.m. until County tabulations are concluded on election days;

L. Upon request of the Secretary of State, KSU shall assist the Secretary of State with identifying, inspecting, and/ or implementing a new state wide voter registration system which will allow integration with the voting system;

M. Upon request of the Secretary of State, KSU shall provide key faculty/employees identified as the Executive Director, Director, and Assistant Director of KSU with Blackberry technology or equivalent email and messaging capabilities;

N. KSU shall coordinate the proper disposal of decommissioned voting system components at the direction of the Elections Division;

O. KSU shall provide consulting services to Secretary of State on legislation or pending legislation and laws affecting elections;

P. KSU shall provide any other election services as may be required by the Elections Division;

ARTICLE II. RESPONSIBILITIES OF KSU

KSU shall continue to maintain a permanent location on the KSU campus for the operation of the Center. The Center shall be operated and maintained by a full-time staff, including but not limited to, an Executive Director, a Center Director, a Center Assistant Director, technical support staff, and student assistants. The Center shall contain voting equipment and software, provided by the Secretary of State, necessary to completely define, setup and conduct a sample election. The Center shall maintain a ballot building facility to house Center staff and Elections Division staff for the purpose of building ballots for counties and municipalities.

KSU shall not possess, obtain, or acquire, either directly or indirectly, a pecuniary interest in any business entity involved in the development, manufacture, marketing, or sale of computer voting equipment or software during the term of this Agreement and for one year after the ending date of this Agreement.

Any software, databases, or other analytic tools obtained or developed in support of activities covered under this Agreement and any work product resulting from activities covered under this Agreement are the property of the Secretary of State and may not be offered or utilized by any other entity in any manner whatsoever, in whole or in part, without the written permission of the Secretary of State or a designee of the Secretary of State.

KSU shall deploy newly purchased property acquired by the Elections Division, only after consultation with the individual within the Elections Division designated by the Elections Division Director for such purpose.

KSU shall require all employees of the Center who have access to the system and system security measures to sign confidentiality agreements, as provided by the Secretary of State.

ARTICLE III. TIME OF PERFORMANCE

6 cert/cat 7 cert/cat

The period of this Agreement shall be from July 1, 2015, through June 30, 2016. Either party may cancel this Agreement upon thirty days written notice to the other party.

ARTICLE IV. COMPENSATION AND PAYMENT

For the satisfactory performance of its duties and obligations set forth herein, KSU shall be compensated for its services for the full year of this Agreement in the amount not to exceed $792,385.00, for the State fiscal year 2017, billable in 12 installments of $66,032.08. Invoices shall be submitted to the Secretary of State on a monthly basis. KSU's services shall include support for such professional services, including secretarial, student assistants, mail and express mail delivery, telephone, computer charges, computer equipment and software, photocopying and other staff expenses as set forth in Appendix "A" attached hereto and incorporated herein by reference KSU's services and obligations under this Agreement shall be completed at or prior to the time of final payment. In the event of cancellation under Article III, no further payments shall be required under this Agreement beyond the end of the month in which the cancellation is executed.

ARTICLE V. RETENTION OF RECORDS

KSU shall keep and maintain as records of the Secretary of State all records and other documents pertaining to the performance of this Agreement until the final payment of funds to

KSU by the Secretary of State pursuant to this Agreement has been completed. At such time, physical custody of the records and documents shall be returned to the Secretary of State.

The University and KSU shall give immediate notice by telephone to the Elections Division Director of the Secretary of State of any open records request made pursuant to O.C.G.A. § 50-18-70 *et seq.*, request for production of documents and things, or subpoena associated with any litigation relating to any computer programs, computer software, equipment, or any other documents, issues or materials relating to the Voting System or any of its components. The University and KSU acknowledge that computer programs and computer software may be exempted from disclosure when meeting the definitions and provisions of O.C.G.A. § 50-18-72(f) and that an open records request may affect State or vendor rights. The University and KSU shall deliver to the Elections Division Director a copy of any written open records request received by the University or KSU promptly by electronic transmission, facsimile or in any event within 24-hours of its receipt of the request. In so far as possible, the University and KSU will allow the Secretary of State prior opportunity to comment on any response to any open records request within this paragraph; however, such review shall be for the convenience of the Secretary of State, without responsibility or liability to the University or KSU.

ARTICLE VI. REPORTING AND AUDITING REQUIREMENTS

KSU shall provide monthly reports to Secretary of State to report the status of the Center's performance under the Agreement and the Center's progress toward fulfilling the requirements of the Agreement. KSU shall, if it has expended $100,000 or more during its fiscal year in State funds, provide for and cause to be made annually an audit of the financial affairs and transactions of all the Center's funds and activities. The audit shall be performed in accordance with generally accepted auditing standards. KSU shall, if it has expended less than $100,000 in a fiscal year in state funds, forward to the State auditor and each contracting State organization a copy of the Center's financial statements. If annual financial statements are reported upon by a public accountant, the accountant's report must accompany them. If not, the annual financial statements must be accompanied by the statement of the president or person responsible for the nonprofit organization's financial statements.

ARTICLE VII. MISCELLANEOUS

The University, KSU, and the Secretary of State further mutually agree as follows:

A. This Agreement constitutes the entire agreement between the parties and any amendments to this Agreement must be in writing.

B. The provisions of O.C.G.A. § 45-10-20. *et seq.* will not be violated by the parties to this agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement, this 16th day of June, 2016.

ON BEHALF OF THE SECRETARY OF STATE OF THE STATE OF GEORGIA:

Signature

Timothy K. Fleming
Print Name

Deputy SOS
Title

Date: 5/15/16

ON BEHALF OF THE BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA AND KENNESAW STATE UNIVERSITY:

Signature

Charles J Ambare
Print Name

Vice President for Research
Title

Date: 6/6/16

Appendix A

Budget, FY 2017
Center for Election Systems, Kennesaw State University

Category	FY 2017 Proposed Budget	
Personnel		
Center Executive Director	$	70,800.00
Director	$	87,800.00
Assistant Director	$	56,500.00
Election Professional II	$	48,500.00
Election Professional II	$	44,900.00
Election Professional II	$	43,300.00
IT Sys Supp Pro II	$	41,200.00
IT Sys Supp Pro I	$	36,500.00
Salaries	$	429,500.00
Fringes	$	128,850.00
Salaries and Fringes	$	558,350.00
Student Assistants	$	33,000.00
Temporary Staff Assistants	$	10,000.00
TOTAL PERSONNEL	**$**	**601,350.00**
OFFICE/LAB SPACE RENT	**$**	**41,000.00**
TRAVEL	**$**	**20,000.00**

TELECOMM	**$**	**12,000.00**
SUPPLIES	**$**	**12,000.00**
COPYING	**$**	**2,000.00**
FREIGHT & SHIPPING	**$**	**20,000.00**
COMPUTERS/SOFTWARE	**$**	**12,000.00**
Indirects (10%)	**$**	**72,035.00**
TOTAL BUDGET	**$**	**792,385.00**

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/17/16

item(s) listed below were:
- ☐ Received From
- ☑ Returned To
- ☐ Released To
- ☐ Seized

(Name) [redacted]

(Street Address) [redacted]

(City) [redacted]

Description of Item(s): [redacted]

Received By: _____ (Signature)

Received From: William D Wiseman II (Signature)

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/3/17

item(s) listed below were:
- ☑ Received From
- ☐ Returned To
- ☐ Released To
- ☐ Seized

(Name) [redacted]

(Street Address) [redacted]

(City) [redacted]

Description of Item(s): 1 Dell [redacted]

Received By: _____ (Signature)

Received From: _____ (Signature)

Evidence Tag

Date	Tag No	Case No:	Location
March 2, 2017		20170302CES	Center for Elections Systems

Public Safety Officer(s) involved ___NA___

Description of Property

Server with DNS name elections.kennesaw.edu with KSU asset tag 103019

Signature of Witness	Signature of Person Received Property

Chain of Custody Receipt

Released by (Print and Sign)	Date	Purpose	Received by (Print and Sign)	Date
Merle King	March 2, 2017	Retrieving server after reported data breach. Server will be retrieved by the FBI by UITS ISO	Stephen Rose	1907 March 2, 2017
William Ware Moore	3/3/2017	←Swap Released & Received by →	Stephen Rose	March 3 2017

From: Mariel Louise Fox
To: Stephen Craig Gay
Cc: Tamara Elena Livingston
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:22:40 PM

Stephen,

Below is the communication thread among Steven Dean, Jeff Milsteen and myself.

I'll await your direction and guidance as to next steps in providing consultation to Steven regarding KSU records, and I will communicate that message to Steven shortly.

Thanks!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Mariel Fox" <mfox32@kennesaw.edu>
Sent: Friday, March 10, 2017 1:38:30 PM
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Steven,

Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From: Mariel Louise Fox
To: Steven Jay Dean
Cc: Stephen Craig Gay
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:27:49 PM

Steven,

I just learned that Stephen Gay will be providing direction and guidance concerning your inquiry about records retention/data storage policies and issues.

I'm sure we'll be working together more closely in the future.

Thanks for bringing up these important issues!

Regards,

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Mariel Fox" <mfox32@kennesaw.edu>
Sent: Friday, March 10, 2017 1:38:30 PM
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Steven,

Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From:	Stephen Craig Gay
To:	Steven Jay Dean; Jason Stephen Figueroa
Cc:	Christopher Michael Dehner; James Christopher Gaddis; Michael L. Barnes
Subject:	Fwd: Plan of action for the passing of data
Date:	Wednesday, March 22, 2017 6:27:33 PM
Importance:	High

Steven and Jason,

Please work with Christopher Dehner on this tomorrow, as this functionality is at the core of securely returning the data to the Secretary of State's Office. Chris will pull in additional ISO staff members as needed and I'll be available if any challenges or questions come up.

Thank you,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Forwarded Message -----
From: "Stephen C Gay" <sgay@kennesaw.edu>
To: mbeaver@sos.ga.gov
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>
Sent: Wednesday, March 22, 2017 6:25:02 PM
Subject: Plan of action for the passing of data

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on

the progress and will be available to assist as needed.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From: Stephen Craig Gay
To: Ware, William D. II (AT) (FBI)
Subject: Fwd: Request for data retrieval
Date: Wednesday, March 15, 2017 1:51:26 PM

Agent Ware,

We received the request below from the Center for Election Systems regarding data contained on the seized server which they do not have a backup of. What is the possibility of having the data extracted and us picking it up?

Thank you for your consideration of this request.
Stephen

----- Forwarded Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From:	Stephen Craig Gay
To:	Christopher Michael Dehner
Cc:	Davide Gaetano
Subject:	Infrastructure projects for CES
Date:	Monday, July 10, 2017 5:48:48 PM

Chris,

Speaking to Davide about the infrastructure surplus recommendations and I would like to divide the project into 2 phases, one focused on the surplus, switches, and APC's mentioned in the AAR; and the 2nd focused on the slightly longer plan to add environmental and log monitoring. If you could please connect with him on these projects, I would sincerely appreciate it and if I can assist in any way please let me know.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From:	Stephen Craig Gay
To:	Ware, William D. II (AT) (FBI)
Subject:	Investigative update
Date:	Monday, March 13, 2017 7:59:09 AM

Agent Ware,

Good Monday morning. I wanted to take a moment to reach out to ask for an update on the status of the investigation. If there is anything at all we can do to assist please let me know.

Thank you,
Stephen

Sent from Nine

March 3, 2017

Election-related files

elections.kennesaw.edu

The voting system and electronic pollbooks used in Georgia require files to be named in compliance with the application's requirements. As a consequence, many of the files will have identical names, but their contents vary by county.

Some of the pollbook related files will only contain voter registration values. These files are used to update the electors list, indicating voters who were issued ballots during advance/early voting. Other pollbook files will contain the state's entire electors list.

The folder names relate to the content contained within the files placed within the folders, back to the county to which they are assigned. We developed a folder for each county (159) and within each folder we placed files generated for that individual county.

Examples of files posted for a county to pull down:

./Appling County/Proof/Audio/Appling Audio.zip – This zip file contains audio files linked within the county's election database. This files are posted so a county can proof whether the candidate's name, ballot information headers, race headers are all present and recorded properly. The file is zipped due to file size.

./Appling County/Proof/Ballot/01 – Appling.zip – This zip file contains ballot proofs for a given election. These files are provided to each county to allow them to confirm that the contents of their ballots are accurate for the given election. The file is zipped due to files size.

./Appling County/Proof/Ballots/Ballot and Audio Proofs Signoff_v2.pdf – This file is provided to every county when proofing audio files and ballot proofs. We require each county to return a signed signoff form to our office after they have completed their proofing. This form allows the completed election database to be released from us to the jurisdiction for use in the given election. "V2" indicates that this is the second version of this form.

./Appling County/ExpressPoll/Numbered_List/001 (11-08-2016).pdf – This file is provided to every county after the completion of the given election. This file contains a list of those voters who participated at their assigned polling location on Election Day in sequential order.

./Appling County/ExpressPoll/ABSFile/PollData.db3 – This is a data file for use within the assigned county on their ExpressPoll units that are used to create voter access cards given to voters during the Advance Voting period. No individual voter data is contained within this file. A file of this nature is created for each county prior to a given election. "ABS" relates to voters casting ballots prior to Election Day.

./Appling County/ExpressPoll/ABSFile/Expoll.resources – This file accompanies the above mention file. The resource file instructs the ExpressPoll device what operations to allow and what buttons to display on screen to the user of the ExpressPoll device.

./Baldwin County/ExpressPoll/ED_Files/November 2016 General Voter Lookup.zip – This file is not built for all counties. This file is only built for those counties who request it from our office. This file contains the elector's list for the county for the given election, but it is not used to create any voter access cards. The file is zipped due to size of the files content.

./Baldwin County/ExpressPoll/ED_Files/November 2016 General Voter Lookup Password Memo.pdf – This file accompanies the above mentioned file. This file contains what the passwords are to access the data contained in the zipped file above when loaded onto an ExpressPoll. These passwords are changed for every election.

./Cherokee County/ExpressPoll/ED_Files/November2016GeneralElectionDay.zip – This is not a file posted for each county. This file is only posted to those counties who produce the storage media loaded into the jurisdictions' ExpressPolls themselves. Counties that do this operation are: Fulton, Cobb, Dekalb, Gwinnett, Forsyth, Chatham, Muscogee, Henry, Columbia, Clayton, and Cherokee. This file contains the full elector's list for the state for a given election.

./Cherokee County/ExpressPoll/ED_Files/November 2016 General Election Day Password Memo.pdf - This file accompanies the above mentioned file. This file contains what the passwords are to access the data contained in the zipped file above when loaded onto an ExpressPoll. These passwords are changed for every election.

./Clayton County/GEMS_DB/****.gbf – This is a file posted to a county only in select circumstances. This is an election database file containing the ballot contents for a given election. These files are accessed by the GEMS application.

./Pickens County/ExpressPoll/ED_Files/ExpReport.exe – File allows a county to produce a numbered list of voters directly from the ExpressPoll media, when installed on the ExpressPoll media.

./Pickens County/ExpressPoll/ED_Files/System.Data.SQLite.DLL – This file allows the file mentioned above to operate on the ExpressPoll. The above file is inoperative without this file.

./Richmond County/GEMS_DB/2. GEMS Instructions.pdf – This is a manual on GEMS operations. Only posted if requested by a county.

./Richmond County/GEMS_DB/GeneralDemo.zip – Only posted if requested by a county. Contains a demonstration election database.

This concludes the types of files placed within the county folders for distribution to counties

Attached is the known county user accounts allowing access to these to county folders. When an account is created, the county recipient is automatically sent (by Drupal) an email that contains a password reset link. Counties create their own passwords for accessing the folders.

