United States Government Accountability Office

Report to Congressional Requesters

September 2014

HEALTHCARE.GOV

Actions Needed to Address Weaknesses in Information Security and Privacy Controls

HEALTHCARE.GOV

Actions Needed to Address Weaknesses in Information Security and Privacy Controls

Why GAO Did This Study

PPACA required the establishment of health insurance marketplaces to assist individuals in obtaining private health insurance coverage. The Department of Health and Human Services' CMS is responsible for overseeing the establishment of these marketplaces, including creating the website for obtaining coverage. The marketplaces became operational on October 1, 2013. As requested, this report examines the security and privacy of the Healthcare.gov website.

GAO (1) describes the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assesses 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. GAO compared the implementation of controls over Healthcare.gov's supporting systems with privacy and security requirements and guidelines. This is a public version of a limited official use only report that GAO issued in September 2014. Certain information on technical issues has been omitted from this version.

What GAO Recommends

GAO is making six recommendations to implement security and privacy management controls to help ensure that the systems and information related to Healthcare.gov are protected. HHS concurred but disagreed in part with GAO's assessment of the facts for three recommendations. However, GAO continues to believe its recommendations are valid, as discussed in the report.

What GAO Found

Many systems and entities exchange information to carry out functions that support individuals' ability to use Healthcare.gov to compare, select, and enroll in private health insurance plans participating in the federal marketplaces, as required by the Patient Protection and Affordable Care Act (PPACA). The Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key federal systems supporting Healthcare.gov, including the Federally Facilitated Marketplace (FFM) system, which contains several modules that perform key functions related to health plan enrollment, and the Federal Data Services Hub (data hub), which provides connectivity between the FFM and other state and federal systems. CMS is also responsible for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other federal agencies, including the Department of Defense, Department of Homeland Security, Internal Revenue Service, Office of Personnel Management, Peace Corps, Social Security Administration, and the Department of Veterans Affairs also play key roles in maintaining systems that connect with CMS systems to perform eligibility-checking functions. Finally, a number of commercial entities, including CMS contractors, participating issuers of qualified health plans, agents, and others also connect to the network of systems that support enrollment in Healthcare.gov.

While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain both in the processes used for managing information security and privacy as well as the technical implementation of IT security controls. CMS took many steps to protect security and privacy, including developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. However, Healthcare.gov had weaknesses when it was first deployed, including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions. While CMS has taken steps to address some of these weaknesses, it has not yet fully mitigated all of them. In addition, GAO identified weaknesses in the technical controls protecting the confidentiality, integrity, and availability of the FFM. Specifically, CMS had not: always required or enforced strong password controls, adequately restricted access to the Internet, consistently implemented software patches, and properly configured an administrative network. An important reason that all of these weaknesses occurred and some remain is that CMS did not and has not yet ensured a shared understanding of how security was implemented for the FFM among all entities involved in its development. Until these weaknesses are fully addressed, increased and unnecessary risks remain of unauthorized access, disclosure, or modification of the information collected and maintained by Healthcare.gov and related systems, and the disruption of service provided by the systems.

_____ **United States Government Accountability Office**

Contents

Abbreviations

CCIIO	Center for Consumer Information and Insurance Oversight
CHIP	State Children's Health Insurance Program
CMS	Centers for Medicare & Medicaid Services
data hub	Federal Data Services Hub
DHS	Department of Homeland Security
DOD	Department of Defense
FFM	Federally Facilitated Marketplace
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IT	information technology
MIDAS	Multidimensional Insurance Data Analytics System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	privacy impact assessment
PII	personally identifiable information
PPACA	Patient Protection and Affordable Care Act
SSA	Social Security Administration
VA	Department of Veterans Affairs

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

September 16, 2014

Congressional Requesters

The Patient Protection and Affordable Care Act (PPACA),[1] signed into law on March 23, 2010, is intended to reform aspects of the private health insurance market and expand the availability and affordability of health care coverage. It requires the establishment of a health insurance marketplace[2] in each state[3] to assist consumers and small businesses in comparing, selecting, and enrolling in health plans offered by participating private issuers of qualified health plans. 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 in states not establishing their own. CMS staff have worked with a variety of contractors to develop, test, and maintain information technology (IT) systems to support the federally facilitated marketplace. Healthcare.gov is the website that provides a consumer portal to these marketplaces and the related data systems supporting eligibility and enrollment.

The security and privacy of personally identifiable information (PII)[4] that is collected and processed by the Healthcare.gov website and supporting IT systems are critically important. Large numbers of individuals submit extensive amounts of sensitive information, such as employment and wage information, portions of which may be accessed by multiple organizations including CMS, other federal agencies, issuers of qualified health plans, and state agencies. Healthcare.gov and other state-based

---

[1]Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152,124 Stat.1029 (Mar. 30, 2010). In this report, references to PPACA include all amendments made by the Health Care and Education Reconciliation Act.

[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 report, we use the term marketplace.

[3]In this report, the term "state" includes the District of Columbia.

[4]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.

marketplaces began facilitating enrollment on October 1, 2013. CMS has reported that over 8 million individuals applied for healthcare coverage through a state-based marketplace or the federally facilitated marketplace between October 1, 2013 and March 31, 2014.[5] The Congressional Budget Office has estimated that about 25 million people will enroll by 2022.[6]

Given the high degree of Congressional interest in examining the development, launch, and other issues associated with accessing the federal marketplace through Healthcare.gov, GAO is conducting a body of work in order to assist Congress with its oversight responsibilities. Several GAO reviews are currently underway. You requested that we examine the security and privacy of the Healthcare.gov website and its supporting systems at CMS. Our specific objectives 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 the 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.

This is a public version of a limited official use only report we issued in September 2014. Certain information has been omitted. Although the information provided in this report is more limited in scope, it addresses the same objectives as the limited official use only report. Also, the overall methodology used for both reports is the same.

To describe the planned exchanges of information between Healthcare.gov and federal and state organizations, we reviewed PPACA and other relevant laws to identify the responsibilities of CMS and other federal agencies for establishing and participating in health insurance marketplaces. We reviewed and analyzed CMS system and security documentation, including interagency security agreements, with each

---

[5]This number includes individuals who enrolled during the special enrollment period through April 19, 2014.

[6]Congressional Budget Office, *Updated Estimates of the Effects of the Insurance Coverage Provisions of the Affordable Care Act, April 2014* (Washington, D.C.: April 2014).

federal partner in order to identify interconnections between Healthcare.gov and other external partners that are providing or accessing information to support implementation of Healthcare.gov. Further, we obtained documentation and interviewed officials at the following federal agencies that are responsible for supporting implementation of Healthcare.gov: the Department of Defense (DOD), the Department of Homeland Security (DHS), the Internal Revenue Service (IRS), the Office of Personnel Management (OPM), the Peace Corps, the Social Security Administration (SSA), and the Department of Veterans Affairs (VA). We also obtained information and interviewed officials at Experian Information Solutions, which provides services to CMS to support Healthcare.gov. Based on an analysis of the information we received, we described the major types of data connections that are currently in place or planned between systems maintained by CMS to support Healthcare.gov and other internal and external systems. We also reviewed requirements in the Internal Revenue Code and PPACA regarding the disclosure of tax return information to carry out marketplace eligibility determinations to describe how IRS and CMS policies and procedures for sharing tax data adhere to legal requirements.

To 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, we compared the CMS's documented policies, procedures, and practices to the provisions and requirements contained in relevant privacy and information security laws and additional security management criteria, specifically National Institute of Standards and Technology (NIST) standards and guidelines. We also assessed the implementation of controls over Healthcare.gov's supporting systems and interconnections by examining risk assessments, security plans, security control assessments, contingency plans, and remedial action plans. Specifically, we observed controls over the Federally Facilitated Marketplace (FFM) system, including its supporting software, the operating systems, network and computing infrastructure provided by the supporting platform as a service, and infrastructure as a service systems. We performed our work at CMS headquarters in Baltimore, Maryland; and at contractor facilities in Dallas, Texas; and Reston and Chantilly, Virginia.

We conducted this performance audit from December 2013 to September 2014 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. A full description of our objectives, scope, and methodology can be found in appendix I.

Background

PPACA directed each state to establish a state-based health insurance marketplace by January 1, 2014.[7] These marketplaces were intended to provide a seamless, single point-of-access for individuals to enroll in private health plans, apply for income-based financial assistance established under the law, and, as applicable, obtain an eligibility determination for other health coverage programs, such as Medicaid or the State Children's Health Insurance Program (CHIP).[8]

In states electing not to establish and operate a marketplace, PPACA required the federal government to establish and operate a marketplace in that state, referred to as the federally-facilitated marketplace. Thus, the federal government's role for any given state—whether it established a marketplace or oversees a state-based marketplace—was dependent on a state decision. For plan year 2014, 17 states elected to establish their own marketplace, while CMS operated a federally-facilitated marketplace or partnership marketplace[9] for 34 states. Figure 1 shows the states and the types of marketplaces they use.

---

[7]PPACA, § 1311(b)(1), 124 Stat. at 173.

[8]Medicaid is a joint federal-state program that finances health care coverage for certain low-income individuals. CHIP is a federal-state program that provides health care coverage to children 19 years of age and younger living in low-income families whose incomes exceed the eligibility requirements for Medicaid.

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

Figure 1: Type of Health Insurance Marketplace Used by States for Plan Year 2014
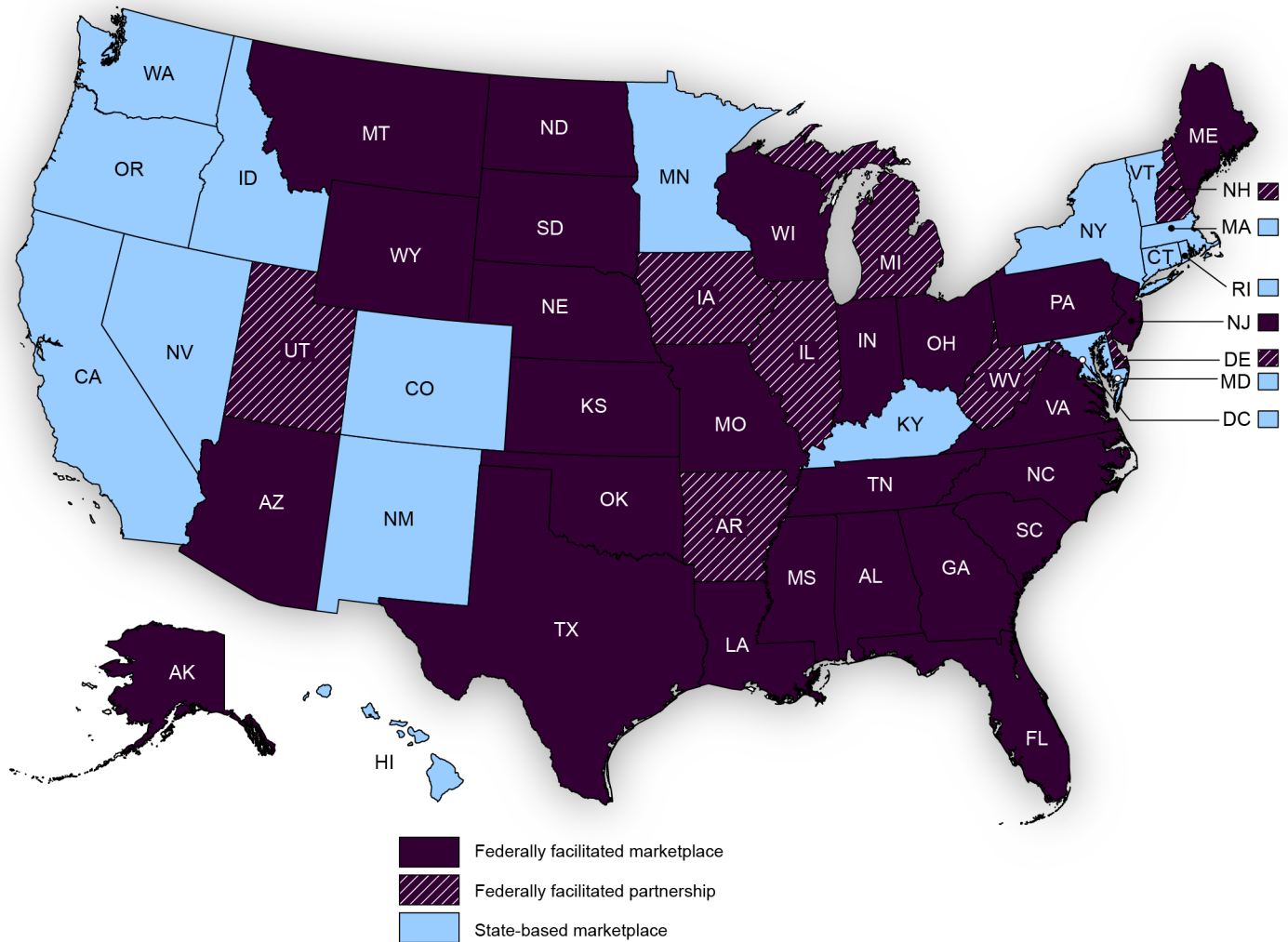
Sources: GAO analysis of CMS data; Map Resources (map). | GAO-14-730

PPACA required state and federal marketplaces to be operational on or before January 1, 2014. Healthcare.gov, the public interface for the federally facilitated marketplace, began facilitating enrollments on October 1, 2013, at the beginning of the first annual open enrollment period established by CMS. This open enrollment period closed on March 31, 2014; however the government granted short extensions on an individual basis to those who had begun, but not completed, their application. According to CMS, the extension was granted due to the

volume of applicants. No applications for the initial enrollment period were accepted after April 15, 2014.[10]

Laws and Regulations Set Requirements for Ensuring the Security and Privacy of Personally Identifiable Information

Federal laws and guidance specify requirements for protecting federal systems and data. This includes systems used or operated by a contractor or other organization on behalf of a federal agency. The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or another organization on behalf of an agency.

