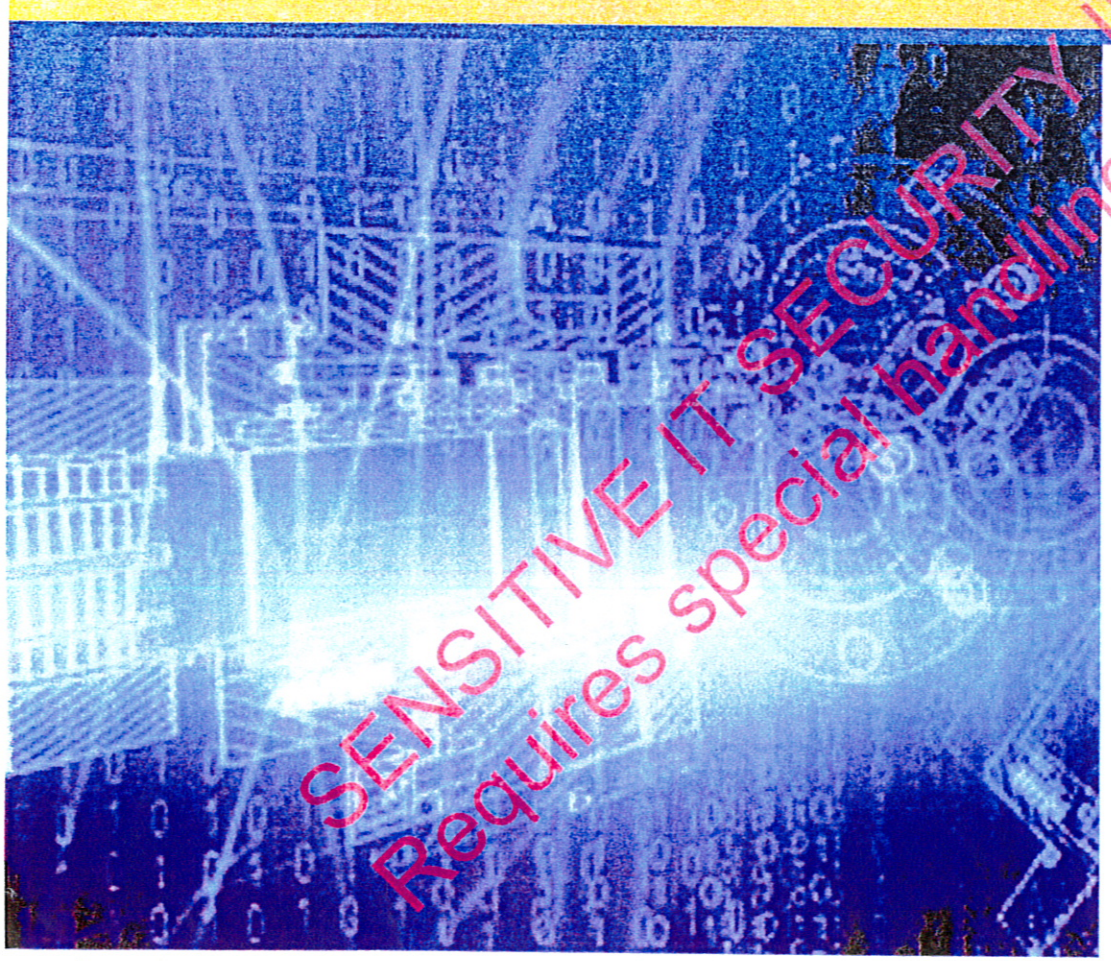
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

Marketplace Security Briefing



September 23, 2013

HIM, I&A, FM and PM Applications

- Full SCA testing was not performed (not all controls tested)
- August and September 2013 assessments did not assess functionally complete versions of these applications in same environment
- SCA testers were unable to adequately test the confidentiality and integrity of applications, including end-to-end testing
- Majority of SCA testing efforts were focused on testing the expected functionality, not security testing
- Testing environments and module interconnections not ready for SCA testing and was inconsistent. Need a dedicated environment to perform tests, such as Denial of Service exploits
- Known functionality was deemed out of scope and not tested, only partial completion of SCA testing scheduled for September 27 (Call Center UI, Notices & Mailing)