Username	Folder	Phone Number
Appling County Elections	Appling County	912-367-8113
Appling County Registrar	Appling County	912-367-8113
Atkinson County Elections	Atkinson County	912-422-3003
Atkinson County Registrar	Atkinson County	912-422-3003
Bacon County Elections	Bacon County	912-632-5551
Bacon County Registrar	Bacon County	912-632-5551
Baker County Elections	Baker County	229-734-3019
Baker County Registrar	Baker County	229-734-3019
Baldwin County Elections	Baldwin County	478-445-4807
Baldwin County Registrar	Baldwin County	478-445-4807
Banks County Elections	Banks County	706-677-6260
Banks County Registrar	Banks County	706-677-6260
Barrow County Elections	Barrow County	770-307-3510
Barrow County Registrar	Barrow County	770-307-3510
Bartow County Elections	Bartow County	770-387-5098
Bartow County Registrar	Bartow County	770-387-5098
Ben Hill County Elections	Ben Hill County	229-426-5151
Ben Hill County Registrar	Ben Hill County	229-426-5151
Berrien County Elections	Berrien County	229-686-5213
Berrien County Registrar	Berrien County	229-686-5213
Bibb County Elections	Bibb County	478-621-6622
Bibb County Registrar	Bibb County	478-621-6622
Bleckley County Elections	Bleckley County	478-934-3204
Bleckley County Registrar	Bleckley County	478-934-3204
Brantley County Elections	Brantley County	912-462-6159
Brantley County Registrar	Brantley County	912-462-6159
Brooks County Elections	Brooks County	229-263-9939
Brooks County Registrar	Brooks County	229-263-9939
Bryan County Elections	Bryan County	912-653-3859
Bryan County Registrar	Bryan County	912-653-3859
Bulloch County Elections	Bulloch County	912-764-6502
Bulloch County Registrar	Bulloch County	912-764-6502
Burke County Elections	Burke County	770-775-8299
Burke County Registrar	Burke County	770-775-8299
Butts County Elections	Butts County	770-775-8299
Butts County Registrar	Butts County	770-775-8299

Calhoun County Elections	Calhoun County	229-849-2115
Calhoun County Registrar	Calhoun County	229-849-2115
Camden County Elections	Camden County	912-576-3785
Camden County Registrar	Camden County	912-576-3785
Candler County Elections	Candler County	912-515-4424
Candler County Registrar	Candler County	912-515-4424
Carroll County Elections	Carroll County	770-830-5824
Carroll County Registrar	Carroll County	770-830-5824
Catoosa County Elections	Catoosa County	706-935-3990
Catoosa County Registrar	Catoosa County	706-935-3990
Charlton County Elections	Charlton County	912-496-2607
Charlton County Registrar	Charlton County	912-496-2607
Chatham County Elections	Chatham County	912-201-4375
Chatham County Registrar	Chatham County	912-201-4375
Chattahoochee County Elections	Chattahoochee County	706-989-3603
Chattahoochee County Registrar	Chattahoochee County	706-989-3603
Chattooga County Elections	Chattooga County	706-857-0709
Chattooga County Registrar	Chattooga County	706-857-0709
Cherokee County Elections	Cherokee County	770-479-0407
Cherokee County Registrar	Cherokee County	770-479-0407
Clarke County Elections	Clarke County	706-613-3150
Clarke County Registrar	Clarke County	706-613-3150
Clay County Elections	Clay County	229-768-2445
Clay County Registrar	Clay County	229-768-2445
Clayton County Elections	Clayton County	770-477-4572
Clayton County Registrar	Clayton County	770-477-4572
Clinch County Elections	Clinch County	912-487-3656
Clinch County Registrar	Clinch County	912-487-3656
Cobb County Elections	Cobb County	770-528-2312
Cobb County Registrar	Cobb County	770-528-2312
Coffee County Elections	Coffee County	912-384-7018
Coffee County Registrar	Coffee County	912-384-7018
Colquitt County Elections	Colquitt County	229-616-7415
Colquitt County Registrar	Colquitt County	229-616-7415
Columbia County Elections	Columbia County	706-868-3355
Columbia County Registrar	Columbia County	706-868-3355
Cook County Elections	Cook County	229-896-7925
Cook County Registrar	Cook County	229-896-7925
Coweta County Elections	Coweta County	678-854-0015

Coweta County Registrar	Coweta County	678-854-0015
Crawford County Elections	Crawford County	478-836-1877
Crawford County Registrar	Crawford County	478-836-1877
Crisp County Elections	Crisp County	229-276-2611
Crisp County Registrar	Crisp County	229-276-2611
Dade County Elections	Dade County	706-657-8170
Dade County Registrar	Dade County	706-657-8170
Dawson County Elections	Dawson County	706-344-3640
Dawson County Registrar	Dawson County	706-344-3640
Decatur County Elections	Decatur County	229-243-2087
Decatur County Registrar	Decatur County	229-243-2087
DeKalb County Elections	DeKalb County	404-298-4020
DeKalb County Registrar	DeKalb County	404-298-4020
Dodge County Elections	Dodge County	478-374-3775
Dodge County Registrar	Dodge County	478-374-3775
Dooly County Elections	Dooly County	229-268-9023
Dooly County Registrar	Dooly County	229-268-9023
Dougherty County Elections	Dougherty County	229-431-3247
Dougherty County Registrar	Dougherty County	229-431-3247
Douglas County Elections	Douglas County	770-920-7412
Douglas County Registrar	Douglas County	770-920-7412
Early County Elections	Early County	229-723-4522
Early County Registrar	Early County	229-723-4522
Echols County Elections	Echols County	229-559-7526
Echols County Registrar	Echols County	229-559-7526
Effingham County Elections	Effingham County	912 754-8030
Effingham County Registrar	Effingham County	912 754-8030
Elbert County Elections	Elbert County	706-283-2016
Elbert County Registrar	Elbert County	706-283-2016
Emanuel County Elections	Emanuel County	478-237-3471
Emanuel County Registrar	Emanuel County	478-237-3471
Evans County Elections	Evans County	912-739-4080
Evans County Registrar	Evans County	912-739-4080
Fannin County Elections	Fannin County	706-632-7740
Fannin County Registrar	Fannin County	706-632-7740
Fayette County Elections	Fayette County	770-305-5138
Fayette County Registrar	Fayette County	770-305-5138
Floyd County Elections	Floyd County	706-291-5167
Floyd County Registrar	Floyd County	706-291-5167
Forsyth County Elections	Forsyth County	770-781-2118
Forsyth County Registrar	Forsyth County	770-781-2118

Franklin County Elections	Franklin County	706-384-4390
Franklin County Registrar	Franklin County	706-384-4390
Fulton County Elections	Fulton County	706-384-4390
Fulton County Registrar	Fulton County	706-384-4390
Gilmer County Elections	Gilmer County	706-635-4763
Gilmer County Registrar	Gilmer County	706-635-4763
Glascock County Elections	Glascock County	706-598-3241
Glascock County Registrar	Glascock County	706-598-3241
Glynn County Elections	Glynn County	912-554-7063
Glynn County Registrar	Glynn County	912-554-7063
Gordon County Elections	Gordon County	706-629-7781
Gordon County Registrar	Gordon County	706-629-7781
Grady County Elections	Grady County	229-377-4621
Grady County Registrar	Grady County	229-377-4621
Greene County Elections	Greene County	706-531-1108
Greene County Registrar	Greene County	706-531-1108
Gwinnett County Elections	Gwinnett County	678-226-7231
Gwinnett County Registrar	Gwinnett County	678-226-7231
Habersham County Elections	Habersham County	706-839-0170
Habersham County Registrar	Habersham County	706-839-0170
Hall County Elections	Hall County	770-531-6945
Hall County Registrar	Hall County	770-531-6945
Hancock County Elections	Hancock County	706-444-5259
Hancock County Registrar	Hancock County	706-444-5259
Haralson County Elections	Haralson County	770-646-2010
Haralson County Registrar	Haralson County	770-646-2010
Harris County Elections	Harris County	706-628-5210
Harris County Registrar	Harris County	706-628-5210
Hart County Elections	Hart County	706-376-8911
Hart County Registrar	Hart County	706-376-8911
Heard County Elections	Heard County	706-675-3353
Heard County Registrar	Heard County	706-675-3353
Henry County Elections	Henry County	770-288-6448
Henry County Registrar	Henry County	770-288-6448
Houston County Elections	Houston County	478-987-1973
Houston County Registrar	Houston County	478-987-1973
Irwin County Elections	Irwin County	229-468-5894
Irwin County Registrar	Irwin County	229-468-5894
Jackson County Elections	Jackson County	706-367-6377
Jackson County Registrar	Jackson County	706-367-6377
Jasper County Elections	Jasper County	706-468-4903

Jasper County Registrar	Jasper County	706-468-4903
Jeff Davis County Elections	Jeff Davis County	912-375-6635
Jeff Davis County Registrar	Jeff Davis County	912-375-6635
Jefferson County Elections	Jefferson County	478-625-8357
Jefferson County Registrar	Jefferson County	478-625-8357
Jenkins County Elections	Jenkins County	478-982-5581
Jenkins County Registrar	Jenkins County	478-982-5581
Johnson County Elections	Johnson County	478-864-4019
Johnson County Registrar	Johnson County	478-864-4019
Jones County Elections	Jones County	478-986-8234
Jones County Registrar	Jones County	478-986-8234
Lamar County Elections	Lamar County	770-358-5235
Lamar County Registrar	Lamar County	770-358-5235
Lanier County Elections	Lanier County	229-482-3668
Lanier County Registrar	Lanier County	229-482-3668
Laurens County Elections	Laurens County	478-272-2566
Laurens County Registrar	Laurens County	478-272-2566
Lee County Elections	Lee County	229-759-6002
Lee County Registrar	Lee County	229-759-6002
Liberty County Elections	Liberty County	912-876-3310
Liberty County Registrar	Liberty County	912-876-3310
Lincoln County Elections	Lincoln County	706-359-6126
Lincoln County Registrar	Lincoln County	706-359-6126
Long County Elections	Long County	912-545-2234
Long County Registrar	Long County	912-545-2234
Lowndes County Elections	Lowndes County	229-671-2850
Lowndes County Registrar	Lowndes County	229-671-2850
Lumpkin County Elections	Lumpkin County	706-864-6279
Lumpkin County Registrar	Lumpkin County	706-864-6279
Macon County Elections	Macon County	478-472-8520
Macon County Registrar	Macon County	478-472-8520
Madison County Elections	Madison County	706-795-6335
Madison County Registrar	Madison County	706-795-6335
Marion County Elections	Marion County	229-649-9838
Marion County Registrar	Marion County	229-649-9838
McDuffie County Elections	McDuffie County	706-595-2105
McDuffie County Registrar	McDuffie County	706-595-2105
McIntosh County Elections	McIntosh County	912-437-6605
McIntosh County Registrar	McIntosh County	912-437-6605
Meriwether County Elections	Meriwether County	706-672-9433
Meriwether County Registrar	Meriwether County	706-672-9433

Miller County Elections	Miller County	229-758-4110
Miller County Registrar	Miller County	229-758-4110
Mitchell County Elections	Mitchell County	229-336-2018
Mitchell County Registrar	Mitchell County	229-336-2018
Monroe County Elections	Monroe County	478-994-7036
Monroe County Registrar	Monroe County	478-994-7036
Montgomery County Elections	Montgomery County	912-583-2681
Montgomery County Registrar	Montgomery County	912-583-2681
Morgan County Elections	Morgan County	706-343-6311
Morgan County Registrar	Morgan County	706-343-6311
Murray County Elections	Murray County	706-517-1400 #7
Murray County Registrar	Murray County	706-517-1400 #7
Muscogee County Elections	Muscogee County	706-653-4392
Muscogee County Registrar	Muscogee County	706-653-4392
Newton County Elections	Newton County	678-625-1692
Newton County Registrar	Newton County	678-625-1692
Oconee County Elections	Oconee County	706-769-3958
Oconee County Registrar	Oconee County	706-769-3958
Oglethorpe County Elections	Oglethorpe County	706-743-5350
Oglethorpe County Registrar	Oglethorpe County	706-743-5350
Paulding County Elections	Paulding County	770-443-7503
Paulding County Registrar	Paulding County	770-443-7503
Peach County Elections	Peach County	478-825-3514
Peach County Registrar	Peach County	478-825-3514
Pickens County Elections	Pickens County	706-253-8781
Pickens County Registrar	Pickens County	706-253-8781
Pierce County Elections	Pierce County	912-449-2028
Pierce County Registrar	Pierce County	912-449-2028
Pike County Elections	Pike County	770-567-8734
Pike County Registrar	Pike County	770-567-8734
Polk County Elections	Polk County	770-749-2103
Polk County Registrar	Polk County	770-749-2103
Pulaski County Elections	Pulaski County	478-783-2061
Pulaski County Registrar	Pulaski County	478-783-2061
Putnam County Elections	Putnam County	706-485-8683
Putnam County Registrar	Putnam County	706-485-8683
Quitman County Elections	Quitman County	229-334-2224
Quitman County Registrar	Quitman County	229-334-2224
Rabun County Elections	Rabun County	706-782-1878
Rabun County Registrar	Rabun County	706-782-1878
Randolph County Elections	Randolph County	855-782-6310 ext 5

Randolph County Registrar	Randolph County	855-782-6310 ext 5
Richmond County Elections	Richmond County	706-821-2340
Richmond County Registrar	Richmond County	706-821-2340
Rockdale County Elections	Rockdale County	770-278-7333
Rockdale County Registrar	Rockdale County	770-278-7333
Schley County Elections	Schley County	229-937-2905
Schley County Registrar	Schley County	229-937-2905
Screven County Elections	Screven County	912-564-2783
Screven County Registrar	Screven County	912-564-2783
Seminole County Elections	Seminole County	229-524-5256
Seminole County Registrar	Seminole County	229-524-5256
Spalding County Elections	Spalding County	770-467-4370
Spalding County Registrar	Spalding County	770-467-4370
Stephens County Elections	Stephens County	706-886-8954
Stephens County Registrar	Stephens County	706-886-8954
Stewart County Elections	Stewart County	229-838-4682 ext 210
Stewart County Registrar	Stewart County	229-838-4682 ext 210
Sumter County Elections	Sumter County	229-928-4580
Sumter County Registrar	Sumter County	229-928-4580
Talbot County Elections	Talbot County	706-665-8270
Talbot County Registrar	Talbot County	706-665-8270
Taliaferro County Elections	Taliaferro County	706-456-2253
Taliaferro County Registrar	Taliaferro County	706-456-2253
Tattnall County Elections	Tattnall County	912-557-6417
Tattnall County Registrar	Tattnall County	912-557-6417
Taylor County Elections	Taylor County	478-862-3997
Taylor County Registrar	Taylor County	478-862-3997
Telfair County Elections	Telfair County	229-868-6038
Telfair County Registrar	Telfair County	229-868-6038
Terrell County Elections	Terrell County	229-995-5066
Terrell County Registrar	Terrell County	229-995-5066
Thomas County Elections	Thomas County	229-225-4101
Thomas County Registrar	Thomas County	229-225-4101
Tift County Elections	Tift County	229-386-7915
Tift County Registrar	Tift County	229-386-7915
Toombs County Elections	Toombs County	912-526-8226
Toombs County Registrar	Toombs County	912-526-8226
Towns County Elections	Towns County	706-896-6920
Towns County Registrar	Towns County	706-896-6920

Treutlen County Elections	Treutlen County	912-529-3342
Treutlen County Registrar	Treutlen County	912-529-3342
Troup County Elections	Troup County	706-883-1745
Troup County Registrar	Troup County	706-883-1745
Turner County Elections	Turner County	229-567-2909
Turner County Registrar	Turner County	229-567-2909
Twiggs County Elections	Twiggs County	478-945-3639
Twiggs County Registrar	Twiggs County	478-945-3639
Union County Elections	Union County	706-439-6041
Union County Registrar	Union County	706-439-6041
Upson County Elections	Upson County	706-647-6259
Upson County Registrar	Upson County	706-647-6259
Walker County Elections	Walker County	706-638-4349
Walker County Registrar	Walker County	706-638-4349
Walton County Elections	Walton County	770-267-1337
Walton County Registrar	Walton County	770-267-1337
Ware County Elections	Ware County	912-287-4363
Ware County Registrar	Ware County	912-287-4363
Warren County Elections	Warren County	706-465-2227
Warren County Registrar	Warren County	706-465-2227
Washington County Elections	Washington County	478-552-3304
Washington County Registrar	Washington County	478-552-3304
Wayne County Elections	Wayne County	912-427-5940
Wayne County Registrar	Wayne County	912-427-5940
Webster County Elections	Webster County	229-828-5775
Webster County Registrar	Webster County	229-828-5775
Wheeler County Elections	Wheeler County	912-568-7133
Wheeler County Registrar	Wheeler County	912-568-7133
White County Elections	White County	706-865-4141
White County Registrar	White County	706-865-4141
Whitfield County Elections	Whitfield County	706-278-7183
Whitfield County Registrar	Whitfield County	706-278-7183
Wilcox County Elections	Wilcox County	229-467-2111
Wilcox County Registrar	Wilcox County	229-467-2111
Wilkes County Elections	Wilkes County	706-678-2523
Wilkes County Registrar	Wilkes County	706-678-2523
Wilkinson County Elections	Wilkinson County	478-946-2188
Wilkinson County Registrar	Wilkinson County	478-946-2188
Worth County Elections	Worth County	229-776-8208
Worth County Registrar	Worth County	229-776-8208

From:	Steven Dean
To:	James Christopher Gaddis
Cc:	William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject:	Next steps for elections.kennesaw.edu
Date:	Thursday, March 2, 2017 1:32:27 PM

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From:	Stephen Craig Gay
To:	mbeaver@sos.ga.gov
Cc:	Lectra Lawhorne; Michael L. Barnes
Subject:	Plan of action for the passing of data
Date:	Wednesday, March 22, 2017 6:25:02 PM

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From: Stephen Craig Gay
To: Steven Jay Dean
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Question regarding private network
Date: Friday, June 23, 2017 7:24:59 AM

Steven,

Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

Thanks,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From: Stephen Craig Gay
To: Michael L. Barnes
Subject: Re: Center for Election Systems Contract FY"17
Date: Tuesday, March 7, 2017 9:32:10 AM

Thanks Michael.

