United States Government Accountability Office

Testimony
Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 11:00 a.m. ET
Thursday, September 18, 2014

HEALTHCARE.GOV

Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses

Statement of Gregory C. Wilshusen, Director, Information Security Issues

GAO Highlights

Highlights of GAO-14-871T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

PPACA requires the establishment of health insurance marketplaces in each state to assist individuals in comparing, selecting, and enrolling in health plans offered by participating issuers. CMS is responsible for overseeing these marketplaces, including establishing a federally facilitated marketplace in states that do not establish their own. These marketplaces are supported by an array of IT systems, including Healthcare.gov, the website that serves as the consumer portal to the marketplace.

This statement is based on two September 2014 reports examining the security and privacy of the Healthcare.gov website and related systems. The specific objectives of this work were to (1) describe the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assess the effectiveness of programs and controls implemented by CMS to protect the security and privacy of the information and IT systems supporting Healthcare.gov.

What GAO Recommends

In its September 2014 reports GAO made 6 recommendations to HHS to implement security and privacy controls to enhance the protection of systems and information related to Healthcare.gov. In addition, GAO made 22 recommendations to resolve technical weaknesses in security controls. HHS agreed with 3 of the 6 recommendations, partially agreed with 3, agreed with all 22 technical recommendations, and described plans to implement them.

View GAO-14-871T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

September 18, 2014

HEALTHCARE.GOV

Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses

What GAO Found

Enrollment through Healthcare.gov is supported by the exchange of information among many systems and entities. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key information technology (IT) systems supporting Healthcare.gov. These include, among others, the Federally Facilitated Marketplace (FFM) system, which facilitates eligibility and enrollment, plan management, and financial management, and the Federal Data Services Hub, which acts as the single portal for exchanging information between the FFM and other systems or external partners. CMS relies on a variety of federal, state, and private-sector entities to support Healthcare.gov activities. For example, it exchanges information with the Department of Defense, Department of Homeland Security, Department of Veterans Affairs, Internal Revenue Service, Office of Personnel Management, Peace Corps, and the Social Security Administration to help determine applicants' eligibility for healthcare coverage and/or financial assistance. Healthcare.gov-related systems are also accessed and used by CMS contractors, issuers of qualified health plans, state agencies, and others.

While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put these systems and the sensitive personal information they contain at risk. Specifically, CMS established security-related policies and procedures for Healthcare.gov, including interconnection security agreements with the federal agencies with which it exchanges information. It also instituted certain required privacy protections, such as notifying the public of the types of information that will be maintained in the system. However, weaknesses remained in the security and privacy protections applied to Healthcare.gov and its supporting systems. For example, CMS did not

- ensure system security plans contained all required information, which makes it harder for officials to assess the risks involved in operating those systems;
- analyze privacy risks associated with Healthcare.gov systems or identify mitigating controls;
- perform comprehensive security testing of the FFM system, reducing assurance that security controls are operating as intended; and
- fully establish an alternate processing site for Healthcare.gov systems to ensure that they could be recovered in the event of a disruption or disaster.

In addition, a number of weaknesses in specific technical security controls jeopardized Healthcare.gov-related systems. These included certain systems supporting the FFM not being restricted from accessing the Internet and inconsistent implementation of security patches, among others.

An underlying reason for many of these weaknesses is that CMS did not establish a shared understanding of security roles and responsibilities with all parties involved in securing Healthcare.gov systems. Until these weaknesses are addressed, the systems and the information they contain remain at increased risk of unauthorized use, disclosure, modification, or loss.

Chairman Issa, Ranking Member Cummings, and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the implementation of the Patient Protection and Affordable Care Act (PPACA) and Healthcare.gov. As you know, PPACA requires the establishment of a health insurance marketplace in each state to assist consumers and small businesses in comparing, selecting, and enrolling in health plans offered by participating private insurers. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) is responsible for overseeing the establishment of these marketplaces, including creating a federally facilitated marketplace for states that do not establish their own. This marketplace is supported by an array of information technology (IT) systems, including Healthcare.gov, the website that provides the consumer portal to the marketplace, and related data systems.

To facilitate the enrollment process, Healthcare.gov and its supporting IT systems must collect and process individuals' sensitive personal information, such as employment and tax information. Portions of this information may be accessed by multiple organizations, including CMS, other federal agencies, insurers, and state agencies. Accordingly, ensuring the security and privacy of this information is critically important.