FISMA assigns certain responsibilities to NIST, which is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

Accordingly, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing information security programs. Relevant publications include:

- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[11] requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values

---

[10]Most state-based marketplaces followed the federal guidelines regarding individuals who started the process before March 30, 2014 but could not finish, allowing applicants to complete the application and select a plan by April 15, 2014. Other states, including Colorado, Nevada, Oregon, and Maryland allowed consumers additional time beyond April 15, 2014, to complete the enrollment process and obtain coverage in 2014.

[11]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: Feb. 2004).

assigned to the respective security objectives are the highest values from among the security categories that the agency identifies for each type of information resident on those information systems.

- Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*,[12] specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these minimum security requirements.

- Federal Information Processing Standard 140-2, Security *Requirements for Cryptographic Modules*,[13] requires agencies to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. This standard specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.

- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*,[14] provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The guidance includes privacy controls to be used in conjunction with the specified security controls to achieve comprehensive security and privacy protection.

- NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security*

---

[12]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[13]NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May, 2001).

[14]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

Life Cycle Approach, explains how to apply a risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

- NIST Special Publication 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems* (draft),[15] recommends steps to help develop a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure. While agencies are not yet required to follow these draft guidelines, they establish a benchmark for effectively coordinating security efforts across complex interconnected systems, such as those that support Healthcare.gov.

While agencies are required to use a risk-based approach to ensure that all of their IT systems and information are appropriately secured, they also must adopt specific measures to protect PII and must establish programs to protect the privacy of individuals whose PII they collect and maintain. Agencies that collect or maintain health information also must comply with additional requirements. In addition to FISMA, major laws and regulations[16] establishing requirements for information security and privacy in the federal government include:

- **The Privacy Act of 1974**[17] places limitations on agencies' collection, access, use, and disclosure of personal information maintained in systems of records. The act defines a "record" as any item, collection,

---

[15]NIST, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, SP 800-160, draft, (Gaithersburg, Md.: May, 2014).

[16]Regulations also establish security and privacy requirements that are applicable to the marketplaces or Healthcare.gov-related contracts. For example, in March 2012, CMS issued a Final Rule regarding implementation of the exchanges (marketplaces) under PPACA and it promulgated a regulation regarding privacy and security standards that marketplaces must establish and follow. See 77 Fed. Reg. 18310, 18444 (March 27, 2012), 45 C.F.R. § 155.260. To ensure that federal contractor-operated systems meet federal information security and privacy requirements, the Federal Acquisition Regulation requires that agency acquisition planning for IT comply with the information technology security requirements in FISMA and addresses application of the Privacy Act to contractors. 48 C.F.R. § 7.103(w), and Subpart 24.1.

[17]5 U.S.C. 552a.

or grouping of information about an individual that is maintained by an agency and contains his or her name or another individual identifier. It defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or other individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice in the Federal Register that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and contest its content.[18]

- **The Computer Matching Act** is a set of amendments to the Privacy Act[19] requiring agencies to follow specific procedures before engaging in programs involving the computerized comparison of records for the purpose of establishing or verifying eligibility or recouping payments for a federal benefit program or relating to federal personnel management. The goal of the amendments was to prevent data "fishing expeditions" that could reduce or terminate benefits without verifying the information and notifying affected individuals of the matching program.

  Under these amendments, referred to as the Computer Matching Act, agencies must establish computer matching agreements with participating agencies that specify, among other things, the purpose and legal authority of the program and a justification for the program, including a specific estimate of any savings. A computer matching agreement ensures that there is procedural uniformity in carrying out computer matches and includes due process rights for individuals whose benefits may be affected.

- **The E-Government Act of 2002**[20] strives to enhance protection for personal information in government information systems by requiring

---

[18]Under the Privacy Act, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[19]Computer Matching and Privacy Protection Act of 1988. Pub. L. No. 100-503, 102 Stat. 2507 (Oct. 18, 1988), as amended by Pub. L. No. 101-56, 103 Stat. 149 (July 19, 1989), and Pub. L. No. 101-508, § 7201, 104 Stat. 1388 (Nov. 5, 1990).

[20]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

that agencies conduct, where applicable, a privacy impact assessment for each system. This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to the Office of Management and Budget (OMB) guidance, [21] a privacy impact assessment is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Agencies must conduct a privacy impact assessment before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form or before initiating any new data collections involving identifiable information that will be collected, maintained, or disseminated using IT if the same questions or reporting requirements are imposed on ten or more people.

- **The Health Insurance Portability and Accountability Act of 1996**[22] establishes national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers, and provides for the establishment of privacy and security standards for handling health information. The act calls for the Secretary of HHS to adopt standards for the electronic exchange, privacy, and security of health information, which were codified in the Security and Privacy Rules.[23] The Security Rule specifies a series of administrative, technical, and physical security practices for "covered

---

[21]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

[22]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9). Additional privacy and security protections, and amendments to the HIPAA Privacy and Security Rules, were established by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, Div. A, Title XIII, 123 Stat. 115, 226-279 and Div. B, Title IV, 123 Stat. 467-496 (Feb. 17, 2009).

[23]The Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164 and were updated at 78 Fed. Reg. 5566 (Jan. 25, 2013) and 79 Fed. Reg. 7290 (Feb. 6, 2014).

entities"[24] and their business associates to implement to ensure the confidentiality of electronic health information. The Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information, such as limiting uses and disclosures to intended purposes, notification of privacy practices, allowing individuals to access their protected health information, securing information from improper use or disclosure, and allowing individuals to request changes to inaccurate or incomplete information. The Privacy Rule establishes a category of health information, called "protected health information," which may be used or disclosed to other parties by "covered entities" or their business associates only under specified circumstances or conditions, and generally requires that a covered entity or business associate make reasonable efforts to use, disclose, or request only the minimum necessary protected health information to accomplish the intended purpose.

- **The Internal Revenue Code (IRC)** provides that tax returns and return information are confidential and may not be disclosed by IRS, other federal employees, state employees, and others having access to the information except as provided in Section 6103.[25] IRC Section 6103 allows IRS to disclose taxpayer information to federal agencies and authorized employees of those agencies for certain specified purposes. It specifies which agencies (or other entities) may have access to tax return information, the type of information they may access, for what purposes such access may be granted, and under what conditions the information will be received. For example, there are provisions in IRC section 6103 that will allow the use of tax information in the determination of eligibility for state, local or federal benefit programs administered by either SSA or various departments of human services or for loan programs under the jurisdiction of the Department of Education. Because the confidentiality of tax data is considered crucial to voluntary compliance, if agencies want to establish new uses of tax information, besides ensuring that executive branch policy requiring a business case to be developed for sharing

---

[24]"Covered entities" are defined in regulations implementing the Health Insurance Portability and Accountability Act of 1996 as health plans that provide or pay for the medical care of individuals, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations. 45 C.F.R. § 160.103.

[25]26 U.S.C. § 6103.

tax data, Congress must enact enabling legislation to allow the IRS to disclose the information necessary to meet the agency's needs.

- **IRS Publication 1075** establishes tax information security guidelines for safeguarding federal tax return information used by federal, state and local agencies. This publication provides guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS. The guide details security controls, reporting, record keeping and access control requirements that are aligned with IRS standard practices to meet the requirements of IRC Section 6103.

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

Under FISMA, the Secretary of HHS has the overall responsibility for implementing an agencywide information security program to ensure compliance with all governmentwide legal and policy requirements. That responsibility has been delegated to the HHS Chief Information Officer, who is responsible for ensuring the development and maintenance of a departmentwide IT security and privacy program to include the development and implementation of policies, standards, procedures, and IT security controls resulting in adequate security for all organizational information systems and environments of operation for those systems, including Healthcare.gov. The HHS Chief Information Officer is also responsible for establishing, implementing, and enforcing a departmentwide framework to facilitate an incident response program and the development of privacy impact assessments for all department systems.

The CMS Center for Consumer Information and Insurance Oversight (CCIIO) has overall responsibility for the federal systems supporting the establishment and operation of the federally-facilitated marketplace as well as for overseeing state marketplaces.[26] More specifically, CCIIO develops and implements policies and rules governing state-based marketplaces, oversees the implementation and operations of state-based marketplaces, and administers federally-facilitated marketplaces for states that elect not to establish their own.

---

[26]HHS established the Office of Consumer Information and Insurance Oversight in April 2010 as part of the HHS Office of the Secretary. In January 2011, the office moved to CMS and became CCIIO.

Security and privacy responsibilities for Healthcare.gov and its supporting systems are shared among several offices within CMS. The CMS Chief Information Officer is responsible for implementing and administrating the CMS information security program, which covers the systems developed by CMS to satisfy PPACA requirements. The Chief Information Officer is the designated approving authority for all CMS information systems and develops and implements CMS-specific policies and procedures that implement requirements in FISMA as well as HHS and other governmentwide security directives.

The CMS Chief Information Security Officer is responsible for ensuring the assessment and authorization of all systems, and the completion of periodic risk assessments, including annual security testing and security self-assessments. In addition, the Chief Information Security Officer is responsible for disseminating information on potential security threats and recommended safeguards and for establishing, documenting, and enforcing security requirements and processes for granting and terminating administrative privileges for servers, security domains, local workstations, and other information assets. Furthermore, Chief Information Security Officer responsibilities include supporting the CMS Senior Official for Privacy in documenting and managing privacy implementation in CMS IT systems, and collaborating with the CMS Chief Information Officer to help make security-related risk determinations.

Within component organizations of CMS, individual Information Systems Security Officers have been established to oversee security issues that arise in the development and implementation of specific systems. The Information Systems Security Officer within the CMS Office of e-Health Standards Privacy Policy and Compliance serves as the principal advisor to CCIIO on matters involving the security of information systems developed by CMS in support of Healthcare.gov. Information Systems Security Officer responsibilities include serving as a focal point for information security and privacy incident reporting and resolution, ensuring that standard information security requirements are included in contracts, ensuring that information security notices and advisories are distributed to appropriate CMS and contractor personnel, and ensuring that vendor-issued security patches are expeditiously installed.