Stephen

Sent from Nine

From: Michael Barnes
Sent: Mar 7, 2017 8:57 AM
To: 'Stephen C. Gay'
Subject: Center for Election Systems Contract FY'17

Stephen,

Here is our current contract with the Secretary of State's office. The content of the contract hasn't really changed since 2012 or so.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Christopher Dehner
To: Davide Gaetano
Cc: Casey Darrow; Stephen Gay; Chris Gaddis
Subject: RE: CES Network Assessment Meeting Notes 6/26
Date: Wednesday, July 19, 2017 1:29:00 PM
Attachments: CES Network surplus milestones.xlsx

Davide,

I think we're ready to make the final push on closing the CES AAR recommendations. All we have left is the imaging and transference of services of the two Dell PowerEdge R630s (both in CES private network data center) and the replacement of the UPSs. Per our conversations, one server is for DC/NAS and the other for Epic. I checked with Steven Dean and both servers not running any services so we can begin as soon as possible without impacting their services. The UPSs were ordered last week and we are waiting on delivery. I've included the project milestones and suggested due dates. If these due dates are not feasible, please provide alternative dates. If you have any questions, please feel free to reach out.

Regards,

Chris

From: Christopher Michael Dehner
Sent: Friday, July 7, 2017 11:16 AM
To: Davide Gaetano <dgaetano@students.kennesaw.edu>
Cc: Casey Darrow <cdarrow@kennesaw.edu>; Stephen Craig Gay <sgay@kennesaw.edu>; James Christopher Gaddis <jgaddis6@kennesaw.edu>
Subject: Fw: CES Network Assessment Meeting Notes 6/26

Davide,

I am reseeding this email because for some reason, it was sent to a dgaetano@students.kennesaw.edu account.

Per your instructions regarding the reimaging and installation of the CES server, we DBAN'd the hard drives and delivered the server to TS023. The server is a Dell PowerEdge R610 (Asset Tag: 103019). When it is ready for racking in the CES private network, please let me know and I'll coordinate with the Steven Dean.

Regards,

Chris

From: Christopher Michael Dehner
Sent: Tuesday, June 27, 2017 5:22 PM
To: Stephen Craig Gay; Nickolaus E Hassis; Jason Stephen Figueroa; Steven Jay Dean; Michael L. Barnes; Davide F Gaetano
Subject: CES Network Assessment Meeting Notes 6/26

CES Network Assessment
6/27/17 4:00PM-5:15PM
Attendees:
Nick Hassis, Stephen Gay, Jason Figuero, Steven Dean, Michael Barns, Davide Gaetano

Notes:

CES – is most secure network at KSU, making it more secure
9/10 AAR items closed - Final item: Private Network Inventory

Goal: Reduce number of devices on private network

IMI Card Duplicators also act as data extractor to private network NAS

Reconciled Windows XP devices not captured by network scan

GEMS services dependent on .NET version found on WinXP

Davide – Can GEMS services be virtualized to work on Win7 or Win10?
Steven – Not certain

Stephen: Can we use local authentication instead of domain controller?
Davide: Put domain controllers on Epic and NA

Cellular dialer to send syslog, environment, arpwatch alerts & GPS updates for time keeping.
New Epic and New NAS servicers will also be domain controllers
Cycle hard drive backups to fireproof safe in Secure Storage

Davide suggestions:
- Physically label computers if on private network
- Add distance between private and public network devices
- Replace wifi access point, create new ssid for only CES
- Arpwatch box for public and private networks to prevent network crossovers
- Put CES behind a firewall – force denial and whitelist

Action Items:

CES IT
- Confirm printer has unnecessary services disabled
- Work with vendor on upgrading Epic to more current version of Windows Server

UITS
- Build new XP image
- Windows 10 build for audio box

- Migrate data from Poweredge 1900 to Server TBD and decommission box
- Spin up new servers
- Collaborate with CES on transferring services to new servers
- Chris: Connect with Jonathan on new APCs
- Chris: Wipe R610 server, deliver to Davide & Casey for install
- Chris Schedule update meetings for CES Network Updates (include Casey, Jonathan, and GJ)

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

From: Christopher Dehner
To: Stephen Gay
Cc: Michael Barnes; Steven Dean; Jason Figueroa
Subject: Re: CES server surplus
Date: Wednesday, August 9, 2017 3:54:39 PM

Stephen,

I'm happy to report that the remaining two servers on the AAR were delivered to ITIM and the hard drives were degaussed three times. Additionally, I followed up with Jonathan on replacing the old UPSs with the new ones.

Regards,

Chris

From: Stephen Gay
Sent: Wednesday, August 9, 2017 11:32 AM
To: Christopher Dehner; Steven Dean; Jason Figueroa
Cc: Michael Barnes; Lectra Lawhorne
Subject: Re: CES server surplus

Chris,

This is fantastic news. Great work to all parties on closing the final recommendation from the incident after action report.

In your service,
Stephen.

Sent from Nine

From: Christopher Dehner
Sent: Aug 9, 2017 11:24 AM
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

From: Stephen Gay
To: Christopher Dehner; Steven Dean; Jason Figueroa
Cc: Michael Barnes; Lectra Lawhorne
Subject: Re: CES server surplus
Date: Wednesday, August 9, 2017 11:32:38 AM

Chris,

This is fantastic news. Great work to all parties on closing the final recommendation from the incident after action report.

In your service,
Stephen.

Sent from Nine

From: Christopher Dehner
Sent: Aug 9, 2017 11:24 AM
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Get Outlook for Android

From: Steven Dean
To: Mariel Louise Fox
Cc: Steven Jay Dean; Stephen Craig Gay
Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
Date: Wednesday, March 15, 2017 4:31:54 PM

Thank you for your time the other day, Mariel, it was very helpful. I look forward to speaking again about this soon.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 15, 2017, at 4:27 PM, Mariel Fox <mfox32@kennesaw.edu> wrote:

> Steven,
>
> I just learned that Stephen Gay will be providing direction and guidance concerning your inquiry about records retention/data storage policies and issues.
>
> I'm sure we'll be working together more closely in the future.
>
> Thanks for bringing up these important issues!
>
> Regards,
>
> Mariel Fox
> Director, Records & Information Management
> Museums, Archives & Rare Books (MARB)
> LB 216 MD 1704
> Direct: 470-578-2225
> Main: 470-578-6289
>
> ----- Forwarded Message -----
> From: "Jeff Milsteen" <jmilstee@kennesaw.edu>
> To: "Steven Dean" <sdean29@kennesaw.edu>
> Cc: "Mariel Fox" <mfox32@kennesaw.edu>
> Sent: Friday, March 10, 2017 1:38:30 PM
> Subject: Re: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus
>
> Steven,
>
> Mariel forwarded your inquiry to me. I believe there are a number of issues here that will require some additional work. For example, some of the data maintained by the Center is, by contract, property of the Secretary of State. That data would be subject to the Secretary of State's records retention policies and presumably

those records should either be returned to the SOS Office or, if appropriate, destroyed at their direction and pursuant to their policies. All other records of the Center would be subject to the retention policies of KSU and Mariel can probably help you with existing retention guidelines. The trick, of course, is to correctly identify and categorize those records.

I was not clear what was being asked with respect to FOIA requests. If the Center receives any open records requests, those should immediately be forwarded to the Legal Division for review. The requests themselves, like all other official records of the university, are subjection to our retention guidelines.

I hope this helps. If you have additional questions, please let me know. Thanks.

Jeff Milsteen
Chief Legal Affairs Officer

----- Original Message -----
From: "Mariel Fox" <mfox32@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>
Sent: Friday, March 10, 2017 9:26:22 AM
Subject: Fwd: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Jeff,

This request (see below) for advice came from Steven Dean (sdean29@kennesaw.edu), IT Systems Support at the Center for Election Systems.

I spoke to him on the phone concerning what types of records to keep and how long to keep them, directing him to the State of Georgia retention schedules on the Georgia Archives website.

As to his question about FOIA requests, I said that for KSU open records requests, those are handled by Legal Affairs. But for the Center's records, I did not know. I told him I would forward this question to you.

Please let me know if you have any questions, of if you have any suggestions on how to handle such inquiries in the future.

Thank you!

Mariel Fox
Director, Records & Information Management
Museums, Archives & Rare Books (MARB)
LB 216 MD 1704
Direct: 470-578-2225
Main: 470-578-6289

----- Forwarded Message -----
From: stevendean@kennesaw.edu
To: "records2go" <records2go@kennesaw.edu>
Sent: Thursday, March 9, 2017 1:58:52 PM
Subject: CONSULTATION REQUEST from Steven Dean, Kennesaw Campus

Date Available for Consultation: No in-person consolation needed.

REQUESTED BY: Steven Dean Phone# 470-578-2120

Campus: Kennesaw
Department: Center for Election Systems
Office Location: House 3205

Advice requested for:
Myself and my supervisor or manager.

Need advice on:
['Which records do we need to keep?', 'How long do we need to keep records?', 'Do we need to keep both hard copy and digitial files?', 'What are our records responsibilities?', 'Topic not listed above. Describe in comments.']

Additional comments:
In writing new policies for data storage for the Center, I'd like to see your written policies for data storage periods as relating to FOIA requests.

Preferred communication method: Email.

From: Ware, William D. II (AT) (FBI)
To: Stephen Craig Gay
Subject: RE: Investigative update
Date: Tuesday, March 14, 2017 9:02:53 AM

Hi Stephen,

Sorry for the late reply. The investigation is moving along. We are reviewing the logs and issuing legal process. The legal process is what will take the longest. It could take from two weeks to a month depending on the Internet Service Provider.

Thanks,
SA Davey Ware
FBI - Atlanta Division
2635 Century Parkway, NE
Suite 400
Atlanta, GA
O: 404-679-6126
C: 404-520-3342
F: 404-679-1417

From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, March 13, 2017 7:59 AM
To: Ware, William D. II (AT) (FBI) <William.Ware@ic.fbi.gov>
Subject: Investigative update

Agent Ware,

Good Monday morning. I wanted to take a moment to reach out to ask for an update on the status of the investigation. If there is anything at all we can do to assist please let me know.

Thank you,
Stephen

Sent from Nine

From: Koonce, Steven
To: Christopher Michael Dehner
Cc: Oliver, James; Stephen Craig Gay; Steven Jay Dean; Jason Stephen Figueroa; James Christopher Gaddis
Subject: RE: KSU Account Creation and SFTP Key Management
Date: Friday, March 24, 2017 11:47:05 AM

Our current FTP server uses FTPS (also known as FTP with SSL). Whether we remain on the existing server or stand up a new server, the FTP accounts we are setting up will use a secure protocol, most likely FTPS.

-----Original Message-----
From: Christopher M. Dehner [mailto:cmd9090@kennesaw.edu]
Sent: Friday, March 24, 2017 11:42 AM
To: Koonce, Steven <skoonce@sos.ga.gov>
Cc: Oliver, James <Joliver@sos.ga.gov>; sgay <sgay@kennesaw.edu>; Steven Dean <sdean29@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; jgaddis6 <jgaddis6@kennesaw.edu>
Subject: Re: KSU Account Creation and SFTP Key Management

Steven,

Just a quick point of clarification, when referring to FTP in your email, are you including SFTP or FTPS in your conversations? Per USG Policy and information security best practices, KSU don't allow straight FTP transfers. External file transfers are managed through SFTP or FTPS. Can you confirm that we'll be using SFTP or FTPS to manage these transfers.

Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Koonce, Steven" <skoonce@sos.ga.gov>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "Oliver, James" <Joliver@sos.ga.gov>, "sgay" <sgay@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "jgaddis6" <jgaddis6@kennesaw.edu>
Sent: Friday, March 24, 2017 11:33:01 AM
Subject: RE: KSU Account Creation and SFTP Key Management

We are having an Internal IT meeting Monday to review governance of our FTP site and to decide if a separate FTP server will be used for Elections processes.

I am going to work on the accounts below this afternoon so that they will be ready to go on Monday provided we have no significant changes in our FTP Infrastructure.

-----Original Message-----
From: Christopher M. Dehner [mailto:cmd9090@kennesaw.edu]
Sent: Friday, March 24, 2017 11:23 AM

To: Koonce, Steven <skoonce@sos.ga.gov>
Cc: Oliver, James <Joliver@sos.ga.gov>; Stephen C. Gay <sgay@kennesaw.edu>; Steven Dean <sdean29@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>
Subject: KSU Account Creation and SFTP Key Management

Steven,

My name is Christopher Dehner and I work in the KSU Information Security Office. I've been tasked to cooridnate with you on creating accounts for KSU Center for Elections Systems technicians in the Secretary of State's SFTP server. We would like the following users added:

Steven Dean
Jason Figueroa
Christopher Dehner

I would like to have my account disabled but still in the system. This will allow us to reactivate the account if my support is needed. Additionally, are you able to accommodate specific password requirements (length, special characters, annual expiration, etc.). If at all possible, we would like to align it with our institutional practices. If not, we can discuss this further.

After the accounts are provisioned but before any data transfers, we would like to validate the SFTP encryption key. Based on our understanding, we'll need to make a connection and have you provide the key which we can validate against the SFTP client. This would probably be best done over the phone. If you have an alternative method of key validation, we'll be happy to discuss.

We're looking forward to patterning with your office in building secures processes for data transfers. If you have any additional questions, comments, or concerns, please feel free to reach out.

Warmest Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

From: Christopher Michael Dehner
To: Casey Darrow
Cc: Stephen Craig Gay; Chase Alexander Elliott; Freddie Lewis
Subject: Re: New server and share
Date: Tuesday, March 21, 2017 3:09:44 PM

Casey,

We would like this only accessible on-campus from the following subnet:

10.62.44.0/24 (House 57)

Additionally, we would like all off-campus traffic prohibited. If you need anything else, just let me know.

Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Casey Darrow" <cdarrow@kennesaw.edu>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "sgay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:44:04 PM
Subject: Re: New server and share

Thanks!

Casey Darrow
Director of Windows Server and Infrastructure
University Information Technology Services
Kennesaw State University
Phone 470-578-2634

From: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
To: "cdarrow" <cdarrow@kennesaw.edu>
Cc: "Stephen C Gay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:43:28 PM
Subject: Re: New server and share

Casey,

I'll co-ordinate with CFES technicians, let me gather that information and get back to you.

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Casey Darrow" <cdarrow@kennesaw.edu>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "sgay" <sgay@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "Freddie Lewis" <flewis15@kennesaw.edu>
Sent: Tuesday, March 21, 2017 2:37:47 PM
Subject: Re: New server and share

Chris,

Can you get us the firewall rules we that are needed? We just need to know what exact IP or what subnets need to access this fileshare. Or should we work directly with Steven Dean on this?

Thanks,
Casey

Casey Darrow
Director of Windows Server and Infrastructure
University Information Technology Services
Kennesaw State University
Phone 470-578-2634

From: "Stephen C Gay" <sgay@kennesaw.edu>
To: "Steven Dean" <stevendean@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Christopher M. Dehner" <cmd9090@kennesaw.edu>, "Chase Elliott" <celliot7@kennesaw.edu>, "cdarrow" <cdarrow@kennesaw.edu>
Sent: Tuesday, March 21, 2017 11:14:06 AM
Subject: Re: New server and share

Steven,

I would like for us to have all safeguards in place before CES begins using the server in a production sense. Chris Dehner is CC'd on this email and, by copy, I'll ask him to coordinate between the WinServ team and CES on making this a priority

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University

Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Elliott Chase" <celliot7@kennesaw.edu>, "Casey Darrow" <cdarrow@kennesaw.edu>
Sent: Tuesday, March 21, 2017 11:04:04 AM
Subject: Re: New server and share

Stephen, thank you. Can we begin using this share today to host our project tracker and inventory lists? Or do we need to wait for the firewall changes?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Mar 21, 2017, at 7:44 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven and Jason,
>
> The WinServ team has provisioned a new server dedicated to CES and created a file share which is locked down to the list of users in the center. The path to the share is
>
> \\FS-ES.kennesaw.edu\shared
>
> As we discussed on Friday, I'd like to use a host-based firewall on the server to only allow traffic from the CES network and the UITS network (for management). As I get more information I'll pass along.
>
> Stephen

From: Beaver, Merritt
To: Stephen Craig Gay; Koonce, Steven; Oliver, James
Cc: Lectra Lawhorne; Michael L. Barnes
Subject: RE: Plan of action for the passing of data
Date: Thursday, March 23, 2017 10:24:00 AM

Stephen

I would like to tie in both Steven Koonce, one of our Network administrators and James Oliver, our security manager. See their emails attached.