My statement today will summarize the key findings from our recently issued work on the privacy and security protections of the Healthcare.gov website and related IT systems.[1] Our specific objectives for that review were to (1) describe the planned exchanges of information between the Healthcare.gov website, supporting IT systems, and the federal, state, and other organizations that are providing or accessing that information, including special arrangements for handling tax information in compliance with legal requirements, and (2) assess the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov. More details on our scope and methodology are contained in the reports.

[1] GAO, *Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls*, GAO-14-730 (Washington, D.C.: Sept. 17, 2014). We issued a second report that had limited distribution because of the sensitive nature of the information it contained.

The work on this statement was based on was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

PPACA directed each state to establish a state-based health insurance marketplace[2] for individuals to enroll in private health insurance plans, apply for income-based financial assistance, and, as applicable, obtain a determination of their eligibility for other health coverage programs, such as Medicaid or the State Children's Health Insurance Program (CHIP). For states that did not establish a marketplace, PPACA required the federal government to establish and operate a marketplace for that state, referred to as the federally facilitated marketplace. For plan year 2014, 17 states elected to establish their own marketplace, and CMS operated a federally facilitated marketplace or partnership marketplace[3] for 34 states.[4]

The act required the marketplaces to be operational on or before January 1, 2014, and Healthcare.gov began facilitating enrollments on October 1, 2013, at the beginning of the first annual open enrollment period established by CMS. The initial open enrollment period ended on April 15, 2014.

[2] PPACA requires the establishment of health insurance exchanges—marketplaces where eligible individuals can compare and select among insurance plans offered by participating issuers of health coverage. In this statement, we use the term "marketplace."

[3] A partnership marketplace is a variation on the federally facilitated marketplace. HHS establishes and operates this type of exchange with states assisting HHS in carrying out certain functions of that marketplace.

[4] These numbers include the 50 states plus the District of Columbia.

Laws and Regulations Establish Requirements for Protecting the Security and Privacy of Personally Identifiable Information

Requirements for ensuring the security and privacy of individuals' personally identifiable information (PII),[5] such as that collected and processed by Healthcare.gov and related systems, have been established by a number of federal laws and guidance. These include the following:

- The Federal Information Security Management Act of 2002 (FISMA), which requires each federal agency to develop, document, and implement an agency-wide information security program.
- National Institute of Standards and Technology (NIST) guidance and standards, which are to be used by agencies to, among other things, categorize their information systems and establish minimum security requirements.
- The Privacy Act of 1974, which places limitations on agencies' collection, access, use, and disclosure of personal information maintained in systems of records.
- The Computer Matching Act, which is a set of amendments to the Privacy Act requiring agencies to follow specific procedures before engaging in computerized comparisons of records for establishing or verifying eligibility or recouping payments for federal benefit programs.
- The E-Government Act of 2002, which requires agencies to analyze how personal information is collected, stored, shared, and managed before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.
- The Health Insurance Portability and Accountability Act of 1996, which requires the adoption of standards for the electronic exchange, privacy, and security of health information.
- The Internal Revenue Code, which provides for the confidentiality of tax returns and return information.

[5] PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

- IRS Publication 1075, which establishes security guidelines for safeguarding federal tax return information used by federal, state, and local agencies.

HHS Responsibilities for Overseeing Implementation of PPACA and Ensuring Security and Privacy of Health Insurance Marketplaces