The CMS Senior Official for Privacy is responsible for coordinating as the lead, in collaboration with the CMS Chief Information Security Officer, in developing and supporting integration of department privacy program initiatives into CMS information security practices. This includes establishing a CMS policy framework to facilitate the development and
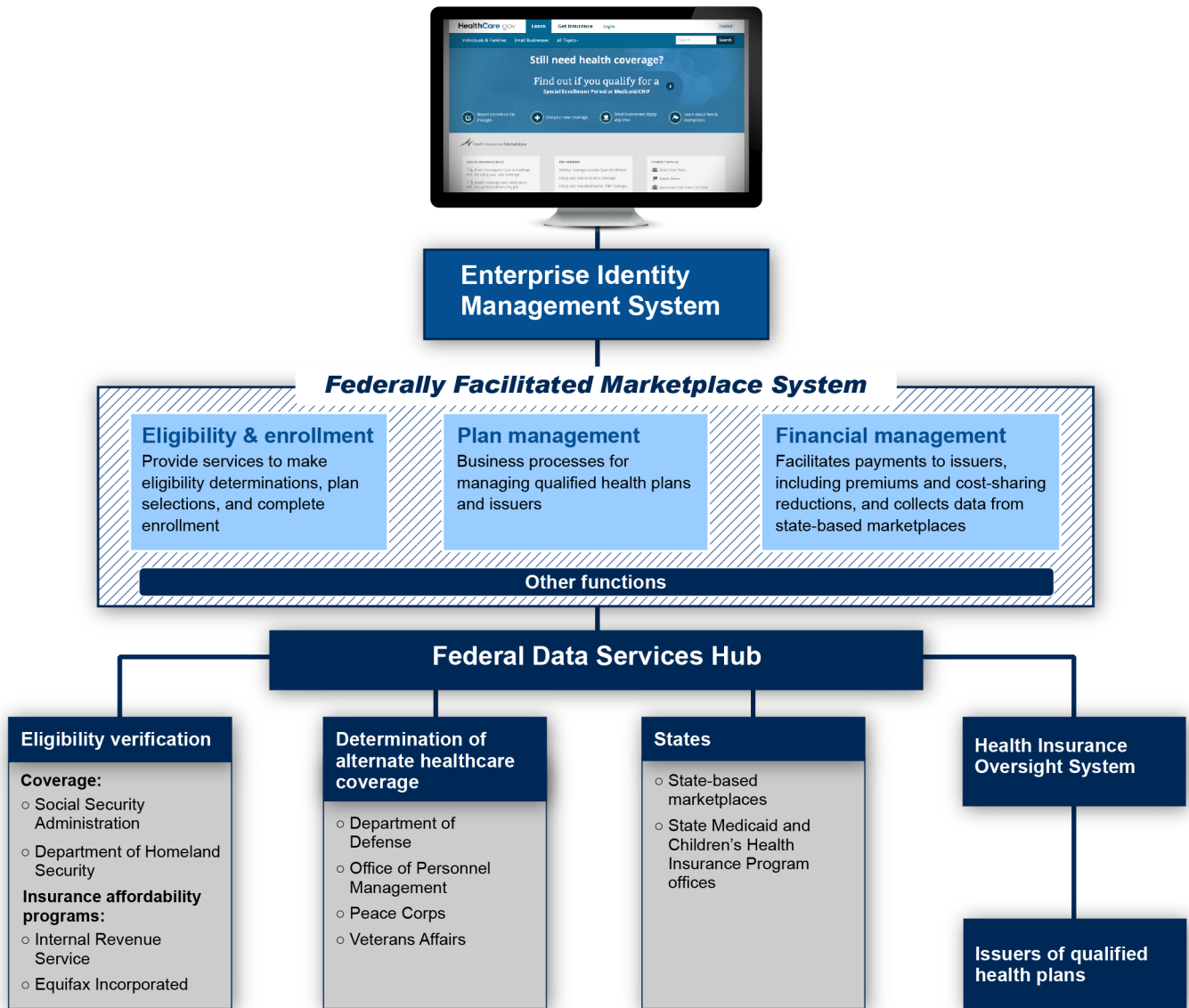
maintenance of privacy impact assessments for all systems, reviewing completed assessments, and attesting that they have been completed adequately and accurately.

The CMS Office of e-Health Standards Privacy Policy and Compliance is the principal authority for the management and oversight of CMS' Privacy Act duties. The CMS Privacy Officer's responsibilities include developing policy, providing program oversight, reviewing new and existing CMS policies, procedures, program memoranda, interagency agreements, and other written arrangements that may have an impact on the personal privacy of an individual, advising and assisting with the development and coordination of computer matching agreements between CMS components and other federal or state agencies, and reviewing and coordinating Privacy Act system of records notices and computer matching agreements.

CMS Exchanges Data with Many Interconnected Systems and External Partners to Facilitate Marketplace Enrollment

PPACA requires that CMS and the states establish automated systems to facilitate the enrollment of eligible individuals in appropriate healthcare coverage. Many systems and entities exchange or plan to exchange information to carry out this requirement. CCIIO has overall responsibility for the federal systems supporting Healthcare.gov and for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other federal agencies also play a role in maintaining systems that connect with the CMS systems to perform eligibility-checking functions. Finally, a number of private entities, including CMS contractors, participating issuers of qualified health plans, agents, and others also connect to the network of systems that support enrollment in Healthcare.gov. Figure 2 shows the major entities that exchange data in support of marketplace enrollment in qualified health plans and how they are connected.

Figure 2: Overview of Healthcare.gov and its Supporting Systems

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-14-730

PPACA directed the creation of exchanges, commonly referred to as "marketplaces," which are intended to facilitate a seamless eligibility and enrollment process through which a consumer submits a single application and receives an eligibility determination for enrollment into private marketplace insurance plans, known as qualified health plans, and

income-based financial subsidies to defray the cost of qualified health plan coverage,[27] and, if applicable, coverage under Medicaid, and CHIP.

PPACA required that marketplaces be operational in each state by January 1, 2014. States could choose to establish and operate their own state-based marketplace or have their residents use the federally-facilitated marketplace.[28] Regardless of whether a state established and operated its own marketplace or used the federally-facilitated marketplace, all marketplaces had to be equipped to carry out two key functions: eligibility and enrollment functions to assess and determine an individual's eligibility for enrollment and enroll eligible individuals in coverage and plan management processes to certify private health insurance plans for participation in the marketplace. Further, the federally-facilitated marketplace is equipped to handle financial management processes to facilitate payments to health insurers. In addition, each marketplace was to provide assistance to consumers in completing an application, obtaining eligibility determinations, comparing coverage options, and enrolling in coverage.

Several Major CMS Systems Support Enrollment-related Activities

The FFM system contains several modules that perform key functions related to obtaining healthcare coverage. In addition to the FFM, CMS operates a system known as the Federal Data Services Hub (data hub), which provides connectivity between the FFM and other state and federal systems. Within CMS, the Office of Information Services/Consumer Information and Insurance Systems Group is tasked with technical oversight of the development and implementation of the FFM and the data hub. Several other CMS systems also play a specific role in the

---

[27]Insurance affordability programs include the advance premium tax credit and cost-sharing reductions. The advance premium tax credit is available on an advance basis, and advance payment of the premium tax credit is reconciled on a tax filer's tax return. The credit is generally available to eligible tax filers and their dependents that are (1) enrolled in one or more qualified health plan through a marketplace and (2) not eligible for other health insurance coverage that meets certain standards. Cost sharing generally refers to costs that an individual must pay when using services that are covered under the health plan that the person is enrolled in. Common forms of cost sharing include copayments and deductibles.

[28]Through subsequent guidance, HHS identified options for states to partner with HHS when HHS establishes and operates an exchange. Specifically, under this model, states may assist HHS in carrying out certain functions of the exchanges, namely plan management and consumer assistance.

enrollment process, including the Enterprise Identity Management System, the Multidimensional Insurance Data Analysis System, the Health Insurance Oversight System, and the Health Insurance General Ledger. These systems are discussed in further detail later in this report.

Healthcare.gov Website

Healthcare.gov is the federal website that serves as the user interface for obtaining coverage through the FFM. Individuals can use the website to obtain information about health coverage, set up a user account, select a health plan, and apply for coverage. The site supports two major functions: providing information about PPACA health insurance reforms and health insurance options (the "Learn" web page) and facilitating enrollment in coverage (the "Get Insurance" web page). The "Learn" page provides basic information on how the marketplace works, how to apply for coverage, and available health plans. It also contains information on plan costs, ways to reduce out-of-pocket costs, and how consumers can protect themselves from fraud. Individuals do not have to provide PII to access this section of the website. In contrast to the information-oriented "Learn" page, the "Get Insurance" page allows a consumer to take steps to apply for health insurance and other associated benefits. In order to do so, a consumer must obtain a login account and prove his or her identity.

Enterprise Identity Management System

Before an individual can apply for health coverage or other benefits, CMS must verify his or her identity to help prevent unauthorized disclosure of PII. The process of verifying an applicant's identity and establishing a login account is facilitated by CMS' Enterprise Identity Management System. The system is intended to provide identity and access management services to protect CMS data while ensuring that users are identity-proofed and only authorized users are allowed and capable of accessing CMS resources.

To create a login account, the applicant provides a name and e-mail address and creates a password. Once an account has been created, the identity is confirmed using additional information, which may include Social Security number, current address, phone number, and date of birth. This information is transferred to Experian Information Solutions, Inc., a CMS contractor, which matches the information against its records.

In order to verify an applicant's identity, Experian must pull the applicant's credit profile to generate questions for the applicant. Experian's authority to receive PII and access the applicant's credit profile is stated in the terms of use of the Marketplace, and is granted by the applicant before the application process begins. The PII involved includes the applicant's

name, Social Security number (when provided), current address, phone number, and date of birth.

Experian's Remote Identity Proofing service verifies the applicant's identity using an application that interacts directly with the Enterprise Identity Management System. During the applicant registration process, the Enterprise Identity Management System sends the applicant's information to the Remote Identity Proofing service to match the information against Experian's records. A series of questions are then generated based on the applicant's information on file at Experian, and the applicant's responses are used to establish the identity of the person requesting the account. If an applicant fails the identity proofing process online, they must contact Experian's call center to take further steps to confirm their identity. If the applicant's identity cannot be confirmed via the call center, a manual review of documentation proving the applicant's identity is to be conducted by a separate contractor.

The Enterprise Identity Management System was developed by Quality Software Services, Inc. and made available for use on October 1, 2013, to support the 2014 health coverage enrollment season, which extended from October 1, 2013, through March 31, 2014.[29]

Federally Facilitated Marketplace System

The core of the FFM is a transactional database that was originally developed by CGI Federal, Inc., and since January 2014 has been further developed and maintained by Accenture, Inc. The FFM is intended to facilitate the eligibility verification process, enrollment process, plan management, financial management services, and other functions, such as quality control and oversight. It consists of three major modules: eligibility and enrollment, plan management, and financial management.

- **Eligibility and enrollment module**. Residents of states that operate their own state-based marketplaces enroll in healthcare plans via those marketplaces, which will be discussed subsequently. All others use the eligibility and enrollment module of the FFM system, which is intended to guide applicants through a step-by-step process to determine his or her eligibility for coverage and financial assistance, after which he or she is shown applicable coverage options and has the opportunity to enroll.

---

[29]The Enterprise Identity Management System is a CMS enterprisewide system that was not developed solely to support the FFM.

For the eligibility determination process, an applicant is asked questions on citizenship or immigration status, income, residency, and incarceration status. In each case, the applicant is asked a series of questions tailored to the responses he or she provides. PII asked of applicants generally includes:

- First, middle, and last name
- Date of birth
- Social Security number
- Ethnicity (optional)
- Home address (including city, state, county, and zip code)
- Phone number
- Citizenship or immigration status
- Employer name and address

Applicants requesting financial assistance answer additional questions regarding income to determine eligibility for advance payments of the premium tax credit and cost-sharing reductions, and assess or determine for potential eligibility for Medicaid and CHIP programs. This information includes:

- Wage and other income amounts
- Tax deduction amounts
- Information on existing health coverage enrollment

Throughout the eligibility and enrollment process, the applicant's information is collected and stored in the FFM's database and compared with records maintained by other federal agencies and other private entities to determine whether an applicant is eligible to enroll in a qualified health plan and, if so, to receive advance payments of the premium tax credit and cost-sharing reductions to defray the cost of this coverage. As part of this process, the system performs checks with other federal agencies to determine whether an applicant is eligible for coverage or benefits through other federal programs or agencies, such as the Federal Employee Health Benefits program or the VA.

Once a complete eligibility determination has been made, the FFM allows an applicant to view, compare, select, and enroll in a qualified health plan. Options are displayed to the applicant on the Healthcare.gov webpage, and applicants can use the "Plan Compare" function to view and compare plan details. The applicant can customize and filter the plans by plan type, premium amount, maximum out-of-pocket expenses, deductible, availability of cost-

sharing reductions, or insurance company. Once an applicant has signed up for a qualified health plan on Healthcare.gov, the FFM relays information about the enrollment to the chosen health plan.

The eligibility and enrollment module was developed and made available for public use beginning October 1, 2013, to support the 2014 health coverage enrollment season.

- **Plan management module**. While the eligibility and enrollment module supports individual applicants, the plan management module is intended to interact primarily with state agencies and issuers of qualified health plans. Specifically, the plan management module is intended to provide a suite of services for submitting, certifying, monitoring, and renewing qualified health plans, as well as managing their withdrawal. This module allows states and issuers to submit "bids" detailing proposed health plans to be offered on Healthcare.gov, including rate and benefits information. CMS personnel use the system to review, monitor, and certify or decertify the bids submitted by issuers. Once a bid has been approved, it is made available on Healthcare.gov. Like the eligibility and enrollment module, the plan management module uses a MarkLogic database.

  The plan management module was not operational during the initial 2014 enrollment period that began October 1, 2013. According to CMS officials, development and implementation of the module has occurred in incremental updates, and basic functionality, such as the ability to submit information about a proposed health plan for review by CMS, was intended to become available in the second quarter of 2014 for use during the 2015 enrollment period that begins November 15, 2014.