I talked with my team and our election's team and we would like to just create a new set of SFTP folders for this effort. The old folder was set up the exchange sample ballot forms and we would like to not repurpose that folder for this new use. There will be a need for KSU to upload files to SOS and also for SOS to send files to KSU. We are suggesting that we have two folders to serve each of these purposes. Both of these folders will only hold data for 30 days and after that time any files left will be automatically deleted as these will be transfer folders only.

I will let Steven and James work with your team to best set this environment up.

Thanks

Merritt

S. Merritt Beaver
Chief Information Officer
Office of Georgia Secretary of State Brian P. Kemp
Office (404) 656-7744 Mobile: (770)330-0016
mbeaver@sos.ga.gov

-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Wednesday, March 22, 2017 6:25 PM
To: Beaver, Merritt <mbeaver@sos.ga.gov>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Subject: Plan of action for the passing of data

Merritt,

Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:

Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.

Tasks:
- Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
- Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
- Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
- Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
- Test the clients and processes, and resolve any challenges.

If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From: Michael L. Barnes
To: Stephen Craig Gay
Subject: Re: Plan of action for the passing of data
Date: Wednesday, March 22, 2017 6:26:57 PM

Thank you jumping on this quickly.

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 22, 2017, at 6:25 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

> Merritt,
>
> Thank you for the conversation regarding the ExpressPoll file pickup and discussion on getting the processed data back to your office. Looking over my notes, I have the following plan of action from our discussion:
>
> Objective: KSU will use the Secretary of State SFTP server to upload the data moving forward, after which members of your team will coordinate the distribution to the counties which require the data.
>
> Tasks:
> - Remove all users/rights with the current KSU folder on the Secretary of State SFTP Server and provision new accounts for specified users (Likely SDean, MFiguero, CDehner)
> - Work with Chris Dehner, in the UITS Information Security Office, to share and validate SFTP certificate for server.
> - Work with Chris Dehner and members of CES to develop process for file transfer, account password expiration, and archiving of file and associated password sharing
> - Chris Dehner will work with Steven and Jason on selecting the archive software client, SFTP client and validating the functionality
> - Test the clients and processes, and resolve any challenges.
>
> If you could send me the contact information for James and Stephen on your team I will share with the team and ask that they connect 1st thing tomorrow. I don't want to be a roadblock to these tasks and progress, but will check-in on the progress and will be available to assist as needed.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University

Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

From: Michael L. Barnes
To: Christopher Michael Dehner
Cc: Steven Jay Dean; Stephen Craig Gay
Subject: Re: Question
Date: Wednesday, March 29, 2017 12:10:55 PM

Will do.

Thank you.

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 29, 2017, at 12:10 PM, Christopher M. Dehner <cmd9090@kennesaw.edu> wrote:

> Michael,
>
> From a security perspective we don't have an issue with sending a sample ballot via email, as it contains no confidential data. I would advise to double check with the SoS investigator that this is their preferred method of transmission. As we continue to collaborate with the SoS IT department, we can standardize and document these processes.
>
> Regards,
>
> ---
> Christopher Dehner, CISA
> IT Security Professional III
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 027
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: 470-578-6620
> Fax: 470-578-9050
> cmd9090@kennesaw.edu
>
> ----- Original Message -----
> From: "Michael Barnes" <mbarne28@kennesaw.edu>
> To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
> Cc: "Steven Dean" <sdean29@kennesaw.edu>
> Sent: Wednesday, March 29, 2017 11:12:29 AM
> Subject: Question

Chris,

We received a request from a Secretary of State investigator this morning for a sample ballot from 2016. We have the means to produce the sample ballot the investigator is wishing to review and make part of his investigation. In the past, we would simply email the PDF.

Going forward, how should we forward this information to the Secretary of State's investigative staff when these requests arise?

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Steven Jay Dean
To: Stephen Craig Gay
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Tuesday, June 27, 2017 3:24:52 PM
Attachments: CES Private Network 2017-06-27.xlsx

Stephen, I've attached a spreadsheet with a few changes.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 27, 2017, at 3:04 PM, Steven Dean <sdean29@kennesaw.edu> wrote:
>
> Working on it now. I'll send you a copy before the meeting.
>
> Steven Dean
> Technical Coordinator
> KSU Center for Election Systems
> 3205 Campus Loop Road
> Kennesaw, GA 30144
> P: 470-578-6900 F: 470-578-9012
>
> On Jun 27, 2017, at 2:56 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> > Steven,
> >
> > Do you have a updated/completed version for our 4pm meeting today?
> >
> > Stephen C Gay CISSP CISA
> > KSU Chief Information Security Officer & UITS Executive Director
> > Information Security Office
> > University Information Technology Services (UITS)
> > Kennesaw State University
> > Technology Services Bldg, Room 031
> > 1075 Canton Pl, MB #3503
> > Kennesaw, GA 30144
> > Phone: (470) 578-6620
> > Fax: (470) 578-9050
> > sgay@kennesaw.edu
> >
> > ----- Original Message -----
> > From: "Steven Dean" <sdean29@kennesaw.edu>

To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 9:42:35 AM
Subject: Re: Question regarding private network

We'll take a look and send back any necessary changes.

To your previous email: Yes, we should be able to update everything except the Windows XP workstations and the duplicators.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 9:38 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.
>
> Thank you,
>
> Stephen C Gay CISSP CISA
>
> KSU Chief Information Security Officer & UITS Executive Director
>
> Information Security Office
>
> University Information Technology Services (UITS)
>
> Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

----- Original Message -----

From: "Stephen C Gay" <sgay@kennesaw.edu>

To: "Steven Dean" <sdean29@kennesaw.edu>

Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>

Sent: Friday, June 23, 2017 8:48:20 AM

Subject: Re: Question regarding private network

Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA

KSU Chief Information Security Officer & UITS Executive Director

Information Security Office

University Information Technology Services (UITS)

Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

----- Original Message -----

From: "Steven Dean" <sdean29@kennesaw.edu>

To: "Stephen C Gay" <sgay@kennesaw.edu>

Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>

Sent: Friday, June 23, 2017 8:12:07 AM

Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean

Technical Coordinator

KSU Center for Election Systems

3205 Campus Loop Road

Kennesaw, GA 30144

P: 470-578-6900 F: 470-578-9012

On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

Steven,

Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

Thanks,

Stephen C Gay CISSP CISA

KSU Chief Information Security Officer &
UITS Executive Director

Information Security Office

University Information Technology Services
(UITS)

Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

<CES Private Network.xlsx>

From: Steven Jay Dean
To: Stephen Craig Gay
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Tuesday, June 27, 2017 3:04:56 PM

Working on it now. I'll send you a copy before the meeting.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Jun 27, 2017, at 2:56 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

> Steven,
>
> Do you have a updated/completed version for our 4pm meeting today?
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Original Message -----
> From: "Steven Dean" <sdean29@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
> Sent: Friday, June 23, 2017 9:42:35 AM
> Subject: Re: Question regarding private network
>
> We'll take a look and send back any necessary changes.
>
> To your previous email: Yes, we should be able to update everything except the Windows XP workstations and the duplicators.
>
> Steven Dean
> Technical Coordinator
> KSU Center for Election Systems
> 3205 Campus Loop Road

Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Jun 23, 2017, at 9:38 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

Steven,

Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.

Thank you,

Stephen C Gay CISSP CISA

KSU Chief Information Security Officer & UITS Executive Director

Information Security Office

University Information Technology Services (UITS)

Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

----- Original Message -----

From: "Stephen C Gay" <sgay@kennesaw.edu>

To: "Steven Dean" <sdean29@kennesaw.edu>

Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>

Sent: Friday, June 23, 2017 8:48:20 AM

Subject: Re: Question regarding private network

Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA

KSU Chief Information Security Officer & UITS Executive Director

Information Security Office

University Information Technology Services (UITS)

Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

----- Original Message -----

From: "Steven Dean" <sdean29@kennesaw.edu>

To: "Stephen C Gay" <sgay@kennesaw.edu>

Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>

Sent: Friday, June 23, 2017 8:12:07 AM

Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean

Technical Coordinator

KSU Center for Election Systems

3205 Campus Loop Road

Kennesaw, GA 30144

P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES

private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

Thanks,

Stephen C Gay CISSP CISA

KSU Chief Information Security Officer & UITS Executive Director

Information Security Office

University Information Technology Services (UITS)

Kennesaw State University

Technology Services Bldg, Room 031

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: (470) 578-6620

Fax: (470) 578-9050

sgay@kennesaw.edu

<CES Private Network.xlsx>

From: Stephen Craig Gay
To: Steven Jay Dean
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Tuesday, June 27, 2017 2:56:55 PM

Steven,

Do you have a updated/completed version for our 4pm meeting today?

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <sdean29@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 9:42:35 AM
Subject: Re: Question regarding private network

We'll take a look and send back any necessary changes.

To your previous email: Yes, we should be able to update everything except the Windows XP workstations and the duplicators.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 9:38 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.
>
> Thank you,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)

> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Original Message -----
> From: "Stephen C Gay" <sgay@kennesaw.edu>
> To: "Steven Dean" <sdean29@kennesaw.edu>
> Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
> Sent: Friday, June 23, 2017 8:48:20 AM
> Subject: Re: Question regarding private network
>
> Steven,
>
> Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Original Message -----
> From: "Steven Dean" <sdean29@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
> Sent: Friday, June 23, 2017 8:12:07 AM
> Subject: Re: Question regarding private network
>
> Stephen,
>
> Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.
>
> Steven Dean
> Technical Coordinator
> KSU Center for Election Systems
> 3205 Campus Loop Road
> Kennesaw, GA 30144
> P: 470-578-6900 F: 470-578-9012
>

>> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>>
>> Steven,
>>
>> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?
>>
>> Thanks,
>>
>> Stephen C Gay CISSP CISA
>> KSU Chief Information Security Officer & UITS Executive Director
>> Information Security Office
>> University Information Technology Services (UITS)
>> Kennesaw State University
>> Technology Services Bldg, Room 031
>> 1075 Canton Pl, MB #3503
>> Kennesaw, GA 30144
>> Phone: (470) 578-6620
>> Fax: (470) 578-9050
>> sgay@kennesaw.edu
> <CES Private Network.xlsx>

From: Michael L. Barnes
To: Steven Jay Dean
Cc: Stephen Craig Gay; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Friday, June 23, 2017 9:45:11 AM

We will need to discuss if we can update our box running EPIC. If an update is done affecting the SQL server configurations it could result in EPIC not functioning.

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Jun 23, 2017, at 8:42 AM, Steven Dean <sdean29@kennesaw.edu> wrote:

> We'll take a look and send back any necessary changes.
>
> To your previous email: Yes, we should be able to update everything except the Windows XP workstations and the duplicators.
>
> Steven Dean
> Technical Coordinator
> KSU Center for Election Systems
> 3205 Campus Loop Road
> Kennesaw, GA 30144
> P: 470-578-6900 F: 470-578-9012
>
> On Jun 23, 2017, at 9:38 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.
>
> Thank you,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University

Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Stephen C Gay" <sgay@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:48:20 AM
Subject: Re: Question regarding private network

Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <sdean29@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:12:07 AM
Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will

run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?
>
> Thanks,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

<CES Private Network.xlsx>

From: Steven Jay Dean
To: Stephen Craig Gay
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Friday, June 23, 2017 9:42:47 AM

We'll take a look and send back any necessary changes.

To your previous email: Yes, we should be able to update everything except the Windows XP workstations and the duplicators.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 9:38 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.
>
> Thank you,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Original Message -----
> From: "Stephen C Gay" <sgay@kennesaw.edu>
> To: "Steven Dean" <sdean29@kennesaw.edu>
> Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
> Sent: Friday, June 23, 2017 8:48:20 AM
> Subject: Re: Question regarding private network
>
> Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <sdean29@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:12:07 AM
Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,

Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

Thanks,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

<CES Private Network.xlsx>

From:	Stephen Craig Gay
To:	Steven Jay Dean
Cc:	Michael L. Barnes; Christopher Michael Dehner
Subject:	Re: Question regarding private network
Date:	Friday, June 23, 2017 9:38:57 AM
Attachments:	CES Private Network.xlsx

Steven,

Following up on this, we need to develop a comprehensive inventory of all assets on the CES private network. I have attached my first attempt. Can you and/or Jason review and supplement information as needed and get back to me today. We will use this as the "punch-list" for next week's infrastructure conversation.

Thank you,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Stephen C Gay" <sgay@kennesaw.edu>
To: "Steven Dean" <sdean29@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:48:20 AM
Subject: Re: Question regarding private network

Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <sdean29@kennesaw.edu>

To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:12:07 AM
Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?
>
> Thanks,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

From: Stephen Craig Gay
To: Steven Jay Dean
Cc: Michael L. Barnes; Christopher Michael Dehner
Subject: Re: Question regarding private network
Date: Friday, June 23, 2017 8:48:20 AM

Steven,

Thanks for the quick response. Just so I'm understanding, it sounds like we could update everything except the Windows XP workstations and the card duplicators in partnership with the Secretary of State's Office? I know that we would need to do any migrations in a logical manner which includes testing and the ability to roll-back, and all of this is going to have to be isolated in the same manner the current network is configured.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <sdean29@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>
Sent: Friday, June 23, 2017 8:12:07 AM
Subject: Re: Question regarding private network

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in

this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?

>

> Thanks,

>

> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

From:	Steven Jay Dean
To:	Stephen Craig Gay
Cc:	Michael L. Barnes; Christopher Michael Dehner
Subject:	Re: Question regarding private network
Date:	Friday, June 23, 2017 8:12:15 AM

Stephen,

Everything in the server closet can in theory be updated to the latest version of Windows. The only exception may be the Epic server, which will need testing and verification that the Epic application will run successfully on the latest version. The workstations outside the closet must stay on Windows XP because of ballot building. The duplicators could also in theory be updated, but they are running Suse Linux and I don't know for sure that the duplication software will run on a newer kernel. I believe in the past we had sent them in to IMI for updating since the hardware and software are proprietary.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Jun 23, 2017, at 7:24 AM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Steven,
>
> Quick question: In preparation for next week's infrastructure meeting regarding the devices on the CES private network, I was curious how many of these devices allow for us to update or modify them? For example, the 16 Card Duplicators are likely dictated by the Secretary of State's Office and I would assume that there are other devices in this same scenario (GEMS server), but which devices could allow us to install local firewalls or run the latest version of operating software (Windows file server perhaps)?
>
> Thanks,
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

From: Christopher Michael Dehner
To: Michael L. Barnes
Cc: Steven Jay Dean; Stephen Craig Gay
Subject: Re: Question
Date: Wednesday, March 29, 2017 12:10:11 PM

Michael,

From a security perspective we don't have an issue with sending a sample ballot via email, as it contains no confidential data. I would advise to double check with the SoS investigator that this is their preferred method of transmission. As we continue to collaborate with the SoS IT department, we can standardize and document these processes.

Regards,

Christopher Dehner, CISA
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 027
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: 470-578-6620
Fax: 470-578-9050
cmd9090@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>
Sent: Wednesday, March 29, 2017 11:12:29 AM
Subject: Question

Chris,

We received a request from a Secretary of State investigator this morning for a sample ballot from 2016. We have the means to produce the sample ballot the investigator is wishing to review and make part of his investigation. In the past, we would simply email the PDF.

Going forward, how should we forward this information to the Secretary of State's investigative staff when these requests arise?

Michael Barnes
Director

Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Michael L. Barnes
To: Stephen Craig Gay
Cc: Steven Jay Dean; Merle Steven King; Lectra Lawhorne
Subject: RE: Request for data retrieval
Date: Friday, March 17, 2017 9:10:57 AM

Stephen,

Thank you. Steven and Jason will be available first thing Monday to assist.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Friday, March 17, 2017 9:09 AM
To: Michael Barnes <mbarne28@kennesaw.edu>
Cc: Steven Dean <sdean29@kennesaw.edu>; Merle King <mking@kennesaw.edu>;
Lectra Lawhorne <llawhorn@kennesaw.edu>
Subject: Re: Request for data retrieval

Michael,

I have contacted the Federal investigators and they have agreed to return the server. I will be meeting with them late this afternoon to receive it and then secure it within ISO Secure Storage. I have asked the team to make this a top priority and to work with Steven and Jason on the request data retrieval 1st thing on Monday.

Please let me know if you have any questions or if I can assist further in any way, Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Ware, William D. II (AT) (FBI)
To: Stephen Craig Gay
Subject: RE: Request for data retrieval
Date: Thursday, March 16, 2017 7:44:15 PM

How about a little after 4 pm?