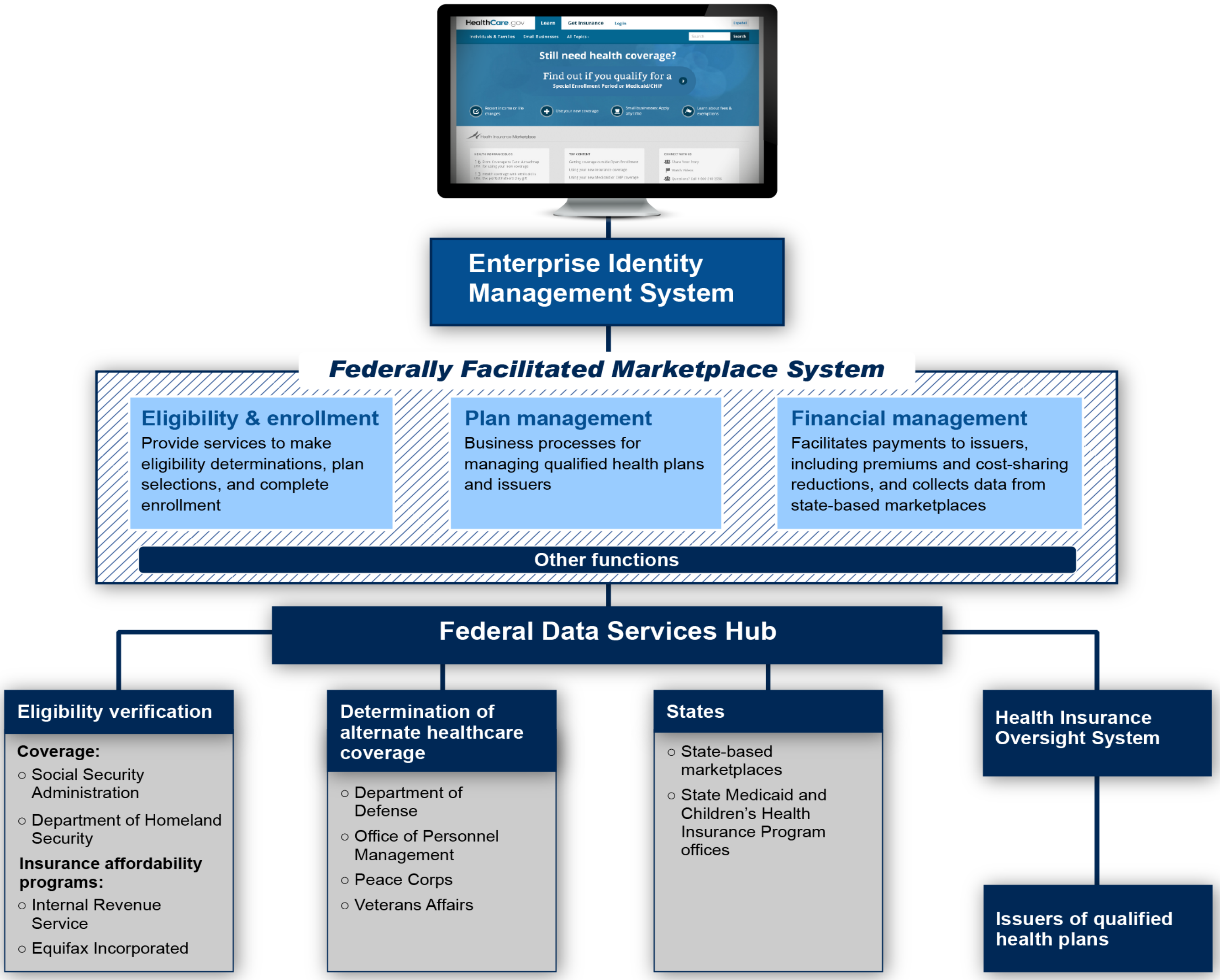
Under FISMA, the Secretary of HHS has overall responsibility for the department’s agency-wide information security program; this responsibility has been delegated to the department’s Chief Information Officer (CIO). The HHS CIO is also responsible for the department’s response to information security incidents and the development of privacy impact assessments for the department’s systems.

The CMS Center for Consumer Information and Insurance Oversight has overall responsibilities for federal systems supporting the federally facilitated marketplace and for overseeing state marketplaces. Further, security and privacy responsibilities for Healthcare.gov and supporting systems are shared among several offices and individuals within CMS, including the CIO, the Chief Information Security Officer, component-level information systems security officers, the CMS Senior Official for Privacy, and the CMS Office of e-Health Standards Privacy Policy and Compliance. In particular, the CMS CIO is responsible for implementing and administering the CMS information security program, which covers the systems developed by CMS to satisfy PPACA requirements. The Chief Information Security Officer is responsible for, among other things, ensuring the assessment and authorization of all systems and the completion of periodic risk assessments, including annual security testing and security self-assessments.

Marketplace Enrollment Is Facilitated by Data Exchanges among Many Interconnected Systems and Partners

The process of enrolling for insurance through Healthcare.gov is facilitated by a number of major systems managed by CMS. Figure 1 shows the major entities that exchange data in support of marketplace enrollment in qualified health plans and how they are connected.