- **Financial management module**. Like plan management, the financial management module interacts primarily with issuers of qualified health plans. The module is intended to facilitate payments to health insurers through transactions based on the Electronic Data Interchange protocol.[30] Additional services include payment calculation for reinsurance, risk adjustment analysis, and the data
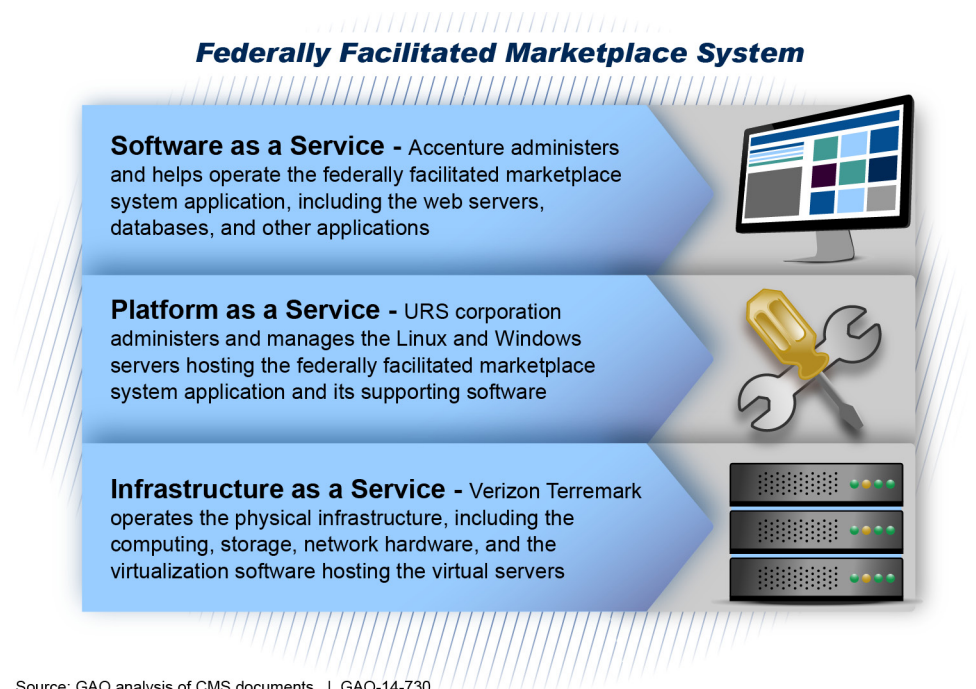
---

[30]The Electronic Data Interchange protocol establishes uniform data requirements and content that support standards such as the American National Standards Institute standard ASC X12, Benefit Enrollment and Maintenance (834), which is used to transfer enrollment information from a qualified health plan issuer to an applicant.

collection required to support these services. Transactions to be supported by the module include payments of premiums and cost-sharing reductions for individual enrollments, reinsurance, and risk adjustments.

Like the plan management module, the financial management module was not operational during the 2014 enrollment period. According to CMS officials, development and implementation of the module is occurring in incremental updates scheduled to be implemented throughout 2014. Functionality to support payments to insurers covering cost-sharing reductions and the advance premium tax credit was scheduled for the second quarter of 2014.

From a technical perspective, the FFM leverages data processing and storage resources that are available from private sector vendors over the Internet, a type of capability known as cloud-based services. The functionality provided by the system exists in several "layers" of services, including infrastructure as a service, platform as a service, and software as a service. Figure 3 depicts how the FFM is deployed across cloud service layers.

Figure 3: High-level Architecture of FFM System and Supporting Infrastructure

Federally Facilitated Marketplace System

Software as a Service - Accenture administers and helps operate the federally facilitated marketplace system application, including the web servers, databases, and other applications

Platform as a Service - URS corporation administers and manages the Linux and Windows servers hosting the federally facilitated marketplace system application and its supporting software

Infrastructure as a Service - Verizon Terremark operates the physical infrastructure, including the computing, storage, network hardware, and the virtualization software hosting the virtual servers

Source: GAO analysis of CMS documents. | GAO-14-730

- **Infrastructure as a service** — the service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment upon which a platform (i.e., operating system and programming tools and services) to develop and execute applications can be developed by the customer. Verizon Terremark provides this service for CMS, which includes helping CMS operate the data center, managing the physical computing and network hardware, and administering the virtualization software, on top of which run the operating systems.

- **Platform as a service** — the service provider delivers and manages the underlying infrastructure (i.e., servers, software, storage, and network equipment), as well as the platform (i.e., operating system, and programming tools and services) upon which the customer can create applications using programming tools supported by the service provider or other sources. URS Corporation, a subcontractor to Verizon Terremark, provides this service for CMS, acting as the Windows and Linux administrators for the virtual servers on top of which the FFM application runs.

- **Software as a service** — runs on a software platform and infrastructure managed by other vendors and delivers a complete application, such as the Healthcare.gov website, that individuals interact with when applying for healthcare coverage. CGI Federal originally designed, developed, and assisted with the operation of the FFM for CMS, but in January 2014 Accenture took over as the system's operator. Accenture's responsibilities include administering the web servers, databases, and applications running on top of the application operating system, as well as operating some security appliances that provide security controls for the FFM applications.

Federal Data Services Hub

The data hub is a CMS system that acts as a single portal for exchanging information between the FFM and CMS's external partners, including other federal agencies, state-based marketplaces, other state agencies, other CMS systems, and issuers of qualified health plans. The data hub was developed under contract by Quality Software Services, Inc., and made available for use on October 1, 2013, to support the 2014 health coverage enrollment season, which extended from October 1, 2013,

through March 31, 2014. The data hub was designed as a "private cloud" service[31] supporting the following primary functions:

- **Real-time eligibility queries**. The FFM, state-based marketplaces, and Medicaid/CHIP agencies transmit queries to various external entities, including other federal agencies, state agencies, and commercial verification services to verify information provided by applicants, such as immigration and citizenship data, income data, individual coverage data, and incarceration data.

- **Transfer of application information**. The FFM or a state-based marketplace transfers application information to state Medicaid/CHIP agencies. Conversely, state agencies also use the data hub to transfer application information to the FFM.

- **Transfer of taxpayer information**. The IRS transmits taxpayer information to the FFM or a state-based marketplace to support the verification of household income and family size when determining eligibility for advance payments of the premium tax credit and cost-sharing reductions

- **Exchange of enrollment information with issuers of qualified health plans**. The FFM sends enrollment information to appropriate issuers of qualified health plans, which respond with confirmation messages back to CMS when they have effectuated enrollment. State-based marketplaces also send enrollment confirmations, which CMS uses to administer the advance premium tax credit and cost-sharing reductions and to track overall marketplace enrollment.

- **Monitoring of enrollment information**. CMS, issuers of qualified health plans, and state-based marketplaces exchange enrollment information on a monthly basis to reconcile enrollment records.

- **Submission of health plan applications**. Issuers of qualified health plans submit "bids" for health plan offerings for validation by CMS.

---

[31]Although exact definitions vary, cloud computing can, at a high level, be described as a form of computing where users have access to scalable, on-demand IT capabilities that are provided through Internet-based technologies. A private cloud is operated solely for a single organization and the technologies may be on or off the premises.

To support these functions, each entity establishes Web services[32] that are used by the data hub for exchanging data with them. The data hub determines which entity has the data needed to answer a request from the FFM or a state-based marketplace during the application process. The data hub may connect with multiple data sources to provide a single answer to a request, which it provides in real-time, in a standard format.

Connections between external entities and the data hub are made through an Internet protocol that establishes an encrypted system-to-system web browser connection. Encryption of the data transfer between the two entities is designed to meet NIST standards, including Federal Information Processing Standard 140-2.[33] This type of connection is intended to ensure that only authorized systems can access the data exchange, thus safeguarding against cyber attacks attempting to intercept the data.

The data hub is designed to not retain any of the data that it transmits in permanent storage devices, such as hard disks. According to CMS officials, data is stored only momentarily in the data hub's active memory. The entities that transmit the data are responsible for maintaining copies of their transmissions in case the data needs to be re-transmitted. As a result, CMS does not consider the data hub to be a repository of personally identifiable information.[34]

Other CMS Systems

Several other CMS systems also support Healthcare.gov-related activities, including:

---

[32]Web services are client and server applications that communicate over the World Wide Web's HyperText Transfer Protocol. Web services provide a standard means of interoperating between software applications running on a variety of platforms and frameworks.

[33]Agencies are required to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. FIPS 140-2 specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md: May, 2001).

[34]In terms of the Privacy Act of 1974, CMS has determined that the data hub is not a system of records subject to the act's provisions.

- **Multidimensional Insurance Data Analytics System (MIDAS)**. This is a data warehouse system that is intended to provide reporting and performance metrics related to the FFM and other Healthcare.gov-related systems. The system offers several pre-defined reports, which are generated upon request and contain aggregated information about enrollments. According to CMS officials, the MIDAS system has been operational since before the beginning of the first enrollment period in October 2013.

- **Health Insurance Oversight System**. The system is intended to provide an interface for issuers of qualified health plans to submit information about qualified health plans. This information is to be transmitted to the plan management module of the FFM once that module is operational. According to CMS officials, the system serves a security function by keeping issuers of qualified health plans from having to connect directly with the FFM.

- **Health Insurance General Ledger**. The system is a longstanding internal CMS accounting system that handles payments and financial collections, including payments associated with the advance premium tax credit and cost-sharing reductions.

Many External Partner Entities Connect with the FFM and Data Hub

CMS relies on a variety of federal, state, and private-sector entities to support its Healthcare.gov-related activities, including other federal agencies, state-based marketplaces and supporting systems, issuers of qualified health plans, and agents and brokers.

Federal agencies and private entities assisting in making determinations for eligibility and financial assistance

Several federal agencies and one commercial verification service connect with the FFM and data hub to obtain and compare applicant data with their records to help CMS determine applicants' eligibility for coverage in a qualified health plan and for insurance affordability programs.[35] These entities include SSA, DHS, IRS, and Equifax, Inc.

- **Social Security Administration**. SSA's primary role is to assist CMS in confirming applicant-supplied information by comparing it with citizenship, Social Security number, death records, and incarceration

---

[35]To be eligible to enroll in a qualified health plan offered through a marketplace, an individual must be a U.S. citizen or national, or otherwise lawfully present in the United States, reside in the marketplace service area, and not be incarcerated (unless jailed while awaiting final disposition).

status maintained by SSA. This information is used to determine eligibility for enrollment in marketplace coverage. In addition to confirming citizenship data, death records, and incarceration status, SSA confirms disability benefits information to assist CMS in determining an applicant's qualification for insurance affordability programs, such as the advance premium tax credit, cost-sharing reductions, Medicaid, CHIP, and exemptions from the individual responsibility requirement. [36]

In order to assist CMS in confirming citizenship and whether identification information provided by an applicant corresponds to a deceased individual, SSA matches and validates data provided by applicants, including Social Security number, name, and date of birth with its internal systems, including the Master Files of Social Security Number Holders and Social Security Applications, which contains name, date of birth, place of birth, parents' names, citizenship status, date of death (if applicable) and associated Social Security number. The result is then sent to CMS to assist in making a determination of eligibility.

When requested by CMS, SSA provides incarceration status from its Prisoner Update Processing System. Incarceration status is verified for applicants who have attested that they are not currently incarcerated. Verification may occur for applicants to Medicaid and CHIP programs as well as qualified health plans under PPACA. The PII involved includes the applicant's Social Security number, name, and date of birth. If a positive incarceration status is identified, SSA transmits the relevant prisoner identification number, date of confinement, facility type, and contact information to CMS for use in determining eligibility.

Further, when requested by CMS, SSA provides monthly and annual Social Security Act benefit information and Social Security Act disability information from its Master Beneficiary Record database to CMS for determination or assessment of an applicant's eligibility to participate in insurance affordability programs. The information provided includes a disability indicator, current benefit status, and

---

[36]PPACA requires individuals to maintain health coverage that meets certain minimum requirements and imposes penalties on those who do not do so unless they have been granted an exemption from the requirement.

quarters of coverage. SSA may also provide information to CMS on monthly or annual benefits received by the applicant.

- **Department of Homeland Security**. DHS verifies the naturalized, acquired, or derived citizenship or immigration status of applicants as needed by CMS. DHS generally undertakes this verification only if CMS is unable to verify an applicant's status with SSA using a Social Security number or if the applicant indicates he or she is not a U.S. citizen on the application. In addition, DHS verifies the status of non-citizens who are lawfully present in the U.S. and seeking eligibility to enroll in a qualified health plan or participate in Medicaid, CHIP, or a state-based health plan as well as current beneficiaries who have had a change in immigration status or whose status may have expired. Within DHS, U.S. Citizenship and Immigration Services is responsible for verifying immigration status based on immigration status-related information provided by CMS, where appropriate, to assist CMS with its eligibility determination. Verification can be performed at any point during the benefit year and involves an initial electronic query and potentially two additional verification steps, if needed.

