FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

December 13, 2013

To: Subcommittee on Oversight and Investigations Democratic Members and Staff

Fr: Reps. Henry A. Waxman and Diana DeGette

Re: Briefing on Healthcare.gov Security Issues

I. BACKGROUND

Members have raised questions about data security on the Healthcare.gov website at recent Committee hearings. In response to these concerns, Department of Health and Human Services (HHS) officials and website security contractors have described the security procedures in place and have expressed confidence in overall system security of Healthcare.gov.

On December 11, in order to address ongoing questions, Committee members and staff received a classified briefing from Dr. Kevin Charest, the HHS Chief Information Security Officer, and Ned Holland, HHS Assistant Secretary for Administration. Portions of this briefing were classified to protect information relevant to national security. This memo contains a summary of the unclassified portion of the briefing.

II. HEALTHCARE.GOV SECURITY INCIDENTS

The briefing revealed that there have been no successful security attacks on Healthcare.gov. According to Dr. Charest, no person or group has hacked into Healthcare.gov, and no person or group has maliciously accessed any personally identifiable information from users.

HHS reported that there have been a total of 32 Healthcare.gov Information Security Incidents. These are events that rise to a level where they are investigated and addressed if necessary. Eleven of these incidents are still under investigation.

Of the remaining 21 events, three were classified as non-incidents, reports that ultimately turned out to be of no concern.

One of the events involved an attempted probe or scan of the system. This scan was not successful, and additional steps were taken to prevent further attempts.

Two events were classified as "inappropriate usage," involving the violation of acceptable computing use policies. One such effort has been made public: a denial of service attempt using malware named "Destroy Obamacare."[1]

Fifteen events were classified as "unauthorized access." These involve incidents where an individual accidentally gained unauthorized access to information. These 15 events were isolated in nature and generally involved glitches in computing code. In one example that has been made public, a South Carolina man's personal information was inadvertently sent to another individual in North Carolina.[2] None of these events involved a significant breach of personal information. All the known glitches that caused these incidents have been fixed.

The information provided in the briefing was reassuring. The security of Healthcare.gov has not been breached, and hackers have had no access to personally identifiable information. HHS officials indicated that they were conducting 24-7 system monitoring and ongoing assessments in order to ensure and strengthen system security.

[1] See, e.g., *The New Hacking Tool: Destroy Obamacare*, Bloomberg (Nov. 14, 2013) (online at http://www.bloomberg.com/video/the-new-hacking-tool-destroy-obamacare-PDBJSXi9Tk6Of68QLrkUJg.html)

[2] *Healthcare.gov Official Questioned about Website Security*, McClatchy (Nov. 5, 2013) (online at http://www.mcclatchydc.com/2013/11/05/207568/healthcaregov-official-questioned.html).