Figure 1: Overview of Healthcare.gov and Its Supporting Systems



HealthCare.gov
Learn
Get Insurance
Log in
Still need health coverage?
Find out if you qualify for a Special Enrollment Period or Medicaid/CHIP
Enterprise Identity Management System
Federally Facilitated Marketplace System
Eligibility & enrollment
Provide services to make eligibility determinations, plan selections, and complete enrollment
Plan management
Business processes for managing qualified health plans and issuers
Financial management
Facilitates payments to issuers, including premiums and cost-sharing reductions, and collects data from state-based marketplaces
Other functions
Federal Data Services Hub
Eligibility verification
Coverage:
○ Social Security Administration
○ Department of Homeland Security
Insurance affordability programs:
○ Internal Revenue Service
○ Equifax Incorporated
Determination of alternate healthcare coverage
○ Department of Defense
○ Office of Personnel Management
○ Peace Corps
○ Veterans Affairs
States
○ State-based marketplaces
○ State Medicaid and Children's Health Insurance Program offices
Health Insurance Oversight System
Issuers of qualified health plans

Source: GAO analysis of CMS data. | GAO-14-871T

The major systems that facilitate enrollment include the following:

The Healthcare.gov website: This serves as the user interface for individuals to obtain coverage through a federally facilitated marketplace. It has two major functions: (1) providing information about PPACA health insurance reforms and health insurance options and (2) facilitating enrollment in coverage.

Enterprise Identity Management System: This system allows CMS to verify the identity of an individual applying for coverage and establish a login account for that user. Once an account is created using a name and e-mail address, the person's identity is confirmed using additional information, which can include a Social Security number, address, phone number, and date of birth.

Federally Facilitated Marketplace System (FFM): This system consists of three major modules to facilitate (1) eligibility and enrollment, (2) plan management, and (3) financial management. For eligibility, an applicant's information is collected to determine whether they are eligible for insurance coverage and financial assistance. Once eligibility is determined, the system allows the applicant to view, compare, select, and enroll in a qualified health plan. The plan management module is to provide state agencies and issuers of qualified health plans with the ability to submit, certify, monitor, and renew qualifying health plans. The financial management module is to facilitate payments to health insurers, among other things. From a technical perspective, the FFM system relies on "cloud-based" data processing and storage services from private-sector vendors.

Federal Data Services Hub: This system acts as a single portal for exchanging information between the FFM system and other systems or external partners, which include other federal agencies, state-based marketplaces, other state agencies, other CMS systems, and issuers of qualified health plans. The data hub supports, among other things, real-time eligibility queries, transfer of applicant and taxpayer information, exchange of enrollment information with plan issuers, monitoring of enrollment information, and submission of health plan applications.

Healthcare.gov-related activities are also supported by other CMS systems, including a data warehouse system to provide reporting and performance metrics; the Health Insurance Oversight System, which provides an interface for issuers of qualified health plans to submit information about qualifying health plans; and a general accounting system that handles payments associated with advance premium tax credits and cost-sharing reductions.

In addition, CMS relies on a variety of federal, state, and private-sector entities to support Healthcare.gov-related activities, and these entities exchange information with CMS's systems:

- Federal agencies such as the Social Security Administration (SSA), Department of Homeland Security (DHS), and Internal Revenue Service (IRS), along with Equifax, Inc. (a private-sector credit agency under contract with CMS) provide or verify information used in making determinations of a person's eligibility for coverage and financial assistance.

- The Department of Defense (DOD), Office of Personnel Management (OPM), Peace Corps, and Department of Veterans Affairs (VA) assist in determining whether a potential applicant has alternate means for obtaining minimum essential coverage.

- State-based marketplaces may rely on the FFM system for certain functions, and state Medicaid and CHIP agencies may connect to the FFM to exchange enrollment data, which are typically routed through CMS's data hub.

- In addition to accessing the plan management and financial management modules of the FFM, issuers of qualified health plans receive information from the system when an individual completes the application process.

- Agents and brokers may access the Healthcare.gov website on behalf of applicants.

- To facilitate offline, paper-based applications, CMS contracted with a private-sector company for intake, routing, review, and troubleshooting of paper applications for enrollment into health plans and insurance affordability programs.

CMS Established a Security and Privacy Program for Healthcare.gov and Related Systems, but Actions Are Needed to Resolve Weaknesses

While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put the personal information these systems collect, process, and maintain at risk of inappropriate modification, loss, or disclosure. The agency needs to take a number of actions to address these deficiencies in order to better protect individuals' personally identifiable information.