  The Systematic Alien Verification for Entitlements program accesses immigrant, non-immigrant, and derived and naturalized citizen status information from federal immigration databases through the Verification Information System. Initially, DHS attempts to verify status based on an applicant's immigration identification number, name, date of birth, and immigration document type using an automated verification process. If DHS cannot verify the status with this information alone, then it will prompt CMS to request additional information, at which time DHS will manually research the case. If DHS is still unable to verify the status, it will prompt CMS to submit copies of the applicant's immigration documents and a completed DHS Document Verification Request form to DHS for a final attempt to verify status. The verified immigration status or naturalized, acquired, or derived citizenship information is then transmitted through the data hub to the FFM to support eligibility and enrollment determination.

- **Internal Revenue Service**. IRS's role is to provide federal tax information to be used by CMS to determine or assess income and determine an applicant's eligibility for insurance affordability programs, including the advance premium tax credit, cost-sharing reductions, Medicaid, and CHIP. The IRS also provides an optional service for CMS to use in calculating the maximum amount of advance payments of the premium tax credit, which an eligible

applicant can elect to receive for assistance in paying monthly premiums.

In order to perform these functions, the IRS matches the applicant's Social Security number with tax return information and provides CMS with the applicant's Social Security number, family size, filing status, modified adjusted gross income, taxable year, and any other items authorized pursuant to the Internal Revenue Code. CMS may initiate this process by either an individual request or a bulk request.

The IRS Customer Account Data Engine supports this process. The data engine maintains records of tax returns, return transactions, and authorized taxpayer representatives. This system extracts and transmits tax return data to the CMS FFM, which then gives the applicant an opportunity to resolve any inconsistencies between the attestation and the matched IRS tax return information.

The IRS Advance Premium Tax Credit Computation Engine is then used by CMS to calculate the maximum allowable amount of the advance payments of the premium tax credit and also to calculate the remainder of the household contribution.[37] In order to calculate these amounts, the computation engine uses information about household income, the corresponding federal poverty level, family size, state of residency, and the cost to the applicant of subscribing to a qualified health plan. The IRS does not retain information about the applicant once it has sent the results to the FFM. IRS and CMS are to retain the raw data they exchange only to provide calculation results and perform IT integrity checks. CMS also retains a record of the amount of the advance payment of the premium tax credit that the applicant chooses to accept.

- **Equifax, Inc.** Equifax's role is to verify information about an applicant's current income and employment to assist CMS in making a determination about an applicant's qualification for insurance affordability programs, such as the advance premium tax credit and cost-sharing reductions. Specifically, according to CMS, the FFM sends an applicant's name, Social Security number, and date of birth

---

[37]Treasury Inspector General for Tax Administration, *Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project*, 2013-23-119 (Washington, D.C.: Sept. 27, 2013).

through the data hub to the Equifax Workforce Solutions Data Center, using an Equifax web service interface.

When it receives a request, Equifax searches for an exact match of the Social Security number supplied in the request and calculates a confidence score based upon additional information (name and date of birth) in the request. If the confidence score is above a threshold agreed upon with CMS and all required data elements are present, Equifax returns income and employment verification information (including employee and employer identification, employment status, base compensation, annual compensation, and pay period information) through the data hub to be used by CMS in determining eligibility for insurance affordability programs.

Federal agencies determining whether alternate healthcare coverage is available

Several additional federal agencies connect with the FFM and data hub to support CMS in determining whether a potential applicant has alternative means for obtaining minimum essential coverage[38] and therefore may not be eligible to receive the advance premium tax credit and cost-sharing reductions. For example, applicants could have minimum essential coverage if they are enrolled in a government program, such as Medicare or Medicaid, or certain employer-sponsored programs, such as the Federal Employees Health Benefits program. Those agencies responsible for determining if an applicant has minimum essential coverage include the following:

- **Department of Defense**. DOD's role is to verify the applicant's eligibility for TRICARE, the department's health care system for active duty military personnel and their families. DOD maintains TRICARE coverage information for all enrollees and beneficiaries within DOD. This information is matched by CMS to determine if an individual has minimum essential coverage.

   The Defense Manpower Data Center provides data used to determine TRICARE eligibility, enrollment, and medical claims payments via the Defense Enrollment Eligibility Reporting System. DOD initiates the verification process in the system once it receives a request from CMS with applicant data, including Social Security number, name,

---

[38]Minimum essential coverage includes health plans such as individual market health plans, eligible employer-sponsored health plans (if they meet affordability and quality standards), or government-sponsored health coverage such as Medicare, Medicaid, and the Children's Health Insurance Program. See 26 U.S.C. § 5000A(f).

date of birth, gender, and requested qualified health plan effective coverage start and end date. DOD determines if the individual is a beneficiary and if so, it responds to the verification request with the insurance end date (if TRICARE coverage has lapsed), Social Security number ID, and response code to verify the status of an individual's TRICARE coverage.

- **Office of Personnel Management**. OPM's role is to provide health insurance coverage data to CMS for federal employees so that CMS can determine if an individual has minimum essential coverage.

  CMS performs the matching function itself, using a data file provided periodically by OPM. OPM transmits this data file to CMS on a monthly basis that contains coverage information of all employees who receive health benefits through the federal government. In addition to the personnel data file, OPM also sends an annual premium index file that contains information on the costs of health plans available to federal employees.

  OPM's Enterprise Human Resources Integration office relies on its Statistical Data Mart to support this function. The Statistical Data Mart transmits a file via a secure private link to the CMS Data Center, which then routes the file through the data hub to the FFM. The file contains Social Security number, name, gender, date of birth, employment data, and health plan coverage information for all federal employees who have employer-sponsored coverage.

- **Peace Corps**. The Peace Corps' role is similar to OPM's. It provides CMS with information on active Peace Corps volunteers to facilitate verification of an applicant's coverage under the Peace Corps' volunteer health benefits program. The Peace Corps is responsible for providing medical care to all Peace Corps volunteers throughout their service, and such medical care is considered minimum essential coverage.

  The Peace Corps sends a data file to CMS containing information on all current volunteers five times per week. The information is based on the agency's Volunteer Applicant and Service Records system, which includes records of current and former Peace Corps volunteers, trainees, and applicants for volunteer service, including Peace Corps United Nations volunteers. The file includes all volunteers and trainees who have received health benefits in the previous three calendar months. Although the volunteer's Social Security number and eligibility start date are the only PII required to verify coverage,

the Peace Corps sends additional data elements, including name, gender, date of birth, eligibility end date for those who are no longer in service, and projected end date for those still in service, in case that information is needed to handle specific CMS queries.

- **Department of Veterans Affairs**. VA's role is to validate the existing coverage of VA health beneficiaries so CMS can determine if an individual has minimum essential coverage. The Veterans Health Administration within VA is responsible for this process.

  In order to verify existing coverage, VA matches applicant information to Veterans Health Administration's Health Care Program beneficiary records. CMS requests data from VA's records only when it is necessary to determine if an individual has minimum essential coverage. The PII matched includes: Social Security number, name, gender, date of birth, requested qualified health plan effective coverage date, and requested qualified health plan end date.

  VA relies on records from the Veterans Information & Eligibility Reporting Services system, which gathers and catalogs data from various sources, applications, and databases across VA and DOD. Once an applicant's identity has been matched, the system retrieves coverage information from VA's supporting systems. Based on the applicant's enrollment status, VA's Virtual Lifetime Electronic Record Data Access Service passes back a response to CMS that includes the verified Social Security number and the relevant VA health coverage start date and end date, if applicable.

State-based marketplaces and other state systems

In most states, multiple government entities may need to connect to the FFM and data hub to carry out a variety of functions related to healthcare enrollment. State-based marketplaces generally perform the same functions that the FFM performs for states that do not maintain their own marketplace. However, in certain cases, known as partnership marketplaces, states may elect to perform one or both of the plan management and consumer assistance functions while the FFM performs the rest. The specific functions performed by each partner vary from state to state. Figure 4 shows what functions are performed by each type of marketplace.

Figure 4: Functions Performed by the Various Types of Marketplaces

Federally Facilitated Marketplace
- Eligibility and enrollment
- Financial management
- Plan management
- Consumer assistance

Federally Facilitated Partnership
- Eligibility and enrollment
- Financial management
- Plan management
- Consumer assistance

State-based Marketplace
- Eligibility and enrollment
- Financial management
- Plan management
- Consumer assistance

■ Functions performed by CMS
■ Functions performed by States

Source: GAO analysis of CMS data. | GAO-14-730

Regardless of whether a state operates its own marketplace, most states need to connect their state Medicaid and CHIP agencies to either their state-based marketplace or the FFM to exchange data about enrollment in these programs. Such data exchanges are generally routed through the CMS data hub. In addition, states may need to connect with the IRS (also through the data hub) in order to verify an applicant's income and family size for the purpose of determining eligibility for or the amount of the advance premium tax credit and cost-sharing reductions. Finally, state-based marketplaces are to send enrollment confirmations to the FFM so that CMS can administer advance payments of the premium tax credit and cost-sharing payments and track overall marketplace enrollment.

Issuers of Qualified Health Plans	Issuers of qualified health plans access the FFM separately from individual applicants, using CMS's Health Insurance Oversight System. The primary data transfer to issuers is the passing of enrollment information from the FFM when an individual completes the application process. In this case, the FFM transmits the enrollment information to the data hub, which forwards it to the cognizant issuer of qualified health plans in a standardized Electronic Data Interchange format. The issuer then replies with a confirmation message that is also formatted according to the standard. According to CMS, there were 219 issuers of qualified health plans that participated during the 2014 plan year.

Apart from enrollment, issuers of qualified health plans are to interact with the FFM through the Plan Management and Financial Management modules, as previously described.

CMS established procedures to help ensure the security of data transmissions between the FFM and issuers of qualified health plans. Specifically, each issuer is required to digitally sign all transmissions with an encryption key that can be used by the FFM (and vice versa) to ensure that the transmissions are authentic. According to CMS officials, as transactions are readied for transmission, the CMS MIDAS system checks the data to ensure that it is being routed to the right provider. Subsequent to the transmission, MIDAS takes additional steps to confirm that the transmission was executed correctly. Issuers of qualified health plans also sign trading partner agreements with CMS requiring that the Electronic Data Interchange transactions they conduct be in accordance with CMS security and privacy policies.

Agents and brokers

In addition to applicants themselves, agents and brokers may access the Healthcare.gov website to perform enrollment-related activities on behalf of applicants. It is up to individual states to determine whether to allow agents and brokers to carry out these activities, which can include enrolling in healthcare plans and applying for the advance premium tax credit and cost-sharing reductions.

To perform these functions, agents and brokers need to first, be licensed by their state. They are then required to complete registration requirements, which include participating in a training course in using the FFM and electronically signing an agreement on the use of the system that includes adherence to FFM security and privacy policies. FFM user accounts are created for these individuals after they are authenticated through the Enterprise Identity Management System. According to CMS,

71,103 agents and brokers have completed the registration process for plan year 2014.

Offline functions

Individuals can also use a paper application when applying for health insurance under PPACA. CMS awarded a contract for eligibility support services to Serco Inc. for the intake, routing, review, and troubleshooting of paper applications submitted for enrollment into a qualified health plan and for insurance affordability programs including, but not limited to, the advance premium tax credit, cost-sharing reductions, Medicaid, and CHIP. Serco Inc. is also expected to provide records management and verification support.

CMS and IRS Took Steps to Protect Taxpayer Information

IRS and CMS have taken steps to establish policies and procedures for complying with requirements for protecting taxpayer information, including the Internal Revenue Code, which provides that tax returns and return information are confidential and may not be disclosed by IRS except for certain purposes specified in section 6103 of the Internal Revenue Code.[39] PPACA amended section 6103(l) (21) of the Internal Revenue Code to authorize the IRS, upon written request from the Secretary of HHS, to disclose certain taxpayer PII, in order to assist in carrying out eligibility determinations for financial assistance through the data hub and FFM.

Additionally, IRS Publication 1075 establishes guidelines for safeguarding federal tax return information used by federal, state, and local agencies. This publication details security controls, reporting, record keeping, and access control requirements that are aligned with IRS standard practices to meet the requirements of section 6103 of the code.

