From: **Sara Ghazal** <[redacted]@georgiademocrat.org>
Date: Sat, Nov 3, 2018 at 11:42 AM
Subject: Potential cyber-vulnerability on SOS Voter page
To: [REDACTED]

Dear [REDACTED],

I hope you both are well, and do not mind that I am reaching out to you directly.

We received an email today with the attached data. If this report is accurate, it is a massive vulnerability. I do not have the sort of technical background to evaluate it properly.

Thank you for your time, and I look forward to hearing from you. I also hope you both might be available AFTER November 6 to have a longer conversation about election security and election systems.

Best regards,

Sara

Sara Tindall Ghazal

Voter Protection Director

Democratic Party of Georgia

www.georgiademocrat.org

Direct: [redacted]

Here is Richard Wright's email to Rachel Small (volunteer for the Democratic Party of Georgia):

---------- Forwarded message ---------
From: **Richard Wright** <[REDACTED]>
Date: Sat, Nov 3, 2018 at 10:48 AMP
Subject: SOS Voter page issue details
To: [REDACTED], Rachel Small <[REDACTED]>

Hey Rachel,

Nate asked me to provide you with details on the issues that I've discovered, and I believe he spoke to you about.

I've attached a postman file which shows details on the two issues I've discovered. The first issue is with the [redacted]. It has a [redacted] allows you to download any file on the system. The second issue is with the online voter registration. On that site, you can [redacted] That url [redacted] ..., you can download anyones data and that includes lots of PII (ie drivers license and last 4 of Ssn).

Feel free to call me at [REDACTED] if you have questions.

Richard

The paragraph from Richard's email was lifted and sent to Sara Ghazal, Voter Protection Director for the Democratic Party of Georgia. Here is Rachel's email to Sara, which is apparently the focus for the Kemp campaign to involve the FBI in making bogus allegations:

---------- Forwarded message ---------
From: **Rachel Small** <[REDACTED]>
Date: Sat, Nov 3, 2018 at 11:18 AM
Subject: Fwd: SOS Voter page issue details
To: Sara Ghazal <[REDACTED]>

I've attached a postman file which shows details on the two issues I've discovered. The first issue is with [redacted]. It has a [redacted] allows you to download any file on the system. The second issue is with the online voter registration. On that site, you can [redacted] That url [redacted] ..., you can download anyones data and that includes lots of PII (ie drivers license and last 4 of Ssn).

As is abundantly clear in Richard's email, it was HIM, not Rachel, who performed the actions described. The Kemp campaign has no case. Further, they neglect to realize that "Fwd:" means "forward" of an email, not an original email.

-------- Original message --------
From: "Cross, David D." <[redacted]@mofo.com>
Date: 11/3/18 11:59 AM (GMT-05:00)
To: "Hunt, Chad R. (AT) (FBI)" <[redacted]@fbi.gov>
Cc: "Carlin, John P." <[redacted]@mofo.com>, "Newman, David A." <[redacted]@mofo.com>
Subject:

Hi Chad -

I understand John alerted you to an issue that's just been brought to our attention. By way of background, we represent GA voters in a case pending against the state regarding vulnerabilities in the current election system. This includes confidential information that a white hat hacker discovered was publicly available in 2016 on a GA election website. The FBI got involved then, including confiscating a GA state election server.

Because of this case and the publicity around it, a GA voter recently contacted us about another vulnerability he believes he stumbled upon involving the state myvoter page: https://www.mvp.sos.ga.gov/MVP/mvp.do. He believes there are files that are publicly available that shouldn't be, such as voter registration information. He told us he didn't do much digging because he was worried about accessing something he shouldn't, and so it's unclear what all is available and whether it's actually not supposed to be available.

We didn't want to sound a false alarm when we received this vague information late yesterday afternoon. So we quickly consulted a reputable cybersecurity firm about the report that we received while emphasizing the importance of not accessing confidential data or altering or extracting data. They stumbled upon absentee voter information that looks like maybe it should be confidential, but since neither they nor we have examined that data, we don't know for sure whether it's confidential or not.

In short, given the history of confidential information previously available on a GA election website, we are concerned that there may be confidential voter/election information available on the GA myvoter website. So we felt obliged to alert you so that the appropriate federal authorities could investigate and determine whether there is an actual breach or vulnerability here and assess what, if anything, should be done to address this issue before the election. Given the ongoing litigation, we also plan to alert the state via their counsel and possibly the court.

Thanks for your attention to this. We are available to discuss further, including over the weekend.

DC

From: "Cross, David D." <[redacted]@mofo.com>
Date: November 4, 2018 at 4:59:55 PM EST
To: "Cross, David D." <[redacted]@mofo.com>
Subject: FW: Re:

You can see below that I specifically flagged voter registration info as accessible in my email to the FBI, not just absentee voter information. And the agent indicates that he's passing this along to the SoS in GA. So the claim from the SoS that the reported vulnerability concerned only absentee voter information and not voter registration information is demonstrably false.

From: Hunt, Chad R. (AT) (FBI) [redacted]@fbi.gov>
Date: Saturday, Nov 03, 2018, 1:31 PM
To: Cross, David D. <[redacted]@mofo.com>
Cc: Carlin, John P. <[redacted]@mofo.com>, Newman, David A. [redacted]@mofo.com>
Subject: Re:

- External Email -

Thanks!