Risks:

- Unknown risk of applications to withstand attacks aimed at system availability – high risk
- Unknown risks associated with those controls and those functionalities that were not tested – high risk
- Risk of code being released into production and available to the public, which is not functionally complete or security tested
- Risk of being vulnerable to attacks [redacted]
- [redacted]

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

December 16, 2013

The Honorable Darrell Issa
Chairman
Committee on Oversight and Investigation
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In follow-up to a specific request from Committee staff, we are enclosing a copy of a written presentation dated September 23, 2013, reflecting the status, at that time, of certain security measures being taken in connection with the Federally-facilitated Marketplace (FFM) and the Data Services Hub (Hub).

Please note that the enclosed document includes certain information also contained in one of the Security Control Assessments (SCAs) that the MITRE Corporation (MITRE) previously produced to the Committee, in redacted form and more recently, in response to the Committee's subpoena, in unredacted form. As MITRE has emphasized to the Committee on a number of occasions, even the unredacted portions of the redacted SCAs it produced contain highly sensitive information that could put the Information Technology (IT) systems at risk if further released. As the Department of Health and Human Services (HHS) has made clear in prior correspondence with the Committee, we share MITRE's concerns about the risks and responsibilities assumed in connection with both the unredacted and redacted SCAs, and related material such as the enclosed Powerpoint.

Specifically, our concern is not the current security status of the Federal IT systems involved, but future security risks assumed in the event of further disclosure. As we have previously advised, documents such as the SCAs and the material we are concurrently transmitting by encrypted email could provide a roadmap for malicious actors seeking to compromise Federal IT systems and/or gain access to personally identifiable information, and could expose some of the most sensitive sites the Federal government operates to cyber attack. We therefore respectfully reiterate our previous requests that the Committee not further disseminate this type of material, and our request to discuss with the Committee ways to protect the highly sensitive information now in your possession.

Since we are sending this document individually and without additional context, we wanted to provide some relevant background information on states' connections to the Hub that is not included in this document. Each state that was connected either had received an authority to connect (ATC), or was granted a 60-day ATC. States that were not connected to the Hub were able to verify eligibility for the Medicaid and CHIP programs through the customary process they had been using for years prior to October 1. States verified income, citizenship and immigration status by secure, electronic exchanges of information with the Department of Homeland Security, the Social Security Administration and the Internal Revenue Service.

Please also note that the transmittal of this information follows up on the Committee's October 10, 2013 and October 24, 2013 letters, and the Committee's October 30, 2013 subpoena regarding the Health Insurance Marketplace. We continue to identify responsive documents and are providing the Committee with a rolling production of responsive documents. Since the Affordable Care Act became law, HHS and the Centers for Medicare & Medicaid Services (CMS) have worked diligently to accommodate numerous and far-reaching Congressional oversight requests regarding the Affordable Care Act, including from your Committee, and continue to do so. Since the Act became law, HHS and CMS have provided agency staff dozens of Committee interviews and briefings on a wide array of topics. HHS officials have testified at more than two dozen Congressional hearings, including ten in the last two months, and have produced tens of thousands of pages of documents on Affordable Care Act-related matters to Congress in response to Congressional oversight requests.

We are also working with your staff to accommodate the Committee's pending and new requests for transcribed interviews with additional numbers of CMS officials. In order for us to make each of these officials and staff members available, we must ask them to take time away from their official duties – which in most cases involve working on improvements to the website – in order to accommodate the Committee's various oversight interests. We remain willing to continue working with the Committee to accommodate its continuing oversight interests. As noted in our letter of December 13, we are also anxious to discuss protocols for the handling of the sensitive IT security documents in the Committee's possession, and with respect to those you continue to seek so that the Committee's legitimate oversight may be accommodated and the IT assets involved may continue to be protected.

Sincerely,

Jim R. Esquea
Assistant Secretary for Legislation

Enclosure

cc: The Honorable Elijah Cummings
Ranking Member