In order to document the safeguards in place to protect taxpayer information received during the Healthcare.gov enrollment process, IRS required CMS to complete and submit a Safeguard Procedures Report outlining the security configurations and controls it intended to implement. For example, in order to address Internal Revenue Code section 6103 (p)(4)(C), which requires any entity or person receiving a return or return information to restrict access to the return or return information only to persons whose duties or responsibilities require access and to whom

---

[39]26 U.S.C.§ 6103.

disclosure may be made, CMS reported that it restricts access to taxpayer data only to individuals who require the data to perform their official duties and as authorized under the code through separation of duties, role-based security for all employees and contractors, and minimum required access for duties. In September 2013, IRS's Director of the Office of Privacy, Governmental Liaison and Disclosure informed CMS that IRS accepted its report as certification that the confidentiality of federal tax information disclosed to CMS would be adequately protected.

Information Security and Privacy Weaknesses Place Healthcare.gov Data at Risk

While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain in both the processes used for managing security and privacy as well as the technical implementation of IT security controls. CMS took steps to protect security and privacy, including developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. However, CMS has not fully addressed security and privacy management weaknesses, including having incomplete security plans and privacy documentation, conducting incomplete security tests, and not establishing an alternate processing site to avoid major service disruptions. In addition, we identified weaknesses in the technical controls protecting the confidentiality, integrity, and availability of the data maintained in the FFM. An important reason for these security and privacy weaknesses is that CMS did not ensure a shared understanding of how security was implemented for the FFM among all entities involved in its development. Until these weaknesses are addressed, increased and unnecessary risks remain of unauthorized access, disclosure, or modification of the information collected and maintained by Healthcare.gov and related systems or the disruption of service provided by the systems.

CMS Established a Security and Privacy Program for Healthcare.gov and Related Systems

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout an information system's life cycle; and a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices.

In addition, OMB Circular A-130, Appendix III, requires federal agencies to establish interconnection security agreements before connecting their IT systems to other IT systems, based on an acceptable level of risk. The authorization should define the rules of behavior and controls that must be maintained for the system interconnection. Further, NIST guidance states that the interconnection agreement should document the requirements for connecting the IT systems and describe the security controls that will be used to protect the systems and data.[40]

As previously discussed, the Privacy Act requires agencies that establish or make changes to a system of records, to develop a system of records notice that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and contest its content.[41] Further, the E-Government Act of 2002 requires agencies to conduct a privacy impact assessment. This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

In addition, NIST issued guidance in 2013 on establishing privacy protections as part of an overall information security program.[42] The guidance is intended to serve as a road map for identifying and implementing privacy controls based on the need to protect the PII of individuals collected and maintained by an organization's information systems and programs. For example, NIST states that organizations should administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII and ensure that personnel certify acceptance of responsibilities for privacy requirements. In addition, NIST requires organizations to develop and implement a privacy incident response plan and provide an organized and effective response to privacy incidents in accordance with the plan. The plan should include, among other things:

---

[40]NIST, *Security Guide for Interconnecting Information Technology Systems (Gaithersburg, Md.,* August 2002*).*

[41]Under the Privacy Act, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[42]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md., April 2013).

GAO-14-730 Healthcare.gov

- the establishment of a cross-functional privacy incident response team that reviews, approves, and participates in the execution of the plan;
- a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; and
- a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly.

CMS developed security-related policies and procedures

CMS took steps to establish protections for Healthcare.gov and related systems as part of its information security program. It assigned overall responsibility for securing the agency's information and systems to appropriate officials, including the agency Chief Information Officer and Chief Information Security Officer, and designated information system security officers to assist in certifying information systems of particular CMS components. Additionally, CMS business owners are responsible for ensuring CMS systems they are responsible for are developed in accordance with, and comply with, CMS information security policies.

CMS also documented information security policies and procedures to safeguard the agency's information and systems and to reduce the risk of and minimize the effects of security incidents. For example, *CMS's Policy for the Information Security Program*[43] established its overall information security program and set ground rules under which the agency is to operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents. This policy establishes preventive measures and controls designed to detect any incidents that occur. It also addresses the recovery of information resources in the event of a disaster.

Further, CMS has also developed a process for planning, implementing, evaluating, and documenting remedial actions to address identified deficiencies in information security policies, procedures, and practices. The process specifies that plans of action and milestones are to be developed within 30 days of the final results of any external assessment or review, and that remedial actions are to be tracked monthly until the deficiency has been resolved, as determined by a security controls assessment, continuous monitoring, or security impact analysis. CMS has

---

[43]CMS, *CMS Policy For the Information Security Program* (Baltimore, Md., August 2010).

established a tracking system, called the CMS FISMA Controls Tracking System, which it uses to track plans of action and milestones for addressing identified deficiencies. In addition, according to CMS officials, a dedicated team has been established to monitor the security of Healthcare.gov and related systems on a continuous basis.

CMS established interconnection security agreements with federal partners

CMS established interconnection security agreements with the federal agencies it exchanges information with, including DHS, DOD, IRS, SSA, and VA. These agreements identify the requirements for the connection, the roles and responsibilities for each party, the security controls protecting the connection, the sensitivity of the data to be exchanged, and the training requirements and background checks required for personnel with access to the connection.

CMS took steps to protect the privacy of Healthcare.gov applicants' information

To address Privacy Act requirements, CMS published and updated a system-of-records notice for Healthcare.gov that addresses all required information. The notice includes, among other things, a description of the types of individuals that will have their PII contained in the system, the type of information that will be maintained in the system, and external entities who may receive such information without the explicit consent of affected individuals.

CMS has developed basic privacy training for all staff and role-based training for staff who need it, such as individuals who have access to PII while executing their routine duties. The Director of CMS's Privacy Policy and Compliance Group stated that all personnel, including contractor staff, working with databases or IT systems were required to attend privacy training based on their responsibilities related to Healthcare.gov. Contractors are required to submit evidence that this training has taken place.

Further, CMS has also established an incident handling and breach response plan and an incident response team to help manage response efforts for privacy incidents, to identify trends, and make recommendations to HHS to reduce the risks to PII. The plan outlines CMS's processes to detect a potential security incident, report it, and limit the scope and magnitude of an incident. The plan outlines the factors that CMS will consider when assessing the likely risk of harm caused by an

incident and specifies policies and procedures for notifying individuals affected by a breach of PII.[44]

CMS Accepted Increased Security Risks When Healthcare.gov Was Deployed in October 2013

In granting the FFM system an "authority to operate" in September 2013 and allowing states to connect to the data hub that had not fulfilled all security requirements, CMS accepted increased security risks. However, accepting such risks meant that the overall risk was heightened that a compromise could occur to the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. CMS subsequently took steps to mitigate the risks identified at the time of the interim authority to operate and the interim state interconnection authorizations.

CMS accepted risks in authorizing states to connect to the data hub

CMS is responsible for the overall security of the data hub, which includes ensuring that the states connecting to it have complied with CMS's security review process.[45] Any state seeking to gain an "authority to

---

[44]In 2013, we reported that CMS had developed, but inconsistently implemented, policies and procedures for responding to a data breach involving PII that addressed key practices specified by the OMB and NIST. We recommended that the Secretary of Health and Human Services direct the Administrator for the Centers for Medicare & Medicaid Services to: (1) require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations; (2) document the number of affected individuals associated with each incident involving PII; and (3) require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices. For more information, see GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO-14-34, (Washington, D.C.: Dec. 9, 2013).

[45]CMS developed a document, called the *Minimum Acceptable Risk Standards for Exchanges*, which defines a set of minimum standards for acceptable security risk that the marketplaces must address and is based on NIST standards and the IRS Safeguards Program.

connect" to the data hub was required to submit documentation that it had properly secured its planned connection.[46]

However, not all states seeking to connect to the FFM through the data hub had satisfactorily completed all the CMS requirements prior to the start of the open enrollment season on October 1, 2013. According to the Information Systems Security Officer within the Consumer Information and Insurance Systems Group, four states (Mississippi, Oklahoma, Utah, and West Virginia) did not resolve issues identified in CMS's review of their documentation prior to October 1, 2013. Rather than deny these states the ability to connect, CMS accepted the security risks and gave the states an interim 60-day authorization. (In contrast, the 38 states that fully met requirements were granted a 3-year authorization.) The same official stated that examples of issues that led to an interim authorization were (1) high-risk findings remaining open from security testing, (2) a large number of lower risk findings remaining open from testing, or (3) the lack of a third-party independent security assessment. According to this official, no states seeking to connect to the data hub at the beginning of open season were denied the ability to do so because CMS officials deemed it critically important that all states be able to connect to Healthcare.gov if they sought to do so.

In cases where CMS granted an interim authorization, officials told us the CMS Chief Information Officer sent a letter to the state specifying the tasks that had to be completed before a full 3-year authorization would be granted. As CMS officials pointed out, their decision to allow these states to connect on an interim basis was in accordance with NIST standards, which state that "interim approval may be granted if the planned interconnection does not meet the requirements stated in the interconnection security agreement, but mission criticality requires that

---

[46]The documentation required by CMS includes: (1) a system security plan describing the design of the system and the process for identifying and mitigating security risks, (2) a report documenting an assessment of the security risks for the system conducted either internally or through a third party, (3) a plan of action and milestones and corrective action plan for mitigating any risks identified by the security risk assessment, (4) a signed information exchange agreement documenting roles and responsibilities for protecting data, and (5) an interconnection security agreement specifying the interconnection arrangements and responsibilities for all parties, the security controls implemented by the state, the technical and operational security requirements that the state follows, and attesting that the state IT system is designed, managed, and operated in compliance with the CMS standards.

the interconnection must be established and cannot be delayed.[47] According to CMS, no compromises of data resulted from its acceptance of these risks and each of these states subsequently addressed the deficiencies in its original submission and received a 3-year authorization.

CMS accepted significant risks in initially authorizing the FFM to operate

In addition to allowing four states to connect without fulfilling all security requirements, CMS also authorized the FFM to operate in September 2013 though testing for several support systems had not been completed and high-risk findings had been identified in the testing that was completed. NIST guidelines state that the authorizing official is to determine whether the risks to organizational operations, organizational assets, individuals, and other organizations, are acceptable.[48] Further, *CMS's Information Security Authorization to Operate Guide* states that a system should be denied an authorization to operate if there are open high-risk findings; the authorization to operate package is missing the system security plan, risk assessment, or security assessment; or a known vulnerability has been exploited.

The FFM was initially granted authorization to operate on September 3, 2013, even though high-risk weaknesses existed. This authorization was for a limited configuration of the system that included only modules for qualified health plans and for dental coverage. For this configuration, the CMS Chief Information Officer deemed the existing risks to the system as acceptable, despite the fact that two high-risk findings remained open because an action plan had been developed for addressing the risks and the approval was predicated on completion of those actions. In addition, four other findings had not been addressed. According to CMS officials, a subsequent decision was made to take offline the modules of the FFM that had been authorized on September 3, 2013, because the high-risk findings associated with them could not be mitigated before the beginning of open enrollment on October 1.

An additional decision memorandum, dated September 27, 2013, addressed other modules of the FFM. It noted that CMS's security

---

[47]NIST, *Security Guide for Interconnecting Information Technology Systems*, SP 800-47 (Gaithersburg, Md., August 2002).

[48]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md., February 2010).

contractor had not been able to test all of the security controls for the FFM in one complete version of the system. The memorandum granted an authority to operate for six months and stipulated that a full security controls assessment be conducted on the FFM, including all three of its major modules, within 60 to 90 days of October 1.

A complete security controls assessment of the FFM's eligibility and enrollment module was conducted in December 2013, in keeping with the time frames established in the September 27, 2013, memo. However, the other two major modules of the FFM—plan management and financial management—were not tested. These modules had not yet been fully developed and were not made available online on October 1.

CMS Has Not Fully Implemented Security and Privacy Management Controls Associated With Healthcare.gov

Though CMS developed and documented security policies and procedures, it did not fully implement actions required by NIST before Healthcare.gov began collecting and maintaining PII from individual applicants. Specifically, NIST guidelines[49] require that system security plans include a description of the components comprising the system—called an authorization boundary—and a listing of other information systems that interconnect with the system, among other elements. The plans should also identify the individuals responsible for the system and its security, include descriptions of how security controls are implemented, and, in the case of controls recommended by NIST but not implemented, a justification for why the control was deemed not necessary for that system. To the extent that a system relies on controls established for another system (known as inherited controls) or for multiple systems (referred to as common controls), NIST guidelines call for describing those controls as well, noting that organizations should assess how effective they are for the new system being planned and identify compensating or supplementary controls as needed.

