ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

January 15, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On Thursday, the Committee is scheduled to hold its latest hearing on the security of the Healthcare.gov website. I am writing to raise concerns and propose Committee action on three requests so that Committee Members will be able to conduct this hearing in a responsible and bipartisan manner that does not jeopardize the security of the website or the personal information of American citizens.

Lack of Committee Protocol to Safeguard Sensitive Documents

On several occasions since November, I have written to you to request that we meet to discuss the adoption of a bipartisan protocol to safeguard sensitive documents obtained during this investigation and to develop a responsible approach to making information public that the Committee determines is important to its investigation.[1]

My concerns are based on explicit and repeated warnings by the MITRE Corporation, which conducted security testing on the Healthcare.gov website. MITRE officials warned in four different letters to the Committee—on November 5, November 22, December 4, and December 13—that the documents it produced to the Committee include software code and other technical information that is highly sensitive and could give hackers a roadmap to compromise the security of the website and the personal information of consumers.[2]

---

[1] *See, e.g.,* Letter from Ranking Member Elijah E. Cummings to Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Nov. 6, 2013).

[2] Letter from Kathleen Golden, Government Relations Manager, MITRE Corporation, to Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Nov. 5, 2013); Letter from Sol Glasner, Vice President, General Counsel, MITRE Corporation, to Counsel for Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Nov. 22, 2013); Letter from Alfred Grasso, President and Chief Executive Officer, MITRE Corporation, to Chairman Darrell E. Issa, House Committee on Oversight and Government

When MITRE produced these documents to the Committee in unredacted form on December 13, 2013, the company's President and Chief Executive Officer warned:

> In the wrong hands, this information could cause irreparable harm to the basic security architecture of HealthCare.gov and potentially to the security of other CMS data networks that share attributes of this architecture. The resulting potential for risk to the privacy of Americans' personal information is the reason that MITRE remains concerned about disclosure of the previously redacted information.[3]

Despite multiple requests and MITRE's repeated warnings, you have not responded to any of my inquiries. As a result, Committee Members participating in Thursday's hearing have no protocol in place to help them determine which documents may be used in open session and which documents should be protected to prevent against attacks by domestic hackers, foreign entities, and other seeking to harm our national interests. This lack of clear guidance creates an unnecessary risk of accidental or inadvertent disclosures that otherwise could be avoided.

I also remain concerned with the unilateral release by your office of partial transcripts and select document excerpts to promote partisan narratives that often turn out to be inaccurate, particularly when these releases are not part of any official report, correspondence, or other Committee action. Not only is this a disservice to the American people and the goals we share, but it undermines the credibility and integrity of the Committee.

One option for the Committee would be to consider adopting the document protocol approved by the Committee when Rep. Dan Burton was Chairman and Rep. Henry Waxman was Ranking Member. In 1998, after significant deliberation among the majority and minority, the Committee proceeded as I am proposing now and adopted a protocol for handling sensitive documents obtained during its investigation of the Clinton Administration's campaign finance activities.[4] Although I am open to additional suggestions, I see no reason you should have objections to the process adopted by former Chairman Burton.

Reform (Dec. 4, 2013); Letter from Alfred Grasso, President and Chief Executive Officer, MITRE Corporation, to Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Dec. 13, 2013).

[3] Letter from Alfred Grasso, President and Chief Executive Officer, MITRE Corporation, to Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Dec. 13, 2013). Another security contractor, Blue Canopy, provided similar warnings when it produced sensitive security documents pursuant to a subpoena from the Committee. *See, e.g.,* Letter from Barbara "Biz" Van Gelder, Dickstein Shapiro, LLP, Counsel for Blue Canopy, to Chairman Darrell E. Issa, House Committee on Oversight and Government Reform (Jan. 10, 2014) ("These unredacted and unencrypted documents are highly sensitive and, as such, we request confidential treatment of these documents since release of them could be misused to develop a targeted intrusion strategy placing the entire healthcare.gov website in jeopardy as well as other CMS data networks that share the attributes of the website's architecture.") (emphasis added).

[4] House Committee on Government Reform and Oversight, *Protocol for Documents* (June 23, 1998) (online at

Lack of Policy on Securing Sensitive Information in Committee's Possession

Another concern is the security of documents in the custody of the Committee. Currently, the Committee has no procedure governing the storage and handling of these sensitive documents. As a result, there have been two separate occasions last week when sensitive documents were left unattended in unlocked rooms accessible by the public. Although I understand that your office believes these documents are not sensitive, one was produced to the Committee in encrypted, password-protected format, and both were marked as sensitive documents that require special handling.

To address this issue, the Committee could consider applying to these sensitive documents the same protections that are currently utilized by the House of Representatives to safeguard its own information. The Committee on House Administration has issued a Security Policy for the Protection of Sensitive Information that sets forth policies to "protect the confidentiality of sensitive information from disclosure to unauthorized individuals or groups." These policies address the physical protection of sensitive information, the electronic protection of sensitive information, personnel precautions, and the disposal of sensitive information.[5]

Lack of Information about Outside Individuals Given Access to Sensitive Information

A third concern relates to providing access to sensitive information to individuals outside the Committee. In December, you stated that you intended to "consult carefully with non-conflicted experts to ensure no information is released that could further jeopardize the website's security."[6] Several days later, you wrote a letter to the Department of Health and Human Services indicating that you had already begun this process, stating that you would "continue" consulting with outside security experts.[7]

Based on your statements, it is unclear who these outside experts are, who they work for, and who they may be affiliated with, raising concerns about what they may do with the information. If they do not work for the government or any of its contractors, it is unclear what contractual or other restrictions they are under not to disclose this sensitive information further.

---

http://democrats.oversight.house.gov/uploads/Burton%20Document%20Protocol%2006-23-98.pdf).

[5] Committee on House Administration, *The United States House of Representatives Information Security Policy for the Protection of Sensitive Information* (HISPOL 010.0) (Jan. 2010).

[6] *Dems Want Briefing on Issa Docs,* The Hill (Dec. 16, 2013) (online at http://thehill.com/blogs/healthwatch/health-reform-implementation/193254-dems-want-briefing-on-issa-docs).

[7] Letter from Chairman Darrell E. Issa, House Committee on Oversight and Government Reform, to The Honorable Kathleen Sebelius, Secretary, Department of Health and Human Services (Dec. 17, 2013) (online at http://oversight.house.gov/wp-content/uploads/2013/12/2013-12-17-DEI-to-Sebelius-re-Security-Testing.pdf).

There have been multiple reports about organizations and individuals who are deliberately targeting the Healthcare.gov website for malicious purposes.[8] The risk that this information could get into the wrong hands increases dramatically as more individuals gain access to it, particularly when these individuals are under no obligation to safeguard it.

To address these concerns, I request that you provide Committee Members with the identities of individuals who are not employed by the Committee who have been granted access to this sensitive information, as well as copies of any confidentiality agreements these individuals entered into in order to protect the sensitive information in these documents.

Conclusion

I believe our Committee acts with greatest authority and credibility when it proceeds in a bipartisan manner. For this reason, I hope you will join me in developing bipartisan protocols to help Committee Members conduct Thursday's hearing and the broader investigation in a responsible manner. Thank you for your consideration of this request.

Sincerely,

Elijah E. Cummings
Ranking Member

[8] *See, e.g., Hackers Threaten Destruction of Website,* InformationWeek (Nov. 8, 2013) (online at www.informationweek.com/security/vulnerabilities-and-threats/hackers-threaten-destruction-of-obamacare-website/d/d-id/1112207?).