CMS established security-related policies and procedures for Healthcare.gov. Specifically, it

- assigned overall responsibility for securing the agency's information and systems to appropriate officials, including the agency CIO and Chief Information Security Officer, and designated information system security officers to assist in certifying particular CMS systems;
- documented information security policies and procedures to safeguard the agency's information and systems;
- developed a process for planning, implementing, evaluating, and documenting remedial actions to address identified information security deficiencies; and
- established interconnection security agreements with the federal agencies with which it exchanges information, including DOD, DHS, IRS, SSA, and VA; these agreements identify the requirements for the connection, the roles and responsibilities of each party, the security controls protecting the connection, the sensitivity of the data to be exchanged, and the required training and background checks for personnel with access to the connection.

In addition, CMS took steps to protect the privacy of applicants' information. For example, it

- published and updated a system-of-records notice for Healthcare.gov that addressed required information such as the types of information that will be maintained in the system and the external entities that may receive such information without affected individuals' explicit consent;
- developed basic privacy training for all staff and role-based training for staff who have access to PII while executing their routine duties; and
- established an incident-handling and breach response plan and an incident response team to manage responses to privacy incidents,

identify trends, and make recommendations to HHS to reduce risks to PII.

However, when Healthcare.gov was deployed in October 2013, CMS accepted increased security risks because of the following:

- CMS allowed four states to connect to the data hub even though they had not completed all CMS security requirements. These states were given a 60-day interim authorization to connect, because CMS officials regarded this as a mission-critical need. Subsequently, all four states addressed the weaknesses in their security assessments and were granted 3-year authorizations.

- CMS authorized the FFM system to operate even though all the security controls had not been tested for a fully integrated version of the system. This authority to operate was granted for 6 months, on the condition that a full security assessment was conducted within 60 to 90 days of October 1, 2013. In December 2013, an assessment of the eligibility and enrollment module was conducted. However, the plan management and financial management modules, which had not yet been fully developed, were not tested.

CMS Has Not Fully Implemented Security and Privacy Management Controls

Although CMS developed and documented security policies and procedures, it did not fully implement required actions before Healthcare.gov began collecting and maintaining PII from individual applicants:

- **System security plans were not complete.** While system security plans for the FFM and data hub incorporated most of the elements specified by NIST, each was missing or had not completed one or more relevant elements. For example, the FFM security plan did not define the system’s accreditation boundary, or explain why five of the security controls called for by NIST guidance were determined not to be applicable. Without complete system security plans, agency officials will be hindered in making fully informed judgments about the risks involved in operating those systems.

- **Interconnection agreements were not all complete.** CMS had not completed security documentation governing its interconnection with Equifax, Inc., but instead was relying on a draft data use agreement that had not been fully approved within CMS. This makes it more difficult for agency officials to ensure that adequate security controls are in place to protect the connection.

- **Privacy risks were not assessed.** In completing privacy impact assessments for the FFM and data hub, CMS did not assess risks associated with the handling of PII or identify mitigating controls to address such risks. Without such an analysis, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems.

- **Interagency agreements governing data exchanges were not complete.** CMS established computer matching agreements with DHS, DOD, IRS, SSA, and VA for its data exchanges to verify eligibility for healthcare coverage and premium tax credits; however, it had not established such agreements with OPM or the Peace Corps. This increases the risk that appropriate protections will not be applied to the PII being exchanged with these agencies.

- **Security testing was not complete.** While CMS has undertaken, through its contractors and at the agency and state levels, a series of security-related testing activities for various Healthcare.gov-related systems, these assessments did not effectively identify and test all relevant security controls prior to deploying the systems.

  For example, the assessments of the FFM did not include all the security controls specified by NIST and CMS, such as incident response controls and controls specified for physical and environmental protection. In addition, CMS could not demonstrate that it had tested all the security controls specified in the FFM's October 2013 security plan, and it did not test all the system's components before deployment or test them on the integrated system. Testing of all deployed eligibility and enrollment modules and plan management modules did not occur until March 2014, and as of June 2014 FFM testing remained incomplete. Without comprehensive testing, CMS lacks assurance that security controls for the FFM system are working as intended.

- **Alternate processing site was not fully established.** CMS developed and documented contingency plans for the FFM and data hub that identified activities, resources, responsibilities, and procedures needed to carry out operations during prolonged disruptions of the systems. It also established system recovery priorities, a line of succession based on the type of disaster, and specific procedures on how to restore both systems and their associated applications in the event of a disaster. However, although the contingency plans designated a site at which to recover the systems, this site had not been established. Specifically, according to

CMS, data supporting the FFM were being backed up at the recovery site, but backup systems are not otherwise supported there, limiting the facility's ability to support disaster recovery efforts.