CMS did not document key controls in system security plans

CMS developed system security plans for the systems supporting Healthcare.gov that document the planned implementation of the controls designed to protect the confidentiality, integrity, and availability of the systems and the information they contain. While the system security plans for the FFM and data hub incorporate most of the elements

---

[49]NIST, *Guide for Developing Security Plans for Federal Information Systems,* Special Publication 800-118 Revision 1 (Gaithersburg, Md., February, 2006).

specified by NIST, each is missing or has not completed one or more relevant elements. For example, the security plan for the FFM does not define the system's authorization boundary, or explain why agency officials determined that four of the controls listed in NIST's guidance were not applicable. Additionally, for 125 inherited controls and control enhancements out of the 312 controls and enhancements in the plan, the plan contains no details other than identifying the system from which they are inherited. Similarly, the data hub security plan does not list the systems with which it has interconnection security agreements, though it connects with systems from many federal agencies, states, and the District of Columbia.[50] CMS officials told us that they believed their security plans were complete. However, the plans they provided did not contain these important elements.

Without complete system security plans, it will be difficult for agency officials to make a fully informed judgment regarding the risks involved in operating those systems, increasing the risk that the confidentiality, integrity, or availability of the system could be compromised.

CMS has not finalized an interconnection security agreement with Equifax

CMS has not completed security documentation governing its interconnection with Equifax Inc., a private company that performs income verification services that CMS uses to determine eligibility for income-based subsidies. In order to perform the verification, CMS transmits PII to Equifax, which responds with information about the applicant's current employer and compensation. As previously discussed, OMB requires agencies to establish interconnection security agreements before connecting their IT systems to other IT systems. CMS officials said they are relying on a draft data use agreement for this exchange of data, because the agreement has not yet been fully approved within CMS.

CMS did not fully assess privacy risks in PIAs

CMS privacy documentation was also incomplete. OMB requires agencies to assess privacy risks as part of the process of developing a privacy impact assessment (PIA).[51] These risk assessments are intended to help program managers and system owners determine appropriate privacy protection policies and techniques to implement those policies.

---

[50]Currently, 47 states, including the District of Columbia have a connection to the data hub.

[51]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

According to OMB, an analysis of privacy risks should be performed to determine the nature of privacy risks and the resulting impact if corrective actions are not in place to mitigate those risks as well as an assessment of alternative processes for handling information to mitigate potential privacy risks.

CMS developed and documented PIAs for the FFM and the data hub. Both PIAs describe, among other things, the purpose of the system; the type of information it will collect, maintain, or share; and whether the system handles PII. The PIA for the data hub states that the system does not collect, maintain, use, or share PII, although it processes and transmits data, including PII, in support of Healthcare.gov and its supporting systems. Both PIAs were approved by the CMS Senior Official for Privacy and the HHS Senior Agency Official for Privacy.

However, in completing these PIAs, CMS did not assess the risks associated with the handling of PII or identify mitigating controls to address such risks. Both PIAs provided only general information about the systems, such as the type of information that the system would collect, the intended uses for the PII that was to be collected, and the external entities with whom the PII would be shared. They did not include an analysis of privacy risks associated with this broad collection of personal information or what steps were taken to mitigate those risks. For example, the data hub PIA did not include an analysis justifying the agency's conclusion that the system does not collect, maintain, use, or share PII. Nor did the FFM PIA include an assessment of alternative processes for handling information to mitigate potential privacy risks associated with the extensive amount of PII collected and maintained by the system.

The Director of CMS's Privacy Policy & Compliance Group stated that discussions about the risks associated with the handling of PII within Healthcare.gov-related systems were conducted during the system's security development process because CMS considered this a security issue. She also stated that CMS's PIAs were intended primarily to look at data flows and authorities to collect the data. However, according to OMB guidance, a PIA should also include an analysis of privacy risks. Without such an analysis, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems.

Likewise, the draft PIA for MIDAS, a data warehouse system that provides reporting and performance metrics related to the FFM and other

supporting systems, does not include an analysis of privacy risks consistent with OMB guidance. According to CMS officials, MIDAS generates reports that aggregate data, including PII collected during the plan enrollment process, to create summary reports. The Director of CMS's Privacy Policy & Compliance Group stated that MIDAS did not contain PII when it first became operational and that a draft PIA was developed after the system's functions were changed to include processing of PII. She also stated that the draft had not yet been finalized but did not indicate whether the final version would include an analysis of privacy risks. Without an approved PIA that includes a thorough analysis of privacy risks, it will be difficult for CMS to demonstrate that it has assessed the potential for PII to be displayed to users, among other risks, and taken steps to ensure that the privacy of that data is protected.

CMS did not establish computer matching agreements with two agencies

CMS did not establish a computer matching agreement with all of the federal agencies with which it exchanges data for the purposes of verifying eligibility for healthcare coverage and the advance premium tax credit, as required by the Computer Matching Act. Specifically, CMS has a computer matching agreement in place with SSA, DHS, IRS, DOD, and VA. These agreements include all required information, including the purpose and legal authority for the exchange, a justification for the exchange, and a description of the records that will be matched.

However, CMS did not develop such an agreement with OPM or the Peace Corps. According to OPM and Peace Corps officials, they determined that a computer matching agreement was not required because they transmitted information to CMS in a batch file format on an intermittent basis rather than establishing a real-time comparison process. Further, they considered their transmission of information to CMS to be a one-way transaction, rather than a direct matching of information in two or more systems. However, the Computer Matching Act neither specifies the connectivity between two automated systems of records nor that the requirement for an agreement applies only to certain types of transfers.[52] Accordingly, since the exchange of data between

---

[52]The Computer Matching amendments to the Privacy Act require a matching agreement when a record is disclosed by an agency to a recipient agency for use in a computer matching program. 5 U.S.C. § 552a(o). The Privacy Act defines "matching program" as any computerized comparison of two or more automated systems of records for the purpose of [among other purposes] establishing or verifying the eligibility of applicants for, or recipients or beneficiaries of, payments under federal benefit programs. 5 U.S.C. § 552a(a)(8).

CMS and OPM and the Peace Corps appears to be a computerized comparison of data from two automated systems of records for purposes of determining eligibility for federal benefits,[53] as described in the act, a computer matching agreement would be required.[54]

Without conducting a complete PIA for systems collecting and maintaining PII and establishing computer matching agreements with all agencies exchanging PII for eligibility determination purposes, increased risk exists that proper protections have not been implemented for the PII being exchanged.

CMS did not conduct complete security testing

FISMA requires agencies to periodically test and evaluate information security controls on information systems to ensure they are being implemented effectively. In addition, NIST and CMS guidance make clear that the security of complex systems such as the FFM and interconnected systems needs to be tested in a comprehensive fashion that takes into consideration how the systems are interconnected and how security controls are managed across all interconnected systems. For example, NIST has developed a risk management framework that, among other things, emphasizes that agencies should test the implementation of security controls to determine the extent to which they are implemented correctly, are operating as intended, and meet security requirements.[55] NIST also notes that security assessments should assess the controls implemented by a system and those inherited from other systems. Draft NIST guidance on security engineering also makes clear that security validation should take place at multiple levels of a system, ranging from individual components and service, up through systems of systems. The framework states that security assessments or testing should be completed before a system is granted an "authority to connect" to other agency systems.

---

[53] PPACA requires individuals to maintain health coverage that meets certain minimum requirements and imposes penalties on those who do not do so. OPM and Peace Corps, among other government agencies, provide health insurance coverage data to CMS for purposes of determining if an individual has minimum essential coverage.

[54] We recently issued a report on computer matching agreements, including the need for additional OMB guidance. See GAO, *Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation*, GAO-14-44 (Jan. 13, 2014).

[55] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37 Revision 1* (Gaithersburg, Md. February 2010).

CMS's system security plan procedures state that a completed system security plan package must contain technical information about the system, its security requirements, and the controls implemented to provide protection against vulnerabilities. CMS procedures also note that for a comprehensive assessment, the assessor is expected to assess all controls, including those that are inherited, and limitations on testing inherited controls should be clearly identified. In addition, CMS policy states that an understanding of all relevant controls and how they are inherited throughout the system is required to evaluate the effectiveness of security controls.

CMS has undertaken, through its contractors and at the agency and state levels, a series of security-related testing activities that began in 2012. Table 1 summarizes these activities through June 2014.

Table 1: Security Testing of the Federally Facilitated Marketplace (FFM) System, Data Hub, and Connections with Federal Partners

Date	Test Performed	Scope
September 2012	Infrastructure as a service security control assessment	Physical environment and hardware in data center.
October 2012	Platform as a service security control assessment	Security controls of the platform as a service general support system.
March-April 2013	First FFM security control assessment	Partial application assessment of the FFM Qualified Health Plans module.
	Data hub testing with Department of Defense begins	Tests performed include functional tests, connectivity tests, and performance tests.
May 2013	Data hub testing with Social Security Administration begins	Tests performed include penetration tests, connectivity tests and performance tests.
	Data hub testing with Department of Homeland Security begins	Tests performed include security assessment, and interface tests.
July 2013	Data hub connection testing with Internal Revenue Service	Tests performed include controls assessments, compliance and vulnerability scanning.
August - September 2013	Second FFM security control assessment	Partial application testing of the deployed FFM eligibility and enrollment module, but with testing hampered by significant functionality issues identified by the tester. Assessment did not including operating systems or network hardware.
	Data hub connection testing with Department of Veterans Affairs	Tests performed include connectivity tests and performance tests.
	Data hub security control assessment	Application testing of the data hub, including operating systems and network hardware.
December 2013	Third FFM security control assessment	Partial application testing of the deployed FFM eligibility and enrollment module, but not including operating systems or network hardware.

Date	Test Performed	Scope
March 2014	Fourth FFM security control assessment	Application testing of the deployed FFM eligibility and enrollment and plan management modules, but not including operating systems or network hardware.
June 2014	Fifth FFM security control assessment	Testing of specific system-level components supporting the FFM, including system configuration settings and network vulnerability testing.

However, these controls assessments did not effectively identify and test all relevant security controls prior to deploying the IT systems supporting Healthcare.gov.

The security control assessments for the FFM did not include tests of the full suite of security controls specified by NIST and CMS. The contractor that conducted these assessments reviewed only the security controls that CMS selected. This testing did not include agency policy and procedures, incident response controls, many of the controls specified for physical and environmental protection, and CMS security program management controls.

CMS could not demonstrate that it had tested all the security controls specified in the October 2013 system security plan for protecting the FFM. Neither the test plan nor the final report of the September 2013 security control assessment states specifically which controls were tested at that time. CMS did not test all of the FFM's components before deployment and did not test them all on an integrated system. Because the eligibility and enrollment module was the only one that was to become operational on October 1, 2013, it was the only FFM module that the contractors tested. Because extensive software development activities were still underway, CMS allowed only very limited independent testing by its contractors. Testing of all deployed eligibility and enrollment modules and plan management modules did not take place until March 2014.

FFM testing remained incomplete as of June 2014. While CMS took steps to address security at specific layers and in specific segments, it had not ensured that controls worked effectively for the entire system. For example, CMS had not yet adequately considered the role of "inherited" controls on the security of the FFM. In tests in August, September, and December of 2013, and March 2014, CMS declared operating system and network infrastructure controls—inherited from the underlying cloud-based services system—as being out of scope for security controls

assessments, or explicitly assumed they were adequate. However, the effectiveness of these inherited controls for the FFM and other Healthcare.gov supporting systems was not confirmed in the FFM testing.

Without comprehensive testing, CMS does not have reasonable assurance that its security controls for the FFM are working as intended, increasing the risk that attackers could compromise the confidentiality, integrity, or availability of the system.

CMS did not establish an alternate processing site to protect against major disruptions

FISMA requires agencies to develop plans and procedures to ensure continuity of operations for IT systems that support their operations and assets. A continuity of operations plan helps ensure that an organization's mission-essential functions can continue during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from the disruption while preserving access to vital information.

NIST has issued guidance that provides agencies with detailed instructions on implementing the provisions of FISMA. For Healthcare.gov and its related systems, which CMS has rated at the "moderate" risk level, NIST guidance requires that a contingency plan be prepared, alternative processing and storage sites established, and information system backup, recovery, and reconstitution procedures implemented to ensure that operations can continue in the event of a disruption.[56] According to NIST guidance, the contingency plan should include a strategy to recover and perform system operations at an alternate facility for an extended period to ensure continuity of operations. Moreover, operations at the alternate site should be governed by an agreement that details the agency's specific needs, including disaster declaration, site availability, information system requirements, security requirements, records management, and service-level management. These alternate facilities must at least have adequate space and infrastructure to support recovery activities, and may contain some or all of the necessary system hardware, software, telecommunications, and power sources.

---

[56]NIST, *Contingency Planning Guide for Federal Information Systems*, SP 800-34 Revision 1 (Gaithersburg, Md., May 2010).