--

-------- Original message --------
From: "Stephen C. Gay" <sgay@kennesaw.edu>
Date: 03/16/2017 3:15 PM (GMT-05:00)
To: "Ware, William D. II (AT) (FBI)" <William.Ware@ic.fbi.gov>
Subject: Re: Request for data retrieval

Agent Ware,

Thank you for the response. I'm open 12:30pm - 1:30pm, 2:30pm - 3:00pm, and after 4pm if any of those work for you?

Stephen
----- Original Message -----
From: "Ware, William D. II (AT) (FBI)" <William.Ware@ic.fbi.gov>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Thursday, March 16, 2017 12:00:13 PM
Subject: RE: Request for data retrieval

Hi Stephen,

We have a forensic image of the server so we can just give you the server back so you guys can do what you want. Are you around tomorrow so I can bring it back?

Davey

--

-------- Original message --------
From: "Stephen C. Gay" <sgay@kennesaw.edu>
Date: 03/15/2017 1:51 PM (GMT-05:00)
To: "Ware, William D. II (AT) (FBI)" <William.Ware@ic.fbi.gov>
Subject: Fwd: Request for data retrieval

Agent Ware,

We received the request below from the Center for Election Systems regarding data contained on the seized server which they do not have a backup of. What is the possibility of having the data extracted and us picking it up?

Thank you for your consideration of this request.
Stephen

----- Forwarded Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Ware, William D. II (AT) (FBI)
To: Stephen Craig Gay
Subject: RE: Request for data retrieval
Date: Thursday, March 16, 2017 12:00:23 PM

Hi Stephen,

We have a forensic image of the server so we can just give you the server back so you guys can do what you want. Are you around tomorrow so I can bring it back?

Davey

--

-------- Original message --------
From: "Stephen C. Gay" <sgay@kennesaw.edu>
Date: 03/15/2017 1:51 PM (GMT-05:00)
To: "Ware, William D. II (AT) (FBI)" <William.Ware@ic.fbi.gov>
Subject: Fwd: Request for data retrieval

Agent Ware,

We received the request below from the Center for Election Systems regarding data contained on the seized server which they do not have a backup of. What is the possibility of having the data extracted and us picking it up?

Thank you for your consideration of this request.
Stephen

----- Forwarded Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Stephen Craig Gay
To: Michael L. Barnes
Cc: Steven Jay Dean; Merle Steven King; Lectra Lawhorne
Subject: Re: Request for data retrieval
Date: Wednesday, March 15, 2017 1:49:53 PM

Michael,

Thank you. Let me pass along to the Federal Investigators and I'll let you know what response I get.

Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Jeff Milsteen
To: Stephen Craig Gay
Cc: Andrew Newton; Lectra Lawhorne
Subject: Re: Scanned documents for review
Date: Monday, March 6, 2017 8:59:32 AM

Thanks, Stephen. I have no objection to releasing the attached documents to Agent Ware.

Jeff

----- Original Message -----
From: "Stephen C. Gay" <sgay@kennesaw.edu>
To: "Jeff Milsteen" <jmilstee@kennesaw.edu>, "Andrew Newton" <anewto19@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>
Sent: Monday, March 6, 2017 8:54:11 AM
Subject: Scanned documents for review

Jeff & Andrew,

We have received the attached documents from the CES regarding the folder structure of the Drupal system and the user accounts for each county. Following up on Friday's conversation, we wanted to run these by you for review and approval before I connected with Agent Ware to pass them along.

Please let me know if we can proceed and thank you.

Stephen

From: Steven Jay Dean
To: Christopher Michael Dehner
Cc: Jason Stephen Figueroa; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject: Re: Secure Fileshare ready for use
Date: Friday, March 24, 2017 10:50:37 AM

Will do. Thank you.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 24, 2017, at 10:44 AM, Christopher M. Dehner <cmd9090@kennesaw.edu> wrote:

> Steven,
>
> We can create a domain bound generic account within active directory that can be used by CFES staff on a shared system. This will allow annual password expiration and alignment with University pass word polices and procedures. I would hold on mounting the share until we get a new account in place.
>
> Regards,
>
> ---
> Christopher Dehner, CISA
> IT Security Professional III
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 027
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: 470-578-6620
> Fax: 470-578-9050
> cmd9090@kennesaw.edu
>
> ----- Original Message -----
> From: "Steven Dean" <sdean29@kennesaw.edu>
> To: "Christopher M. Dehner" <cmd9090@kennesaw.edu>
> Cc: "Jason Figueroa" <jfigue12@kennesaw.edu>, "sgay" <sgay@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
> Sent: Friday, March 24, 2017 10:17:21 AM
> Subject: Re: Secure Fileshare ready for use
>
> This workstation does not have unique logins. It's only used for accessing the database tracker.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 24, 2017, at 10:16 AM, Christopher M. Dehner <cmd9090@kennesaw.edu> wrote:

Steven,

Does this computer require a unique log in or does it use a shared account?

Regards,

Christopher Dehner, CISA

IT Security Professional III

Information Security Office

University Information Technology Services (UITS)

Kennesaw State University

Technology Services Bldg, Room 027

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: 470-578-6620

Fax: 470-578-9050

cmd9090@kennesaw.edu <mailto:cmd9090@kennesaw.edu>

----- Original Message -----

From: "Steven Dean" <sdean29@kennesaw.edu <mailto:sdean29@kennesaw.edu>>

To: "Christopher M. Dehner" <cmd9090@kennesaw.edu <mailto:cmd9090@kennesaw.edu>>

Cc: "Jason Figueroa" <jfigue12@kennesaw.edu <mailto:jfigue12@kennesaw.edu>>, "sgay" <sgay@kennesaw.edu <mailto:sgay@kennesaw.edu>>, "Michael Barnes" <mbarne28@kennesaw.edu <mailto:mbarne28@kennesaw.edu>>, "Merle S. King" <mking@kennesaw.edu <mailto:mking@kennesaw.edu>>

Sent: Friday, March 24, 2017 10:13:50 AM

Subject: Re: Secure Fileshare ready for use

Chris, we have the shared location set up on some of our workstations here and it's working very well. I have one question about user access: We have a shared workstation in the hallway that everyone in the office uses to access the election database tracker from this shared drive. I haven't mounted it yet on this workstation, and I'm curious how you'd like to handle user access for that.

Steven Dean

Technical Coordinator

KSU Center for Election Systems

3205 Campus Loop Road

Kennesaw, GA 30144

P: 470-578-6900 F: 470-578-9012

> On Mar 24, 2017, at 8:36 AM, Steven Dean <sdean29@kennesaw.edu> wrote:
>
> Fantastic. Thank you! We'll begin loading data and I'll let you know if we have any issues or questions.

Steven Dean

Technical Coordinator

KSU Center for Election Systems

3205 Campus Loop Road

Kennesaw, GA 30144

P: 470-578-6900 F: 470-578-9012

> On Mar 24, 2017, at 8:31 AM, Christopher M. Dehner <cmd9090@kennesaw.edu <mailto:cmd9090@kennesaw.edu> <mailto:cmd9090@kennesaw.edu <mailto:cmd9090@kennesaw.edu>>> wrote:
>
> Steven,
>
> The file share FS-ES.kennesaw.edu <http://fs-es.kennesaw.edu/> <http://fs-es.kennesaw.edu/ <http://fs-es.kennesaw.edu/>> is full provisioned, validated, and ready for use. If you guys have any additional questions, please feel free to reach out.
>
> Regards,

Christopher Dehner, CISA

IT Security Professional III

Information Security Office

University Information Technology Services

(UITS)

Kennesaw State University

Technology Services Bldg, Room 027

1075 Canton Pl, MB #3503

Kennesaw, GA 30144

Phone: 470-578-6620

Fax: 470-578-9050

cmd9090@kennesaw.edu
<mailto:cmd9090@kennesaw.edu>
<mailto:cmd9090@kennesaw.edu
<mailto:cmd9090@kennesaw.edu>>

From: Michael L. Barnes
To: Stephen Craig Gay
Cc: Steven Jay Dean; Merle Steven King
Subject: Request for data retrieval
Date: Wednesday, March 15, 2017 1:41:26 PM

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the *cesuser* user directory at /home/cesuser. We would like to retrieve the entire *cesuser* directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From:	Stephen Craig Gay
To:	Jeff Milsteen; Andrew Newton
Cc:	Lectra Lawhorne
Subject:	Scanned documents for review
Date:	Monday, March 6, 2017 8:54:11 AM
Attachments:	Mar03_0258_v1.pdf

Jeff & Andrew,

We have received the attached documents from the CES regarding the folder structure of the Drupal system and the user accounts for each county. Following up on Friday's conversation, we wanted to run these by you for review and approval before I connected with Agent Ware to pass them along.

Please let me know if we can proceed and thank you.

Stephen

From: Michael L. Barnes
To: Stephen Craig Gay
Subject: When you have a moment...
Date: Wednesday, March 22, 2017 4:02:36 PM

Stephen,

When you have a moment can you give me a call at the Center. I need to get you in touch with the Secretary of State's CIO so you can discuss how we may be able to forward materials to them that then need to be disseminated to the counties.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: **Christopher Dehner** cmd9090@kennesaw.edu
Subject: Re: CES server surplus
Date: August 9, 2017 at 3:54 PM
To: Stephen Gay sgay@kennesaw.edu
Cc: Michael Barnes mbarne28@kennesaw.edu, Steven Dean sdean29@kennesaw.edu, Jason Figueroa jfigue12@kennesaw.edu

Stephen,

I'm happy to report that the remaining two servers on the AAR were delivered to ITIM and the hard drives were degaussed three times. Additionally, I followed up with Jonathan on replacing the old UPSs with the new ones.

Regards,

Chris

From: Stephen Gay
Sent: Wednesday, August 9, 2017 11:32 AM
To: Christopher Dehner; Steven Dean; Jason Figueroa
Cc: Michael Barnes; Lectra Lawhorne
Subject: Re: CES server surplus

Chris,

This is fantastic news. Great work to all parties on closing the final recommendation from the incident after action report.

In your service,
Stephen.

Sent from Nine

From: Christopher Dehner
Sent: Aug 9, 2017 11:24 AM
To: Steven Dean; Jason Figueroa
Cc: Michael Barnes; Stephen Gay
Subject: CES server surplus

Fellas,

I will arrive at the center around 1:30 today to pick up the old DC. I will also get the old unicoi server from secure storage. Additionally, I sent in a service ticket for this request.

Regards,

Chris

Chris

Get Outlook for Android

From:	Michael L. Barnes
To:	Stephen Craig Gay
Subject:	Center for Election Systems Contract FY"17
Date:	Tuesday, March 7, 2017 8:57:45 AM
Attachments:	CES_KSU_FY17_060616_with_Budget.pdf

Stephen,

Here is our current contract with the Secretary of State's office. The content of the contract hasn't really changed since 2012 or so.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)
Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the 130.218.254.0/24 – (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.
    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support -- L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Ballot creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus
    8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
   Recommendation: Surplus
10. Web server backup
    Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. **Issue:** An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. **Issue:** A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.
Action Item Owner: UITS-ISO, UITS-ISS

10. **Issue:** Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

    Red = analog voice/phone
    Green = KSU data public network
    Blue = Elections private network
    White = Elections 2nd private network

    Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.
Action Item Owner: UITS-ISO, UITS-ISS

From: **Steven Dean** stevendean@kennesaw.edu
Subject: Re: Center for Elections
Date: March 1, 2017 at 3:31 PM
To: William C. Moore wcmoore@kennesaw.edu
Cc: Steven Dean sdean29@kennesaw.edu, Stephen Rose srose26@kennesaw.edu

Hey Bill, thanks for getting in touch. The two servers are in Nexpose already in a group. I've scanned Unicoi recently but need a little guidance on the specific vulnerabilities encountered.

unicoi.kennesaw.edu
elections.kennesaw.edu

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 1, 2017, at 3:02 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

> Steven,
>
> I understand that you are looking to have the Center for Elections servers reassessed for security vulnerabilities. Can you send us a list of DNS names or IP addresses? We can create a group in Nexpose for those servers and provide you the results of the assessments.
>
> Bill
>
> William C. Moore II CISSP, MEd, MLIS
> Associate Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg. Rm 031
> 1075 Canton Pl
> Kennesaw, GA 30144
> Tel: 470-578-6620
> Fax: 678-915-4940
> wcmoore@kennesaw.edu

From: **William C. Moore** wcmoore@kennesaw.edu
Subject: Center for Elections
Date: March 1, 2017 at 3:02 PM
To: Steven Dean sdean29@kennesaw.edu
Cc: Stephen Rose srose26@kennesaw.edu

Steven,

I understand that you are looking to have the Center for Elections servers reassessed for security vulnerabilities. Can you send us a list of DNS names or IP addresses? We can create a group in Nexpose for those servers and provide you the results of the assessments.

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: **Steven Dean** stevendean@kennesaw.edu
Subject: Re: Center for Elections
Date: March 1, 2017 at 3:31 PM
To: William C. Moore wcmoore@kennesaw.edu
Cc: Steven Dean sdean29@kennesaw.edu, **Stephen Rose** srose26@kennesaw.edu

Hey Bill, thanks for getting in touch. The two servers are in Nexpose already in a group. I've scanned Unicoi recently but need a little guidance on the specific vulnerabilities encountered.

unicoi.kennesaw.edu
elections.kennesaw.edu

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 1, 2017, at 3:02 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

> Steven,
>
> I understand that you are looking to have the Center for Elections servers reassessed for security vulnerabilities. Can you send us a list of DNS names or IP addresses? We can create a group in Nexpose for those servers and provide you the results of the assessments.
>
> Bill
>
> William C. Moore II CISSP, MEd, MLIS
> Associate Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg. Rm 031
> 1075 Canton Pl
> Kennesaw, GA 30144
> Tel: 470-578-6620
> Fax: 678-915-4940
> wcmoore@kennesaw.edu

From: **William C. Moore** wcmoore@kennesaw.edu
Subject: Center for Elections
Date: March 1, 2017 at 3:02 PM
To: Steven Dean sdean29@kennesaw.edu
Cc: Stephen Rose srose26@kennesaw.edu

Steven,

I understand that you are looking to have the Center for Elections servers reassessed for security vulnerabilities. Can you send us a list of DNS names or IP addresses? We can create a group in Nexpose for those servers and provide you the results of the assessments.

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: **Steven Dean** stevendean@kennesaw.edu
Subject: Re: Vulnerability on the elections.kennesaw.edu website
Date: March 1, 2017 at 11:48 PM
To: Merle S. King mking@kennesaw.edu
Cc: Barnes Michael mbarne28@kennesaw.edu

Acknowledging that I've seen this. See you tomorrow.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 1, 2017, at 11:44 PM, Merle S. King <mking@kennesaw.edu> wrote:

> FYI.
>
> Sent from my iPad
>
> Begin forwarded message:
>
> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> Merle,
>
> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.
>
> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Forwarded Message -----
> From: "Andy Green" <agreen57@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Sent: Wednesday, March 1, 2017 9:55:27 PM
> Subject: Vulnerability on the elections.kennesaw.edu website
>
> Stephen,
>
> Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.
>
> My friend shared with me that the exposed directories contained, among other things:
> - voter registration detail files, including DOB and full SSN.
> - PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election

November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d7065722070617261747573

From: **Merle S. King** mking@kennesaw.edu
Subject: Fwd: Vulnerability on the elections.kennesaw.edu website
Date: March 1, 2017 at 11:44 PM
To: Barnes Michael mbarne28@kennesaw.edu, sdean29@kennesaw.edu

FYI.

Sent from my iPad

Begin forwarded message:

From: "Stephen C. Gay" <sgay@kennesaw.edu>
Date: March 1, 2017 at 11:10:16 PM EST
To: Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
Subject: Fwd: Vulnerability on the elections.kennesaw.edu website

Merle,

I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.

I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Forwarded Message -----
From: "Andy Green" <agreen57@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

My friend shared with me that the exposed directories contained, among other things:
- voter registration detail files, including DOB and full SSN.
- PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d7065722070617261747573

From: **Stephen C. Gay** sgay@KENNESAW.EDU
Subject: Fwd: Vulnerability on the elections.kennesaw.edu website
Date: March 1, 2017 at 11:10 PM
To: Merle King mking@kennesaw.edu, Steven Dean sdean29@kennesaw.edu
Cc: Lectra Lawhorne llawhorn@kennesaw.edu, William C. Moore wmoore36@kennesaw.edu

Merle,

I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.

I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Forwarded Message -----
From: "Andy Green" <agreen57@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

My friend shared with me that the exposed directories contained, among other things:
- voter registration detail files, including DOB and full SSN.
- PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d7065722070617261747573

From: **Chris Gaddis** jgaddis6@KENNESAW.EDU
Subject: Re: Next steps for elections.kennesaw.edu
Date: March 2, 2017 at 1:58 PM
To: Steven Dean stevendean@kennesaw.edu
Cc: William C. Moore wcmoore@kennesaw.edu, Stephen C Gay sgay@kennesaw.edu, Michael Barnes mbarne28@kennesaw.edu, Merle S. King mking@kennesaw.edu

Steven,

As long as all log and config files are kept and you keep a record of what actions you are taking then I have no problem with that. We SHOULD have everything we need but you never know what questions might come up based upon the data we are reviewing.

