Reuters: The Clinton Foundation May Have Been Hacked

Bill and Hillary Clinton's charitable foundation hired the security firm FireEye to examine its data systems after seeing indications they might have been hacked, according to two sources familiar with the matter.

So far, no message or document hacked from the New York-based Clinton Foundation has surfaced in public, the sources said.

One of the sources and two U.S. security officials said that like hackers who targeted the Democratic National Committee, Hillary Clinton's presidential campaign and the Democrats' congressional fundraising committee, the hackers appear to have used "spear phishing" techniques to gain access to the foundation's network.

These techniques include creating bogus emails or websites in an effort to gain access to Clinton Foundation staffers' emails and then to the foundation itself.

Speaking on the condition of anonymity, the U.S. officials said the hackers used the same techniques Russian intelligence agencies or their proxies employed against the Democratic Party groups, which suggests that Russians also attacked the foundation.

Kremlin officials dismissed as absurd the allegations of Moscow's involvement, which were made last month amid political party nominating conventions for the Nov. 8 election.

Neither former White House Counsel Kathryn Ruemmler, the Clinton Foundation's principal lawyer, nor a spokeswoman for

the foundation responded to requests for comment on the hacking and the precautions the organization has taken.

Officials with FireEye said the company could not discuss its clients.

Although no documents have emerged, the attacks have left some Democrats and Clinton campaign officials worried that the hackers might have obtained emails and voice messages that could be used to reinforce Republican charges that donors to the Clinton Foundation were rewarded with access to Clinton and her aides while she was secretary of state or to her husband, former President Bill Clinton.

Another concern: hackers or outlets such as the anti-secrecy WikiLeaks website could release documents and emails damaging to her presidential campaign, several people familiar with the foundation's activities said.

The Democratic Congressional Campaign Committee convened a closed-door meeting on Wednesday to discuss best cyber security practices.

The meeting, according to people familiar with it, included a recommendation that staff and lawmakers change their phone numbers and email addresses if that information was published online by hackers believed to be working for or with Russian intelligence agencies.

One of the U.S. officials said, however, that the spear phishing pattern used against several organizations, appears to reinforce the intelligence community's "preliminary assessment" that the attacks were intended more for espionage than for trying to influence the U.S. presidential election.

So far, said a third U.S. official familiar with the attacks, there is no evidence that the hackers were able to follow any of the hacked emails into the State Department's classified email systems.

Anxiety in Washington over the possibility that a foreign power might be using hacked information to meddle in the U.S. election has prompted some Democrats and cyber security experts to urge the Obama administration to blame Russia publicly.

Rep. Jim Himes, a Democrat on the House of Representatives intelligence committee, said the United States should carry “a big stick” in cyber security matters. “The U.S. government needs to be very clear, very direct, and hold these people accountable.”

Current and former White House and intelligence officials said the Obama administration is unlikely to blame Russia publicly, given the difficulty of attributing the attacks without revealing American sources and methods, the geopolitical concerns at play, and a fear that doing so could risk aggravating cyber conflict.