Security Control Weaknesses Could Threaten Healthcare.gov Information and Systems

CMS did not effectively implement or securely configure key security controls on the systems supporting Healthcare.gov. For example:

- Strong passwords (i.e., passwords of sufficient length or complexity) were not always required or enforced on systems supporting the FFM. This increases the likelihood that an attacker could gain access to the system.
- Certain systems supporting the FFM were not restricted from accessing the Internet, increasing the risk that unauthorized users could access data from the FFM network.
- CMS did not consistently apply security patches to FFM systems in a timely manner, and several critical systems had not been patched or were no longer supported by their vendors. This increased the risk that servers supporting the FFM could be compromised through exploitation of known vulnerabilities.
- One of CMS's contractors had not properly secured its administrative network, which could allow for unauthorized access to the FFM network.

In addition to these weaknesses, we also identified weaknesses in security controls related to boundary protection, identification and authentication, authorization, and configuration management. Collectively, these weaknesses put Healthcare.gov systems and the information they contain at increased and unnecessary risk of unauthorized access, use, disclosure, modification, and loss.

CMS Had Not Established a Shared Understanding of How Security Was to Be Implemented for Healthcare.gov-Related Systems

The security weaknesses we identified occurred in part because CMS did not ensure that the multiple parties contributing to the development of the FFM system had a shared understanding of how security controls were to be implemented. Specifically, CMS and contractor staff did not always agree on how security controls for the FFM were to be implemented or who was responsible for ensuring they were functioning properly. For example, although CMS identified one subcontractor as responsible for managing firewall rules, this responsibility was not included in the subcontractor's statement of work, and staff for the subcontractor said that this was the responsibility of a different contractor. Without ensuring agreement on security roles and responsibilities, CMS has less assurance that controls will function as intended, increasing the risk that attackers could compromise the system and the data it contains.

CMS Should Act to Improve Security and Privacy Protections for Healthcare.gov

In our September 2014 report, we made the following six recommendations aimed at improving the management of the security of Healthcare.gov:

1. Ensure that system security plans for the FFM and data hub contain all information recommended by NIST.
2. Ensure that all privacy risks associated with Healthcare.gov are analyzed and documented in privacy impact assessments.
3. Develop computer matching agreements with OPM and the Peace Corps to govern data that are being compared with CMS data to verify eligibility for advance premium tax credits and cost-sharing reductions.
4. Perform a comprehensive security assessment of the FFM, including the infrastructure, platform, and all deployed software elements.
5. Ensure that the planned alternate processing site for the systems supporting Healthcare.gov is established and made operational in a timely fashion.
6. Establish detailed security roles and responsibilities for contractors, including participation in security control reviews, to better ensure effective communication among individuals and entities with responsibility for the security of the FFM and its supporting infrastructure.

In an associated report with limited distribution, we also made 22 recommendations to resolve technical security weaknesses related to access controls, configuration management, and contingency planning.

Implementing these recommendations will enable HHS and CMS to better ensure that Healthcare.gov systems and the information they collect and process are effectively protected from threats to their confidentiality, integrity, and availability.

In its comments on our draft reports, HHS concurred with 3 of the 6 recommendations to fully implement its information security program, partially concurred with the remaining 3 recommendations, and concurred with all 22 of the recommendations to resolve technical weaknesses in security controls, describing actions it had under way or planned related to each of them.

In conclusion, Healthcare.gov and its related systems represent a complex system of systems that interconnects a broad range of federal agency systems, state agencies and systems, and other entities, such as contractors and issuers of health plans. Ensuring the security of such a system poses a significant challenge. While CMS has taken important steps to apply security and privacy safeguards to Healthcare.gov and its supporting systems, significant weaknesses remain that put these systems and the sensitive, personal information they contain at risk of compromise. Given the complexity of the systems and the many interconnections among external partners, it is particularly important to analyze privacy risks, effectively implement technical security controls, comprehensively test the security controls over the system, and ensure that an alternate processing site for the systems is fully established.

Chairman Issa, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be pleased to answer any questions you have.

Contact and Staff Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Other key contributors to this testimony include John de Ferrari, Lon Chin, West Coile, and Duc Ngo (assistant directors); Mark Canter; Marisol Cruz; Sandra George; Nancy Glover; Torrey Hardee; Tammi Kalugdan; Lee McCracken; Monica Perez-Nelson; Justin Palk; and Michael Stevens.

(311329)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.