Thanks,

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Chris Gaddis" <jgaddis6@kennesaw.edu>
Cc: "William C. Moore" <wcmoore@kennesaw.edu>, "Stephen C Gay" <sgay@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
Sent: Thursday, March 2, 2017 1:32:15 PM
Subject: Next steps for elections.kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: **Steven Dean** stevendean@kennesaw.edu
Subject: Next steps for elections.kennesaw.edu
Date: March 2, 2017 at 1:32 PM
To: Chris Gaddis jgaddis6@kennesaw.edu
Cc: William C. Moore wcmoore@kennesaw.edu, Stephen C. Gay sgay@kennesaw.edu, Michael Barnes mbarne28@kennesaw.edu, Merle S. King mking@kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: **Steven Dean** stevendean@kennesaw.edu
Subject: Re: Passwords contained in the database files
Date: March 2, 2017 at 2:54 PM
To: Chris Gaddis jgaddis6@kennesaw.edu
Cc: **William C. Moore** wcmoore@kennesaw.edu, **Stephen C Gay** sgay@kennesaw.edu, **Michael Barnes** mbarne28@kennesaw.edu, **Merle S. King** mking@kennesaw.edu

Thank you Chris. Since these password are changed each election, this will not present a security threat. The config info is from a closed private network between units and also should not present a security threat.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Mar 2, 2017, at 2:51 PM, Chris Gaddis <jgaddis6@kennesaw.edu> wrote:
>
> Steven,
>
> I mentioned in person that the database file contained some usernames and passwords of which I am unsure the origin or purpose. I will include a listing below of the data for your records (passwords redacted)
>
> Username DimsNet Password:s*******
> registarPassword (****)
> SupervisorPassword (****)
> LoginPassword 63********
>
> While not a security risk per se it also gave me internal config data such as :
>
> Integrated Security=false;Server=192.168.0.9;Database=TransactionData
> "networkAddress" "225.5.6.10"
>
> It's strongly advised in any circumstance to change ALL passwords if there is a chance they were disclosed. I am able to tell you the full password in person or over the phone if you need to validate or research which ones this is referring to. I can be reached at 470-578-6303 if you need me.
>
> Thanks,
>
> Chris Gaddis SSCP
> Information Security Engineer
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 029
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144 USA
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> jgaddis6@kennesaw.edu

From: **Chris Gaddis** jgaddis6@KENNESAW.EDU
Subject: Passwords contained in the database files
Date: March 2, 2017 at 2:51 PM
To: Steven Dean stevendean@kennesaw.edu
Cc: William C. Moore wcmoore@kennesaw.edu, **Stephen C Gay** sgay@kennesaw.edu, **Michael Barnes** mbarne28@kennesaw.edu, Merle S. King mking@kennesaw.edu

Steven,

I mentioned in person that the database file contained some usernames and passwords of which I am unsure the origin or purpose. I will include a listing below of the data for your records (passwords redacted)

Username DimsNet Password:s*******
registarPassword (****)
SupervisorPassword (****)
LoginPassword 63********

While not a security risk per se it also gave me internal config data such as :

Integrated Security=false;Server=192.168.0.9;Database=TransactionData
"networkAddress" "225.5.6.10"

It's strongly advised in any circumstance to change ALL passwords if there is a chance they were disclosed. I am able to tell you the full password in person or over the phone if you need to validate or research which ones this is referring to. I can be reached at 470-578-6303 if you need me.

Thanks,

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

From: **Steven Dean** sdean29@kennesaw.edu
Subject: Potentially Vulnerable Data
Date: March 2, 2017 at 1:19 PM
To: William C. Moore wcmoore@kennesaw.edu
Cc: Stephen C. Gay sgay@kennesaw.edu, **Michael Barnes** mbarne28@kennesaw.edu, **Merle S. King** mking@kennesaw.edu

Bill, according to our internal investigation, one of the files deemed potentially vulnerable is the Georgia state electors list. This list contains information pertaining to voter registration records.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

From: **Michael Barnes** mbarne28@kennesaw.edu
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)
Date: March 4, 2017 at 7:11 PM
To: Merle S. King mking@kennesaw.edu
Cc: Lectra Lawhorne llawhorn@kennesaw.edu, Stephen C. Gay sgay@kennesaw.edu, sdean29@kennesaw.edu

Unicoi has been shutdown

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 4, 2017, at 6:17 PM, Merle S. King <mking@kennesaw.edu> wrote:

> Working on it now
>
> --
> Merle S. King
> Executive Director
> Center for Election Systems
> 3205 Campus Loop Road; MD#5700
> Kennesaw State University
> Kennesaw, GA 30144
> Voice: 470-578-6900
> Fax: 470-578-9012
>
> On Mar 4, 2017, at 5:51 PM, Lectra Lawhorne <llawhorn@kennesaw.edu> wrote:
>
> > Stephen.
> >
> > Please call me.
> >
> > Lec
> >
> > On Mar 4, 2017, at 5:48 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
> >
> > > Michael,
> > >
> > > Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.
> > >
> > > Thank you,
> > > Stephen
> > >
> > > Sent from Nine
> > >
> > > **From:** William C. Moore
> > > **Sent:** Mar 4, 2017 5:44 PM
> > > **To:** Stephen Gay
> > > **Cc:** Chris Gaddis
> > > **Subject:** Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)
> > >
> > > Stephen
> > >
> > > The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.

The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.

Bill

William C. Moore II CISSP, MEd,MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

From: Chris Gaddis <jgaddis6@kennesaw.edu>
Date: March 4, 2017 at 17:32:24 EST
To: "William C. Moore" <wmoore36@kennesaw.edu>
Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Bill,

I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.

Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.

http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary 2010.zip <---- main concern
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf

http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

From: **Merle S. King** mking@kennesaw.edu
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)
Date: March 4, 2017 at 6:17 PM
To: Lectra Lawhorne llawhorn@kennesaw.edu
Cc: Stephen C. Gay sgay@kennesaw.edu, Michael Barnes mbarne28@kennesaw.edu, sdean29@kennesaw.edu

Working on it now

--
Merle S. King
Executive Director
Center for Election Systems
3205 Campus Loop Road; MD#5700
Kennesaw State University
Kennesaw, GA 30144
Voice: 470-578-6900
Fax: 470-578-9012

On Mar 4, 2017, at 5:51 PM, Lectra Lawhorne <llawhorn@kennesaw.edu> wrote:

> Stephen,
>
> Please call me.
>
> Lec
>
> On Mar 4, 2017, at 5:48 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> > Michael,
> >
> > Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.
> >
> > Thank you,
> > Stephen
> >
> > Sent from Nine
> >
> > **From:** William C. Moore
> > **Sent:** Mar 4, 2017 5:44 PM
> > **To:** Stephen Gay
> > **Cc:** Chris Gaddis
> > **Subject:** Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)
> >
> > Stephen
> >
> > The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.
> >
> > The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.
> >
> > Bill
> >
> > William C. Moore II CISSP, MEd.MLIS
> > Associate Executive Director

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

From: Chris Gaddis <jgaddis6@kennesaw.edu>
Date: March 4, 2017 at 17:32:24 EST
To: "William C. Moore" <wmoore36@kennesaw.edu>
Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Bill,

I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.

Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.

http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary 2010.zip <---- main concern
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

Michael Barnes

From: Stephen Craig Gay
Sent: Saturday, March 04, 2017 5:49 PM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Merle Steven King
Subject: Fw: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Michael,

Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.

Thank you,
Stephen

Sent from Nine

From: William C. Moore
Sent: Mar 4, 2017 5:44 PM
To: Stephen Gay
Cc: Chris Gaddis
Subject: Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Stephen

The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.

The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.

Bill

William C. Moore II CISSP, MEd,MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620

Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

From: Chris Gaddis <jgaddis6@kennesaw.edu>
Date: March 4, 2017 at 17:32:24 EST
To: "William C. Moore" <wmoore36@kennesaw.edu>
Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Bill,

I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.

Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.

http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary 2010.zip <---- main concern
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf

http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

Michael Barnes

From:	Merle Steven King
Sent:	Sunday, August 28, 2016 3:56 PM
To:	Steven Jay Dean; Jason Stephen Figueroa
Cc:	Michael L. Barnes
Subject:	Fwd: [IMPORTANT] concerning the security of elections.kennesaw.edu

Steven and Jason - Please review this email and advise. Sooner is better than later.

Thanks,

MSK

From: "Logan Lamb"
To: "Merle King"
Cc: research@bastille.net
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of elections.kennesaw.edu

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: https://www.bastille.net/. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"
I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install.

Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"
The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
https://www.drupal.org/project/drupalgeddon
https://www.drupal.org/SA-CORE-2014-005

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

Michael Barnes

From: Merle Steven King
Sent: Wednesday, March 01, 2017 11:45 PM
To: Michael L. Barnes; Steven Jay Dean
Subject: Fwd: Vulnerability on the elections.kennesaw.edu website

FYI.

Sent from my iPad

Begin forwarded message:

> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> Merle,
>
> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.
>
> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Forwarded Message -----

From: "Andy Green" <agreen57@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

My friend shared with me that the exposed directories contained, among other things:
- voter registration detail files, including DOB and full SSN.
- PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d7065722070617261747573

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Thursday, March 02, 2017 1:32 PM
To: James Christopher Gaddis
Cc: William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject: Next steps for elections.kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Steven Jay Dean
Sent: Wednesday, April 26, 2017 3:18 PM
To: Christopher Michael Dehner
Cc: Merle Steven King; Michael L. Barnes; Jason Stephen Figueroa
Subject: Private Network Hardware Assessment

Chris, we recently receive a draft of the Incident report and I would like to go through the hardware section to get a plan outlined for addressing the recommendations. The document states the following:

1. Rackmount UPS Battery backups (one displaying warning light)
   Recommendation: Replace batteries as needed and move under UITS ISS management
2. 3com Switches – Age 10+ years -- No Support -- L2 only
   Recommendation: Replace and move under UITS ISS management
3. Dell 1950 (Windows Domain Controller) – Age 10+ years
   Recommendation: Surplus
4. Dell PowerEdge R630 – Age 1 year
   Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
5. EPIC – Vision Computer – Age Unknown – Electors list creation box
   Recommendation: Continue as ISO/CES managed
6. EPIC Files – Dell 1900 – Age 6+ years – Electors list creation box backups
   Recommendation: Surplus
7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
   Recommendation: Surplus
8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610
   Recommendation: Format and reinstall on CES Isolated Network as NAS
9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
   Recommendation: Surplus
10. Web server backup
    Recommendation: Surplus

We had submitted for approval to UITS the purchase of two new UPS units prior to the incident. Should we continue and order these as previously planned?
Will new hardware (and other equipment) be ordered by ISO under ISO budget, ordered by ISO under CES budget, or ordered by CES? Who will decide what hardware is purchased?
How should we proceed with replacing the Switches and who will install and manage them?
When will the assessment of the private network software commence and what department will handle the migrations and updates? How will this project factor into their schedule?

We would like to get moving on this list as soon as possible. Please let me know what I can do as the next step. Thanks.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road

Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Merle Steven King
Sent: Monday, August 29, 2016 11:06 AM
To: Michael L. Barnes
Subject: Re: Follow Up from earlier email regarding security of elections.kennesaw.edu

Well said. Thanks

--

Merle S. King
Executive Director
Center for Election Systems
3205 Campus Loop Road; MD#5700
Kennesaw State University
Kennesaw, GA 30144
Voice: 470-578-6900
Fax: 470-578-9012

On Aug 29, 2016, at 11:04 AM, Michael Barnes <mbarne28@kennesaw.edu> wrote:

> Stephen,
> In retrospect, I need to pull back my request that you include Logan Lamb or his associated organization Bastille Threat Research Team (www.bastille.net) on a black list of ip addresses. My request was an over-reaction on my part. The quick security assessment they provided us, though unsolicited, did highlight an issue we needed to resolve with our website. To black list them for helping us would be inappropriate.
> Leading up to this election, where the question of whether or not someone can hack election systems is so in the forefront, we will need your team will help us continually analyze our online systems and inspect for any openings that need to be sealed. Our IT staff will be in touch today to let you know what enhancements we have made and will request that your team ping our system to see if you all find other issues.
> Thanks in advance for your help,
> Michael Barnes
> Director
> Center for Election Systems
> Kennesaw State University
> 3205 Campus Loop Road
> Kennesaw, GA 30144
> ph: 470-KSU-6900
> fax: 470-KSU-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Thursday, April 27, 2017 10:29 AM
To: Michael L. Barnes; Merle Steven King
Cc: Lectra Lawhorne; Christopher Michael Dehner
Subject: Re: Incident Reponse Walk through
Attachments: CES AAR Rev04.pdf

Michael and Merle,

Thank you for the edits. I have accepted them and attached the updated version and will be on the lookout for the referenced email.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, April 26, 2017 3:29:43 PM
Subject: RE: Incident Reponse Walk through

Stephen,

Thank you for giving us the opportunity to review the attached. We have provided a few grammatical changes and added just a few clarifying comments.
I am attaching a copy with Change Tracker on so you can quickly see those changes.

We have asked Steven Dean to follow up with Chris Dehner to see what timeline may be in place in relation to items listed in Issue 7. We want to make sure we are doing our part but we will need some guidance.

Please let us know what other assistance we can provide.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144

ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, April 24, 2017 12:01 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher M. Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

Michael Barnes

From: James Christopher Gaddis
Sent: Thursday, March 02, 2017 1:59 PM
To: Steven Dean
Cc: William C. Moore; Stephen Craig Gay; Michael L. Barnes; Merle Steven King
Subject: Re: Next steps for elections.kennesaw.edu

Steven,

As long as all log and config files are kept and you keep a record of what actions you are taking then I have no problem with that. We SHOULD have everything we need but you never know what questions might come up based upon the data we are reviewing.

Thanks,

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

----- Original Message -----
From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Chris Gaddis" <jgaddis6@kennesaw.edu>
Cc: "William C. Moore" <wcmoore@kennesaw.edu>, "Stephen C Gay" <sgay@kennesaw.edu>, "Michael Barnes" <mbarne28@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
Sent: Thursday, March 2, 2017 1:32:15 PM
Subject: Next steps for elections.kennesaw.edu

Chris, is there any further data you need from the server for your investigation? Our next intention is to make a backup of the affected files and remove them from the server. This would only affect files in the county folders, not log files are and config files. After that we will reach out to have the security of the server assessed by your group so that we may bring it back online without any previously vulnerable links.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Saturday, March 04, 2017 7:42 PM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Merle Steven King
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Michael,

Thank you so much and appreciate you coming to KSU to handle this tonight.

Stephen

Sent from Nine

From: Michael Barnes
Sent: Mar 4, 2017 7:11 PM
To: Stephen C. Gay
Cc: Lectra Lawhorne; Merle King
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Unicoi has been shutdown

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 4, 2017, at 5:48 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

> Michael,
>
> Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.
>
> Thank you,
> Stephen
>
> Sent from Nine
>
> **From:** William C. Moore
> **Sent:** Mar 4, 2017 5:44 PM
> **To:** Stephen Gay

Cc: Chris Gaddis
Subject: Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Stephen

The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.

The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.

Bill

William C. Moore II CISSP, MEd,MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

> **From:** Chris Gaddis <jgaddis6@kennesaw.edu>
> **Date:** March 4, 2017 at 17:32:24 EST
> **To:** "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)**
>
> Bill,
>
> I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.
>
> Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.
>
> http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary

2010.zip <---- main concern
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip
http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf

http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf
http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu

Michael Barnes

From: Stephen Craig Gay
Sent: Thursday, May 04, 2017 10:08 AM
To: Michael L. Barnes
Cc: Lectra Lawhorne; Christopher Michael Dehner; Merle Steven King
Subject: Re: Private Network Hardware Assessment

Michael,

Thank you for forwarding the email. UITS, as the provider of network infrastructure & connectivity, will provide the funding and specs for the battery backups as well as replacement switches. Other IT equipment which is specific to CES's mission (desktops/servers on the isolated network) will continue to be funded from the Center's budget and we will all work together on hardware specs which allows for support/maintenance to align with KSU standards.

The assessment & hardening of the private network will begin with the port locks and continue with post moves and equipment surplus as noted in the AAR. Our ultimate goal is to collectively remove all unnecessary services/hardware from the network and further secure and improve the remaining/new systems. I've asked Chris Dehner to take point and, working with his embedded staff, develop a plan for these items.