We'll pass the information along to the Secretary of State's Office for them to evaluate since they are best positioned to address what is described below. We'll also include DHS, since they may be able to assist with mitigation.

If needed, is the researcher and/or the cybersecurity research firm available for contact to get additional details about what was found and/or the vulnerability?

Chad

---------- Forwarded message ---------
From: <[REDACTED]>
Date: Sat, Nov 3, 2018 at 1:05 PM
Subject: RE: Potential cyber-vulnerability on SOS Voter page
To: Sara Ghazal <[REDACTED]>

Sara/[REDACTED],

Thanks for forwarding.

The attached postman file appears to contain the vulnerabilities described. I don't advise encouraging people to poke at MVP with test, random, or personal data because they might click on things that have legal implications.

I know who to send this to. For now let's just keep a record of the email conversations for later use.

Would welcome a discussion after November 6. Do you have my contact information?

[REDACTED]

From: "Cross, David D." <[redacted]@mofo.com>
Date: November 4, 2018 at 5:12:30 PM EST
To: "Cross, David D." <[redacted]@mofo.com>
Subject: FW: Re:

Here's confirmation from the FBI that the information I provided was passed on to Kemp's office and that the FBI would let them know that Wright was available to talk.

From: Hunt, Chad R. (AT) (FBI) <[redacted]@fbi.gov>
Date: Saturday, Nov 03, 2018, 2:23 PM
To: Cross, David D. <[redacted]@mofo.com>
Cc: Carlin, John P. <[redacted]@mofo.com>, Newman, David A. <[redacted]@mofo.com>
Subject: Re: Re:

Thanks! Info passed to GA Sec of State office and DHS along with offer to put them in contact with the researcher and/or the cybersecurity firm.

-

-------- Original message --------
From: "Cross, David D." <[redacted]@mofo.com>
Date: 11/3/18 1:43 PM (GMT-05:00)
To: "Hunt, Chad R. (AT) (FBI)" <[redacted]@fbi.gov>
Cc: "Carlin, John P." <[redacted]@mofo.com>, "Newman, David A." <[redacted]@mofo.com>
Subject: RE: Re:

The researcher who reported it is available. We can make our cybersecurity firm available too if needed. Let us know how we can help. And thanks for looking into this.

From: "Cross, David D." [redacted]@mofo.com>
Date: November 4, 2018 at 5:03:25 PM EST
To: "Cross, David D." [redacted]@mofo.com>
Subject: FW: Here's who contacted us

Here's my email to Salter providing contact information for Wright. I've x'ed out the number to respect Mr. Wright's privacy. The email is otherwise not changed, and I can confirm that the number I provided Salter is the same one Wright gave me and that I spoke to him on during our Friday afternoon call.

From: John Salter <[redacted]barneslawgroup.com>
Date: Saturday, Nov 03, 2018, 4:15 PM
To: Cross, David D. <[redacted]@mofo.com>
Subject: Re: Here's who contacted us

- External Email -

Thanks for the heads up. I'll pass along.
Cheers,
John

Sent from my iPhone

On Nov 3, 2018, at 4:12 PM, Cross, David D. <DCross@mofo.com<mailto:DCross@mofo.com>> wrote:

Richard Wright
xxx.xxx.xxxx

From: "Cross, David D." <[redacted]@mofo.com>
Date: November 4, 2018 at 4:55:43 PM EST
To: "Cross, David D." <[redacted]@mofo.com>
Subject: RE: Important Info re Alleged GA DNC Hacking

I understand the Secretary of State has issued some sort of statement indicating that I provided only vague information focused on absentee information in my call with John Salter yesterday. This is false. I emphasized that we did not know the breadth of the potential vulnerability but that we were told that it looked like potentially all the files sitting behind the website were possibly accessible. I noted the absentee information merely as one example. Moreover, I provided Mr. Wright's contact information to Mr. Salter for the very purpose of the SoS contacting him to investigate his concerns. I encouraged Mr. Salter to have the SoS do this and to have their own election security people investigate the myvoter website. Again, nobody from the SoS has contacted Mr. Wright, he tells me. Nor has anyone from the SoS followed up with me today. If the SoS genuinely wanted to understand and investigate the issue and felt what I provided was too limited, they could and should have immediately contacted Mr. Wright as I encouraged. That they haven't even now raises serious questions about their true intentions and suggests either more ineptitude from this SoS regarding election security or something more nefarious aimed at distracting from yet another failure by Secretary Kemp to secure the GA election system. This is eerily similar to how they attacked Logan Lamb when he found serious online vulnerabilities with the GA election website in 2016 and 2017 and consistent with Secretary Kemp's repeated misleading claims to voters that the GA election system is safe and secure. A US District Court Judge, on a robust record including testimony from witnesses Secretary Kemp offered to defend the system, found that it in fact suffers from significant vulnerabilities and that Secretary Kemp has taken a head in the sand approach to those concerns. That he now has turned this newest vulnerability into a political issue rather than approaching it in the nonpartisan manner it warrants is extremely disappointing and inappropriate.