As always, please let me know if you have any additional questions or if I can assist further in any way,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Merle King" <mking@kennesaw.edu>
Sent: Thursday, April 27, 2017 10:39:08 AM
Subject: FW: Private Network Hardware Assessment

Stephen,

Here is the email Steven Dean sent Chris Dehner yesterday.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University

3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Wednesday, April 26, 2017 3:18 PM
To: Christopher M. Dehner <cmd9090@kennesaw.edu>
Cc: Merle S. King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>
Subject: Private Network Hardware Assessment

Chris, we recently receive a draft of the Incident report and I would like to go through the hardware section to get a plan outlined for addressing the recommendations. The document states the following:

1. Rackmount UPS Battery backups (one displaying warning light)
   Recommendation: Replace batteries as needed and move under UITS ISS management
2. 3com Switches – Age 10+ years -- No Support -- L2 only
   Recommendation: Replace and move under UITS ISS management
3. Dell 1950 (Windows Domain Controller) – Age 10+ years
   Recommendation: Surplus
4. Dell PowerEdge R630 – Age 1 year
   Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
5. EPIC – Vision Computer – Age Unknown – Electors list creation box
   Recommendation: Continue as ISO/CES managed
6. EPIC Files – Dell 1900 – Age 6+ years – Electors list creation box backups
   Recommendation: Surplus
7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
   Recommendation: Surplus
8. elections.kennesaw.edu <http://elections.kennesaw.edu> - Age 5 years - Dell PowerEdge R610
   Recommendation: Format and reinstall on CES Isolated Network as NAS
9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
   Recommendation: Surplus
10. Web server backup
    Recommendation: Surplus

We had submitted for approval to UITS the purchase of two new UPS units prior to the incident. Should we continue and order these as previously

planned?

Will new hardware (and other equipment) be ordered by ISO under ISO budget, ordered by ISO under CES budget, or ordered by CES? Who will decide what hardware is purchased?

How should we proceed with replacing the Switches and who will install and manage them?

When will the assessment of the private network software commence and what department will handle the migrations and updates? How will this project factor into their schedule?

We would like to get moving on this list as soon as possible. Please let me know what I can do as the next step. Thanks.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

Michael Barnes

From: Stephen Craig Gay
Sent: Monday, March 20, 2017 8:54 AM
To: Christopher Michael Dehner
Cc: Steven Jay Dean; Michael L. Barnes; James Christopher Gaddis
Subject: Re: Request for data retrieval

Chris,

This server is physically secured in ISO Evidence Storage. Please coordinate with Chris Gaddis and Steven Dean on the Data Recovery this morning.

Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>
Sent: Friday, March 17, 2017 9:10:57 AM
Subject: RE: Request for data retrieval

Stephen,

Thank you. Steven and Jason will be available first thing Monday to assist.

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Friday, March 17, 2017 9:09 AM
To: Michael Barnes <mbarne28@kennesaw.edu>
Cc: Steven Dean <sdean29@kennesaw.edu>; Merle King <mking@kennesaw.edu>; Lectra Lawhorne <llawhorn@kennesaw.edu>
Subject: Re: Request for data retrieval

Michael,

I have contacted the Federal investigators and they have agreed to return the server. I will be meeting with them late this afternoon to receive it and then secure it within ISO Secure Storage. I have asked the team to make this a top priority and to work with Steven and Jason on the request data retrieval 1st thing on Monday.

Please let me know if you have any questions or if I can assist further in any way, Stephen

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire cesuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 29, 2017 1:43 PM
To: James Christopher Gaddis
Cc: Christopher Michael Dehner
Subject: Re: Unknown files on elections.kennesaw.edu

Importance: High

Chris, here are the data contained in each of the file types you have listed:

>mpearso9/ExpressPoll/L&AFiles/PollData.db3

This type of file may contain a subset of the list of voters and any associated voter information for a given election. The file is used for testing purposes by counties before using an ExpressPoll during an election. The directory listed here indicates that this file was for CES testing purposes and may not contain PII.

>ExpressPoll%20L%26A/PollData.db3.php
>Test%20Staff/ExpressPoll/ABSFile/PollData.db3.php
>County%20User/ExpressPoll/ABSFile/PollData.db3.php

These files enable download of associated "PollData.db3" files by every browser. Note: these are PHP files that only link to other files and do not contain any election data.

>/sites/default/files/vendors/ESandS/Primary%202010.zip

Without analyzing this file, I cannot say for certain what is in it. Previous emails from ISO have indicated that inspection of this file showed it to contain voter information from the time the file was created in 2010. May contain PII.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

> On Mar 29, 2017, at 1:15 PM, Chris Gaddis <jgaddis6@KENNESAW.EDU> wrote:
>
> Steven,
>
> Can you please help me understand what data was contain in the files listed below.
>
> Was this County data?
> Full state data?
> Other Pii?
> Something else?

Also can you please respond ASAP on this.

Unique file names

ExpressPoll%20L%26A/PollData.db3.php
mpearso9/ExpressPoll/L&AFiles/PollData.db3
Test%20Staff/ExpressPoll/ABSFile/PollData.db3.php
County%20User/ExpressPoll/ABSFile/PollData.db3.php
/sites/default/files/vendors/ESandS/Primary%202010.zip

Thanks so much!

-Chris

Michael Barnes

From: Steven Dean <stevendean@kennesaw.edu>
Sent: Wednesday, March 01, 2017 11:49 PM
To: Merle Steven King
Cc: Michael L. Barnes
Subject: Re: Vulnerability on the elections.kennesaw.edu website

Acknowledging that I've seen this. See you tomorrow.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Mar 1, 2017, at 11:44 PM, Merle S. King <mking@kennesaw.edu> wrote:

> FYI.
>
> Sent from my iPad
>
> Begin forwarded message:
>
> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> Merle,
>
> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.
>
> I will be temporarily out of pocket for a short time tomorrow, then remote

thereafter, but your cooperation in this incident response is appreciated.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Forwarded Message -----
From: "Andy Green" <agreen57@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

My friend shared with me that the exposed directories contained, among other things:
- voter registration detail files, including DOB and full SSN.
- PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the

public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d7065722070617261747573

Bill, we updated the production server last night and I initiated a scan this morning. It looks really good to me, I'll just need your guidance on what issues we should address immediately. Thank you again for you and your department's work on the security on campus. This has been a huge help to us.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 12, 2016, at 5:53 PM, Steven Dean <stevendean@kennesaw.edu> wrote:

Bill, thank you! This is great news. The unicoi server doesn't have an ssl cert so the plain text log-ins over http will be corrected when we role the updates into the production server.

Samba shouldn't be running on these servers so that is also easily remedied.

Elections.kennesaw hasn't been updated yet, so that's why you're seeing all of the same vulnerabilities. Now that we've confirmed the updates fix most if not all of the vulnerabilities, we will work after hours in the coming days to transition elections.kennesaw to the latest versions of Debian and PHP, as is currently the case on unicoi.

Thank you for all your help with this, we will let you know when we are ready for the next round of scans.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Wed, Oct 12, 2016 at 2:25 PM -0400, "William C. Moore" <wcmoore@kennesaw.edu> wrote:

Steven,

We have scanned both elections and Unicoi servers with basic level scans. The scan of the Unicoi server identified one critical vulnerability but we also noticed two pages that allowed plaintext logins

(http://unicoi.kennesaw.edu/?q=user/login and the samba-swat login http://unicoi.kennesaw.edu:901/) . I am sure that you are aware that these are opportunities for malicious users to gather account credentials. Therefore, all website logins should be passed through an SSL tunnel such as using https for authentication.

The critical vulnerability discovered on the Unicoi server is for "Invalid CIFS Logins Permitted" which is most likely related to the Samba Configuration file smb.conf (https://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html).

The server elections.kennesaw.edu however is still showing that an outdated version of PHP is running and may be the reason 40+ critical vulnerabilities are being identified as related to PHP.

Can you tell us what version of PHP is running and when we may be allowed to run a more through scan?

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Thursday, October 06, 2016 11:58
To: William C. Moore <wcmoore@kennesaw.edu>
Cc: Michael Barnes <mbarne28@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>; Merle S. King <mking@kennesaw.edu>; Stephen C. Gay <sgay@kennesaw.edu>
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill, we have the backup site up and running (thanks to G.J.!) on the new version of Debian with all packages updated. Can we have unicoi.kennesaw.edu added to NeXpose for scanning?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 4, 2016, at 4:41 PM, Steven Dean <stevendean@kennesaw.edu> wrote:

Bill, thank you for following up. So far we haven't heard from anyone who can help us reconfigure apache and have thus far been unable to get it working. I sent our apache server logs to Matt as requested. Has any information about our configuration come from them?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Oct 4, 2016, at 4:37 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

Steven,

I and my team are taking the ISO lead on working with your team to help resolve any security issues with the server elections.kennesaw.edu. This is the last communication that I was copied on so can you

please provide me an update on where we stand on the server, PHP and Apache configurations? Where can we help and provide the greatest level of security support?

Thanks,

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Thursday, September 15, 2016 12:37
To: Matthew Sims <msims24@kennesaw.edu>
Cc: Michael Barnes <mbarne28@kennesaw.edu>; William C. Moore <wcmoore@kennesaw.edu>; Tyler Hayden <thayden2@kennesaw.edu>; Jason Figueroa <jfigue12@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>; Merle S. King <mking@kennesaw.edu>
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Matt, we've the backup server updated to Debian Jessie, but with the changes to apache between versions, we've discovered we're a little out of our depth in trying to reconfigure apache to work with our website. Can you put us in touch with someone who may be able to help us get the website back up

on the backup server? We're probably up to date with security on the backup server, but it's all for naught if the website doesn't work ;-)

Thank you!

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 12, 2016, at 11:55 AM, Matthew Sims <msims24@kennesaw.edu> wrote:

Steven,

I'm glad that the backup server is up and running. Thank you for the updates, and I hope your roll to production goes smoothly after testing.

From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Matthew Sims" <msims24@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "William C. Moore" <wcmoore@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>, "Merle S. King" <mking@kennesaw.edu>
Sent: Friday, September 9, 2016 3:54:40 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Good afternoon, Matt. We have our backup server up and running and just need to do a little testing before performing the updates. Once we confirm the distro update works on the backup server, we will roll the updates onto the production server and have you begin scans. This will give the most accurate scan results and tells us what we actually need help with security-wise. Thanks for your patience and the offer of help. I'll send you another update early next week. Have a great weekend.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road

Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 7, 2016, at 5:03 PM, Matthew Sims <msims24@kennesaw.edu> wrote:

Steven,

Thank you for the updates and transparency. We look forward to hearing back from you.

Have a good afternoon.

From: "Steven Dean" <stevendean@kennesaw.edu>
To: "Matthew Sims" <msims24@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "William C. Moore" <wcmoore@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Wednesday, September 7, 2016 4:43:28 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Matt, we're still working on getting a fully working clone on another server to perform the updates on. Once we have that working we'll roll the updates onto the production server. Then you can begin a new round of testing through NeXpose. Unfortunately, getting the updates completed with proper backups and testing has been slow going because of the election build, but that is all but passed and we are now working to get the server updated.

We will send you an update tomorrow on our progress and we should have a day for you to begin the new round of testing.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Sep 7, 2016, at 3:29 PM, Matthew Sims <msims24@kennesaw.edu> wrote:

Hi Michael,

I wanted to touch base with you and see what our game plan will be moving forward. Are we still in the stages of upgrading the OS and PHP version or has that already happened? In terms of scanning at the application level, I am trying to iron out a timeline and determine when this can be done using more aggressive scanning similar to Nexpose, but if you are going to be upgrading the OS and PHP version, then I may need to wait and coordinate a later time.

Thanks for your time and please let me know what you think.

From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "William C. Moore" <wcmoore@kennesaw.edu>
Cc: "Steven Dean" <stevendean@kennesaw.edu>, "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Matthew Sims" <msims24@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Friday, September 2, 2016 5:59:17 PM
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill,

Thank you. I will be back in touch on Tuesday to discuss when we would like for these scans to begin.

Sincerely,

Michael Barnes

Director

Center for Election Systems

3205 Campus Loop Road

Kennesaw State University

Kennesaw, GA 30144

ph: 470-578-6900

On Sep 2, 2016, at 5:55 PM, William C. Moore <wcmoore@kennesaw.edu> wrote:

Michael,

The directive to begin more agressive scanning came from Stephen Gay to help ensure that the server was not posing a risk to the Center of Elections missions and objectives.

The probability of damaging your website should be low. We do not wish to take any action that would actually damage any of your data or website(s). Typically a large portion of emails are sent by the

scanning engines auto completing website forms tha are not properly protected. These are usually more of an annoyance than any real damage.

The server does however have a number of critical and severe vulnerabilities some of which are reported to be exploitable. The majority of these are centered around PHP but others are OS related. These may be problematic but we would much rather test under controlled environments instead of the system becoming exploited during a time when your services are under high scrutiny and in great demand by polling stations around the state.

Since we would control the assessment tools the Information Security Office would be able to stop any assessments we (the ISO) are performing as soon as you noticed a degradation in services via a phone call to our team. Of course, I suspect that you have current backups of your website and data in case any other persons are performing malicious attacks against the Center of Elections. We do not of course anticipate you needing these backups for our assessments but you should still keep them and the restoration process up-to-date as a best practice. The Information Security Office does not want to impede the Center's objectives at all. We want to help mitigate any risks that the Center is facing such as the risks that Mr. Lamb from the Bastille Threat Research Team discovered and reported. There are a number of documents found from the Center of Elections website that have been cached by various search engines. These are not threats that we can now prevent; however, we can offer suggestions on how to request those cached documents be removed from the various search engine providers.

I hope that this addresses some of your concerns and since this has to be a two way partnership in our assessment we encourage you to ask questions along the way.

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "William C. Moore" <wcmoore@kennesaw.edu>, "Steven Dean" <stevendean@kennesaw.edu>
Cc: "Tyler Hayden" <thayden2@kennesaw.edu>, "Jason Figueroa" <jfigue12@kennesaw.edu>, "Matthew Sims" <msims24@kennesaw.edu>, "Chris Gaddis" <jgaddis6@kennesaw.edu>
Sent: Wednesday, August 31, 2016 3:15:46 PM
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

Bill,

Before we give go ahead on potential scan periods I have a couple of follow up questions:

1. The directive to begin more aggressive scanning has come from who and for what reason?

2. How high a probability is there of issues being created that could damage the functionality of our website?

We are currently in the busiest time of the year for use of our website by our county clients. The last thing we can afford to have happen is for our website to become unavailable or usable. If the action of conducting these scans were to disable our website, what remedy would be available so the services we provide to the election community in Georgia would not be damaged?

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: William C. Moore [mailto:wcmoore@kennesaw.edu]
Sent: Wednesday, August 31, 2016 2:47 PM
To: 'Steven Dean' <stevendean@kennesaw.edu>
Cc: 'Tyler Hayden' <thayden2@kennesaw.edu>; 'Michael Barnes' <mbarne28@kennesaw.edu>; 'Jason Figueroa' <jfigue12@kennesaw.edu>; 'Matthew Sims' <msims24@kennesaw.edu>; Chris Gaddis <jgaddis6@kennesaw.edu>
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

Steven,

The recent scans have been "Safe Scans w/o Spidering". I have been asked though to begin more aggressive scanning. Since these types of scans have the potential of creating issues such as completing and submitting forms

(creating email messages) interfering with services and/or stopping services which we try to avoid. Since these assessments have the potential of creating issues we need to schedule these types of assessments. Please understand that we do not perform any testing that cannot already be performed by any user on the campus network. We also do not purposefully perform any DOS or DDOS attempts since the network perimeter firewalls provide some level of protection against DDOS attempts.

When is the earliest we can schedule more aggressive scanning of the server?

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:stevendean@kennesaw.edu]
Sent: Wednesday, August 31, 2016 10:38
To: William C. Moore <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu> >
Cc: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >;
Michael Barnes <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >;
Jason Figueroa <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >;
Matthew Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Thanks Bill. I see the list appears to be the same as from the first scan. Jason and I are working on a plan to upgrade to the latest version of Debian which will also allow us to update to the latest version of PHP, where it seems most of the vulnerabilities are. Let me know if there is anything in the scan we should be concerned about that the Debian update may not fix. Thanks for all the help, we really appreciate your time. It has been immensely beneficial.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 31, 2016, at 10:34 AM, William C. Moore <wcmoore@kennesaw.edu <mailto:wcmoore@kennesaw.edu> > wrote:

Steven

The authenticated scan completed last night and I will share the results as soon as my current meeting completes.

William C. Moore II CISSP, MEd,MLIS
Associate Executive Director

Information Security Office

University Information Technology Services (UITS)
Kennesaw State University

Technology Services Bldg. Rm 031

1075 Canton Pl

Kennesaw, GA 30144

Tel: 470-578-6620

Fax: 678-915-4940

wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

On Aug 31, 2016, at 10:00, Steven Dean <stevendean@kennesaw.edu <mailto:stevendean@kennesaw.edu> > wrote:

Sounds good to us. Thanks Tyler.

What is the status of the authenticated scan? I couldn't find where it had been run and when I went to run a scan, the available options made it difficult to choose while not really understanding them.

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Wed, Aug 31, 2016 at 9:56 AM -0400, "Tyler Hayden" <thayden2@kennesaw.edu <mailto:thayden2@kennesaw.edu> > wrote:

Hi Steven,

In addition to the NeXpose scan, we'd also like to scan with IBM AppScan. AppScan will focus more specifically on the Drupal application rather than an overarching system scan with NeXpose. Matt Sims will reach out to you to configure and schedule the AppScan assessment.

Regards,

Tyler Hayden
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503

Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9051
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu>

----- Original Message -----
From: "William C. Moore" <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

To: "Steven Dean" <sdean29@kennesaw.edu<mailto:sdean29@kennesaw.edu> >
Cc: "Tyler Hayden" <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >,
"Michael Barnes" <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >,
"Jason Figueroa" <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >,
"Matthew Sims" <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Sent: Tuesday, August 30, 2016 2:03:57 PM
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>

Yes, this will be a local Linux account. It is preferable that the account be provided sudo privileges only. I strongly recommend that you limit the account to only be allowed to log in locally for your testing purposes and from the IP addresses 130.218.100.80 and 10.97.52.25 (the two current Nexpose scanning engines).

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Tuesday, August 30, 2016 12:21
To: William C. Moore <wcmoore@kennesaw.edu<mailto:wcmoore@kennesaw.edu> >
Cc: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >;
Michael Barnes
<mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >; Jason Figueroa
<jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >; Matthew
Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>

Just to clarify, are the required credentials a linux account for the server itself? Also, could you define "privileged account"? Does it need to be an admin or just have sudo ability?

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 30, 2016, at 11:59 AM, William C. Moore <wcmoore@kennesaw.edu
<mailto:wcmoore@kennesaw.edu>
<mailto:wcmoore@kennesaw.edu> > wrote:

Steven,

Please log back in to Nexpose and use the following steps to add an account for patching and vulnerability verification.

Select Home then scroll though Sites until you find the site "Elections-Server".

Select the Edit icon (pencil) for the Elections-Server site.

Select the Authentication tab at the top of the page.

Click the "Elections-Server-Account" link under Scan Credentials.

You should now be in the Edit Credential page. From this page select

"Account" on the left hand side of the page.

This page already has the Service as Secure Shell (SSH) selected. You should enter the User Name and enter the appropriate password in both the Password field and Confirm Password field.

After you have entered and confirmed the account credentials please click the "Test Credentials" link beside the question mark near the bottom of the page to verify the account and credentials work.

After successfully testing the credentials click the Save button at the bottom of the page then click the Save button at the top right hand side of the page.

Please let us know when you have added, tested and saved the authentication information and we will test the site again for vulnerabilities.

Bill

William C. Moore II CISSP, MEd, MLIS
Associate Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
<mailto:wcmoore@kennesaw.edu> wcmoore@kennesaw.edu
<mailto:wcmoore@kennesaw.edu>

From: Steven Dean [mailto:sdean29@kennesaw.edu]
Sent: Monday, August 29, 2016 16:46
To: Tyler Hayden <thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu>
<mailto:thayden2@kennesaw.edu> >

Cc: Michael Barnes <mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu>
<mailto:mbarne28@kennesaw.edu> >;
Jason Figueroa <jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu>
<mailto:jfigue12@kennesaw.edu> >;
Matthew Sims <msims24@kennesaw.edu<mailto:msims24@kennesaw.edu>
<mailto:msims24@kennesaw.edu> >; William
C. Moore <wmoore36@kennesaw.edu<mailto:wmoore36@kennesaw.edu>
<mailto:wmoore36@kennesaw.edu> >
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu
<http://elections.kennesaw.edu/>
<http://elections.kennesaw.edu<http://elections.kennesaw.edu%3e> >;

Thanks Tyler. I've logged into NeXpose so we're ready to have our server added. Server info:

Hostname: <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >; elections.kennesaw.edu
<http://elections.kennesaw.edu/>

IP: 130.218.251.50

OS: Debian Wheezy v7.11

Hosted Application: Drupal 7.5

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 29, 2016, at 4:22 PM, Tyler Hayden < <mailto:thayden2@kennesaw.edu>
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> > wrote:

Hi Steven,

Thanks for reaching out. We can definitely assist in assessing the security and of your site. For starters, we can arrange for a security and vulnerability assessment scan on your systems via NeXpose to get some better insight.

We can scan both authenticated or unauthenticated. Authenticated scans will

produce more accurate results, but also require credentials for a privileged account. We can configure it to allow you to log in to NeXpose to provide these credentials, if you do not want to provide them to us directly. We'll just need information on the systems you'd want assessed. (Host names, OS, IP address, hosted applications, etc.)

While I am not all too familiar with Drupal, I do know that there are several modules available for restricting content in Drupal, such as the Secure Site module which is available here:

<https://www.drupal.org/project/securesite
<https://www.drupal.org/project/securesite%3E> >;
https://www.drupal.org/project/securesite

This is just one of the available modules, so if this does not suit your needs there are others available. I would also review Drupal's documentation on secure configuration available here:

<https://www.drupal.org/security/secure-configuration
<https://www.drupal.org/security/secure-configuration%3E> >;
https://www.drupal.org/security/secure-configuration

to ensure that your site is following their best practices.

Without doing some research of my own, I am not certain on how to go about restricting file access using the htaccess files. Typically you would include a directive to only allow authenticated users to access the file, however, I am not certain of how Drupal handles it's authentication or if it shares it with the Apache web server. This is something we can look into and let you know what we find.

Regards,

Tyler Hayden
IT Security Professional III
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9051
<mailto:thayden2@kennesaw.edu> thayden2@kennesaw.edu
<mailto:thayden2@kennesaw.edu>

----- Original Message -----
From: "Steven Dean" < <mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> >
To: "Tyler Ray Hayden" < <mailto:thayden2@kennesaw.edu>
thayden2@kennesaw.edu<mailto:thayden2@kennesaw.edu> >

Cc: "Michael Barnes" < <mailto:mbarne28@kennesaw.edu>
mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> >, "Merle S. King" <
<mailto:mking@kennesaw.edu>
mking@kennesaw.edu<mailto:mking@kennesaw.edu> >, "Jason Figueroa" <
<mailto:jfigue12@kennesaw.edu>
jfigue12@kennesaw.edu<mailto:jfigue12@kennesaw.edu> >
Sent: Monday, August 29, 2016 2:39:41 PM
Subject: Re: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/>

Good afternoon, Tyler. I wanted to reach out for some assistance with our website as suggested in Stephen's email below.

For some background information, Jason and I have taken responsibility for the website here at Center for Election Systems. This site was build on Drupal before either of us were employed here and we have spent the last several years simply maintaining it in the order it had been working previously. Obviously this has become untenable in the current atmosphere, and Jason and I must learn more to get the security of the website under control. In this regard we appreciate any help you can offer on security best practices and specific security implementations that will allow us to secure the site.

This morning we implemented a patch to disallow file tree access by anonymous users and we updated our Drupal installation to the current version of Drupal 7. Unfortunately, until today, it seems the file tree had been available to anonymous users. We have denied access by changing the "AllowOverride None" in the apache virtualhost configuration for /var/www/ to "AllowOverride All" so that the .htaccess file parameters will disallow anonymous user access outside Drupal.

While we have denied access to the file tree, we are currently we are having trouble patching the ability for anonymous users to access individual files directly without also disallowing Drupal user access to those files. We have tried adding a <files> tag section tot he apache2.conf to deny access to pdf files, but this breaks Drupal user access as well. I'm sure there is some way to do this in the .htaccess file, but we have so far been unable to find the method.

Please let Jason and I know if you have any insights that will help accomplish this goal, as well as get a local firewall set up to allow us to monitor access through logs.

Thank you,

Steven Dean
Technical Coordinator
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: 470-578-6900 F: 470-578-9012

On Aug 29, 2016, at 11:31 AM, Stephen C. Gay < <mailto:sgay@kennesaw.edu> sgay@kennesaw.edu<mailto:sgay@kennesaw.edu> > wrote:

Michael,

Thanks for reaching out and we stand on ready to help. The source email domain, <http://bastille.net/<http://bastille.net/%3E> >; bastille.net <http://bastille.net/> < <http://bastille.net/<http://bastille.net/%3E> >; http://bastille.net/ <http://bastille.net/%3E> >;, has a valid domain registration through GoDaddy and
located in Atlanta:

Registry Registrant ID:
Registrant Name: Michael Engle
Registrant Organization: Bastille Networks
Registrant Street: 1000 Marietta St NW
Registrant Street: Suite 112
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30318
Registrant Country: US
Registrant Phone: +1.7328200096
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: <mailto:domains@bastillenetworks.com> domains@bastillenetworks.com<mailto:domains@bastillenetworks.com> < <mailto:domains@bastillenetworks.com> mailto:domains@bastillenetworks.com>

We don't put internal domain blocks in place unless we detect a spike in phishing or vulnerability scanning from that domain which, at this point, isn't the case for <http://bastille.net/<http://bastille.net/%3E> >; bastille.net <http://bastille.net/> < <http://bastille.net/ <http://bastille.net/%3E> >; http://bastille.net/ <http://bastille.net/%3E> >;. It's very likely that the tester utilized Google searches on the <http://elections.kennesaw.edu/ <http://elections.kennesaw.edu/%3E> >; elections.kennesaw.edu<http://elections.kennesaw.edu/> < <http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; domain which included file extensions, along
with HTML Headers which include the service versions.

Here the the Google search string which reveals the document he references
".pdf site:elections.kennesaw.edu"
Reporting precincts with cards -

<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;
https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3C>
&A/Reporting%20Precincts%20with%20Cards.pdf<;
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;
https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L
<https://elections.kennesaw.edu/sites/default/files/ExpressPoll%20L&A/Reporting%20Precincts%20with%20Cards.pdf%3E>
&A/Reporting%20Precincts%20with%20Cards.pdf>;

And here is the header response for
<https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >;
https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3C> <;
<https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >;
https://elections.kennesaw.edu/?q=user/login
<https://elections.kennesaw.edu/?q=user/login%3E> >; that gives away the use
of
Drupal
<https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;
https://elections.kennesaw.edu/misc/drupal.js?ococft <
<https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;
https://elections.kennesaw.edu/misc/drupal.js?ococft
<https://elections.kennesaw.edu/misc/drupal.js?ococft%3E> >;

It is reasonable to assume that these types of unsolicited requests are going to increase leading up to the general election in November and we stand on ready to offer application security analysis and recommendations. In turn, I would highly recommend the use of an server based firewall/IDS to track this activity (specifically brute force attempts on the login page) and ensure that all access are logged.

I am cc'ing 2 members of my team, Mr. Tyler Haden and Mr. Bill Moore, to advise on operating system/application vulnerabilities and provide advice on mitigating strategies. Tyler will act as your point of contact and if I can assist in any way please let me know.

In service,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
<mailto:sgay@kennesaw.edu> sgay@kennesaw.edu<mailto:sgay@kennesaw.edu> <
<mailto:sgay@kennesaw.edu>
mailto:sgay@kennesaw.edu>

----- Original Message -----
From: "Michael Barnes" < <mailto:mbarne28@kennesaw.edu>
mbarne28@kennesaw.edu<mailto:mbarne28@kennesaw.edu> <
<mailto:mbarne28@kennesaw.edu>
mailto:mbarne28@kennesaw.edu>>
To: "Stephen C Gay" < <mailto:sgay@kennesaw.edu> sgay@kennesaw.edu
<mailto:sgay@kennesaw.edu> <
<mailto:sgay@kennesaw.edu> mailto:sgay@kennesaw.edu>>
Cc: "Merle King" < <mailto:mking@kennesaw.edu> mking@kennesaw.edu
<mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu>>, "Steven Dean" <
<mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> <
<mailto:sdean29@kennesaw.edu> mailto:sdean29@kennesaw.edu>>, "Jason
Figueroa" < <mailto:jfigue12@kennesaw.edu> jfigue12@kennesaw.edu
<mailto:jfigue12@kennesaw.edu> <
<mailto:jfigue12@kennesaw.edu> mailto:jfigue12@kennesaw.edu>>
Sent: Monday, August 29, 2016 9:24:30 AM
Subject: FW: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;

Stephen,

We received an unsolicited email over the weekend from a Logan Lamb. The content of the email has engaged our staff and we are looking into these claims regarding the security of our website. Would you please add this individual and the organization he claims to be affiliated with to the list of IP addresses most recently black listed? Also, our IT staff, Steven Dean and Jason Figueroa will be reaching out to you and your staff to see what assistance your group can provide us in pinging our site to verify that we are addressing security issues within our site.

Thank you in advance,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Merle S. King [<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu]
Sent: Sunday, August 28, 2016 3:56 PM
To: Steven Dean < <mailto:sdean29@kennesaw.edu> sdean29@kennesaw.edu
<mailto:sdean29@kennesaw.edu> >; Jason
Figueroa
< <mailto:jfigue12@kennesaw.edu> jfigue12@kennesaw.edu
<mailto:jfigue12@kennesaw.edu> >
Cc: Michael Barnes < <mailto:mbarne28@kennesaw.edu> mbarne28@kennesaw.edu
<mailto:mbarne28@kennesaw.edu> >
Subject: Fwd: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/>

Steven and Jason - Please review this email and advise. Sooner is better
than later.

Thanks,

MSK

From: "Logan Lamb" < <mailto:logan@bastille.net> logan@bastille.net
<mailto:logan@bastille.net> <
<mailto:logan@bastille.net> mailto:logan@bastille.net> <
<mailto:logan@bastille.net> mailto:logan@bastille.net<
<mailto:logan@bastille.net> mailto:logan@bastille.net>> >
To: "Merle King" < <mailto:mking@kennesaw.edu> mking@kennesaw.edu
<mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu> <
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu<
<mailto:mking@kennesaw.edu> mailto:mking@kennesaw.edu>> >

Cc: <mailto:research@bastille.net> research@bastille.net
<mailto:research@bastille.net> <
<mailto:research@bastille.net> mailto:research@bastille.net> <
<mailto:research@bastille.net> mailto:research@bastille.net<
<mailto:research@bastille.net> mailto:research@bastille.net>>
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of

Bastille Threat Research Team. We work to secure devices against new and

existing wireless threats: <https://www.bastille.net/
<https://www.bastille.net/%3E> >;
https://www.bastille.net/ < <https://www.bastille.net/
<https://www.bastille.net/%3E> >;
https://www.bastille.net/<https://www.bastille.net/%3E> >;. This past
Tuesday I
went

to Fulton County Government Center to speak with Rick Barron about securing

voting machines against wireless threats. I was then directed to contact you

and the center. I'd like to collaborate with you on securing our state's

election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to

contacting you, I discovered serious vulnerabilities affecting

<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >; <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu%3c> <;
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>; .

The following google searches reveal documents that shouldn't be indexed and

appear to be critical to the elections process. In addition, the Drupal
install

needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu < <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>;
inurl:pdf"

I generally use this type of search to find documents on websites that
lack

search functionality. This search revealed a completely open Drupal install.

Assume any document that requires authorization has already been downloaded

without authorization.

"site:elections.kennesaw.edu < <http://elections.kennesaw.edu/
<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu<http://elections.kennesaw.edu/> <
<http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E> >;
http://elections.kennesaw.edu/<http://elections.kennesaw.edu/%3E%3E> >>;
L&A"

The second search result appears to be for disseminating critical voting

system software. This is especially concerning because, as the following
article

states, there's a strong probability that your site is already compromised.

<https://www.drupal.org/project/drupalgeddon
<https://www.drupal.org/project/drupalgeddon%3E> >;
https://www.drupal.org/project/drupalgeddon<
<https://www.drupal.org/project/drupalgeddon
<https://www.drupal.org/project/drupalgeddon%3E> >;
https://www.drupal.org/project/drupalgeddon
<https://www.drupal.org/project/drupalgeddon%3E> >;

<https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;
https://www.drupal.org/SA-CORE-2014-005<
<https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;
https://www.drupal.org/SA-CORE-2014-005
<https://www.drupal.org/SA-CORE-2014-005%3E> >;

If you have any questions or concerns please contact me. I'm able to come to the

center this Monday for a more thorough discussion.

Take care,

Logan

--

Merle S. King

Executive Director

Center for Election Systems

Kennesaw State University

3205 Campus Loop Road

Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
msims24@kennesaw.edu

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
msims24@kennesaw.edu

--

Matt Sims
Information Security Specialist

Identity & Access Management
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144

Phone: (470) 578-6620
msims24@kennesaw.edu