CMS developed and documented contingency plans for the FFM and data hub. In these plans, CMS identified the activities, resources, responsibilities, and procedures needed to carry out operations during prolonged interruptions of the systems and outlined coordination with other stakeholders participating in contingency activities. 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 after a disaster situation. In these plans, CMS designated a facility as its "warm" disaster recovery site,[57] to hold mirrored databases, servers, and daily replicated enterprise data of its critical IT systems.

However, as noted in the FFM and data hub contingency plans, as of March 2014, the warm disaster recovery site had not yet been established. According to CMS, the data supporting the FFM are being backed up to the designated site, but backup systems are not otherwise supported there, limiting that facility's ability to support disaster recovery efforts. CMS officials stated that the agency is working with a new contractor to establish an alternate recovery site for all Healthcare.gov-related systems, which they said is expected to be operational in the fall of 2014. However they did not provide documentation confirming these plans. Until a designated alternate site is in place and fully operational, CMS remains unprepared to mitigate and recover from a disaster that threatens the availability of vital information.

Control Weaknesses Continue to Threaten Information and Systems Supporting Healthcare.gov

A basic management objective for any organization is to protect confidentiality, integrity, and availability of the information and systems that support its critical operations and assets. Organizations accomplish this by designing and implementing access and other controls that are intended to protect information and systems from unauthorized disclosure, modification, and loss. Specific controls include, among other things, those related to identification and authentication of users, authorization restrictions, and configuration management.

---

[57]According to NIST 800-34, warm disaster recovery sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources for operational readiness in the event of a disaster. However, the equipment is not loaded with the software or data required to operate the system. Recovery to a warm site can take several hours to several days, depending on system complexity and the amount of data to be restored.

CMS did not effectively implement or securely configure key security tools and devices on the systems supporting HealthCare.gov to sufficiently protect the users and information on the system from threats to confidentiality, integrity and availability. For example:

- CMS did not always require or enforce strong password controls on systems supporting the FFM. NIST Special Publication 800-53 recommends and CMS policy sets standards for minimum password length and complexity. Without strong password controls, an attacker attempting to compromise the FFM would have a greater chance of being able to compromise user credentials and access the system.

- CMS did not restrict systems supporting the FFM from accessing the Internet. NIST Special Publication 800-53 recommends that information systems be configured to only provide essential capabilities and functions. However, systems supporting the FFM that we reviewed were able to access the public Internet. Allowing these systems to access the Internet may allow for unauthorized users to access data from the FFM network, increasing the risk that an attacker with access to the FFM could send data to an outside system, or that malware could communicate with a command and control server.

- CMS did not consistently implement patches for several FFM systems. NIST Special Publication 800-53 recommends that organizations test and install newly-released security patches, service packs, and hot fixes. However, CMS did not consistently apply patches to critical systems or applications in a timely manner. Also, several critical systems had not been patched or were no longer supported by their vendors. By not keeping current with security patches, CMS faces an increased risk that servers supporting the FFM could be compromised through exploitation of known vulnerabilities.

- CMS's contractor had not securely configured its administrative network properly. NIST Special Publication 800-53 recommends how such a network should be configured. Without adhering to NIST recommendations, CMS may face an increased risk of unauthorized access to the FFM network.

In addition to the above weaknesses, we identified other security weaknesses in controls related to boundary protection, identification and authentication, authorization, and software updates that limit the effectiveness of the security controls on the systems supporting

HealthCare.gov and unnecessarily place sensitive information at risk of unauthorized disclosure, modification or exfiltration. CMS officials stated that it was difficult to ensure that a system as large and complex as the FFM had no vulnerabilities and that performing assessments to identify vulnerabilities as we did was useful. The control weaknesses we identified during this review are described in a separate report with limited distribution.

Security and Privacy Weaknesses Resulted from CMS Not Establishing a Shared Understanding of How Security Was Implemented for Healthcare.gov-related Systems

One cause of the previously discussed weaknesses is that CMS did not ensure that the multiple entities contributing to the development of the FFM all shared the same understanding of how security controls were implemented. For a complex system of systems like Healthcare.gov, it is important that all participants in the development of the system—both agency officials and contractor staff—share the same understanding of the system's security architecture.[58] Such an understanding is important to ensuring that security controls function effectively as a cohesive whole. Without it, vulnerabilities can exist in the system that may escape the notice of individual system developers. Many of the vulnerabilities identified during our technical controls assessment may be due to the fact that different contractors working on the system had conflicting views on how security controls for Healthcare.gov were to work.

NIST guidelines note that, for complex information systems, knowledge of the security properties of individual subsystems does not necessarily provide complete knowledge of the security properties of the entire system. Controls that are effective within one subsystem may be less adequate when interconnections with other subsystems are taken into account, and an individual subsystem may depend on security controls that are inherited from other systems or the infrastructure the subsystem is built on to provide adequate protection. Accordingly, NIST states that, to be effective, security controls must be mutually supporting, employed with realistic expectations for effectiveness, and implemented as part of an explicit, information system-level security architecture. NIST also notes that, when applying controls, agencies should consider any implementation issues related to the integration or interfaces between

---

[58]A security architecture describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. [NIST, *Managing Information Security Risk*, SP 800-39 (Gaithersburg, Md.: March 2011)].

common, hybrid, and system-specific controls. It recommends that an agency ensure that there are effective communications among the entities providing security capabilities to and receiving security capabilities from others.

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. Although responsibility for implementing security controls for the FFM is spread across multiple systems and parties, CMS officials stated that no one individual was responsible for ensuring consistency of the security controls across the entire system. The Consumer Information and Insurance Systems Group Information System Security Officer stated that the agency generally relied on its contractor security control assessors to have an integrated awareness of the system's overall security posture. However, these assessors had only limited access to the FFM at any given point in time and tested elements of the system only incrementally.

Further, CMS and its contractors did not agree on security responsibilities. For example, although CMS identified one subcontractor as being responsible for managing firewall rules, that responsibility was not included in the subcontractor's statement of work, and staff for the subcontractor indicated it was the responsibility of a different contractor. In another instance, the contractor responsible for managing database accounts said they were unable to do so properly due to large numbers of accounts held by other contractors or users at CMS, and a lack of communication from those entities regarding which accounts were still needed and which could be terminated.

Without ensuring that all parties responsible for the FFM's security controls agree on security roles and responsibilities and share the same understanding of how controls are implemented, the controls may not function as intended, increasing the risk that attackers could compromise the confidentiality or integrity of the system and the data it contains.

Conclusions

Healthcare.gov and its related systems represent a complex system of systems that interconnect a broad range of federal agency systems, state agencies and systems, and other entities, such as contractors and issuers of qualified health plans.

In developing Healthcare.gov and its supporting systems and establishing connections with federal and state partners, CMS took important steps to

help ensure that the site and the PII it maintains are protected from unauthorized access or misuse. However, a system with this degree of complexity and involving such a sizeable number of interconnections can pose many security and privacy risks. CMS did not take all reasonable steps to limit those risks. Security and privacy plans were missing relevant elements, and security testing was incomplete. A number of control weaknesses pose unnecessary and increased security risks to the FFM, interconnected systems, and information. Until it addresses shortcomings in both the technical security controls and its information security program, CMS is exposing Healthcare.gov-related data and its supporting systems to significant risks of unauthorized access, use, disclosure, modification, and disruption.

Recommendations for Executive Action

To fully implement its information security program and ensure that PII contained in its systems is being properly protected from potential privacy threats, we recommend that the Secretary of Health and Human Services direct the Administrator of the Centers for Medicare & Medicaid Services to implement the following six recommendations:

1. Ensure that the system security plans for the FFM and data hub contain all the information recommended by NIST.

2. Ensure that all privacy risks associated with Healthcare.gov are analyzed and documented in their privacy impact assessments.

3. Develop separate computer matching agreements with OPM and the Peace Corps to govern the data that is being compared with CMS data for the purposes of verifying eligibility for the advance premium tax credit 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 controls reviews, to better ensure that communications between individuals and entities with responsibility for the security of the FFM and its supporting infrastructure are effective.

In a separate report with limited distribution, we are also making 22 recommendations to resolve technical information security weaknesses

related to access controls, configuration management, and contingency planning.

Agency Comments and Our Evaluation

We sent draft copies of this report to the eight agencies covered by our review, as well as Experian Information Solutions. We received written responses from the Departments of Health and Human Services (HHS) and Veterans Affairs. HHS fully or partially concurred with all of GAO's recommendations. Further, the Department of Veterans Affairs stated that it generally concurred with our conclusions. These comments are reprinted in appendices II and III.

In addition, on August 27, 2014, we received technical comments via e-mail from the following: (1) the Senior Advisor to Director within the Internal Revenue Service's Office of Governmental Liaison, Disclosure & Safeguards; (2) the Social Security Administration's Chief of Staff; and (3) a program manager within Experian Information Solutions' Cybersecurity Solutions Operations office. Further, on August 28, 2014, a program analyst from the GAO-OIG Liaison Office within the Department of Homeland Security also provided us with technical comments in an e-mail. Finally, on August 29, 2014, a program analyst within the Office of Personnel Management's Merit System Accountability and Compliance - Internal Oversight & Compliance office also provided us with technical comments in an e-mail. All of the technical comments received were incorporated into the draft as appropriate.

Further, on August 25, 2014 and August 29, 2014, respectively, an official from the Peace Corps' Office of Congressional Relations and from the Department of Defense's Office of Inspector General indicated via e-mail that both agencies had no comments on the report.

In its written comments, HHS noted that the Centers for Medicare & Medicaid Services (CMS) developed the Healthcare.gov related systems consistent with federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. Further, HHS stated that CMS did not concur with our draft finding that it accepted significant security risks when it granted the FFM and the data hub an Authority to Operate in September 2013 and allowed states to connect to the data hub. The basis for CMS' view was that (1) independent security testing had been completed on the data hub and the pieces of the FFM that went live on October 1, 2013, with no open high findings, and (2) every state that connected to the data hub had adhered to CMS security procedures. However, we disagree that

these facts justify the conclusion that CMS accepted no significant risks in authorizing the systems to operate in September 2013. The fact that CMS's security contractor had not been able to test all of the security controls for the FFM in one complete version of the system meant that there was an increased risk that undetected security control deficiencies could lead to a compromise that jeopardizes the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. Also, four of the states that were granted an authority to operate were given only interim authorizations because of issues such as: (1) high-risk findings remaining open from security testing, (2) a large number of lower risk findings remaining open from testing, or (3) the lack of a third-party independent security assessment. We believe such shortcomings also posed an increased risk that a compromise could occur to the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. Thus we continue to believe that CMS accepted significant risks in approving Healthcare.gov operations in September 2013.

In response to our 28 recommendations, HHS concurred with three of the six recommendations to fully implement its information security program and all 22 of the recommendations to improve the effectiveness of its information security controls. It also provided information regarding specific actions the agency has taken or plans on taking to address these recommendations. We also received technical comments from HHS, which have been incorporated into the final report as appropriate.

HHS partially concurred with our three remaining information security program-related recommendations. Specifically, regarding our recommendation to ensure that the system security plans for the FFM and Hub contain all the information recommended by NIST, HHS noted that CMS has a master security plan that identifies all of its agency-level controls but acknowledged that the system security plans for the FFM and data hub did not adequately document inherited agency-level controls. We continue to believe that it is important for the system security plans to include all information recommended by NIST, including the system's authorization boundary and explanations for why controls listed in NIST's guidance are not being implemented, elements that were missing from the FFM security plan. CMS stated that it would update its plans to include inherited security controls.

Regarding our recommendation to ensure that all privacy risks associated with HealthCare.gov are analyzed and documented in privacy impact assessments (PIA), CMS partially concurred, stating that the PIAs for the FFM and the data hub were created using the HHS PIA template, which
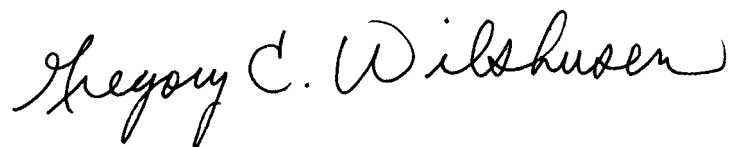
go beyond the requirements set by the Office of Management and Budget guidance on PIAs. However, OMB guidance for implementing the privacy provisions of the E-Government Act of 2002 (OMB Memorandum M-03-22) requires PIAs to include an analysis of privacy risks, and the CMS PIAs did not include such an analysis. Without it, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems. We continue to believe the PIAs should include an analysis of all privacy risks associated with HealthCare.gov operations.

Regarding our recommendation to perform a comprehensive security assessment of the FFM, including the infrastructure, platform, and all deployed software elements, CMS concurred that comprehensive security assessments are important, but disagreed that the infrastructure, platform, or software elements had not been tested. It noted that a security control assessment was completed separately for the infrastructure as a service and platform as a service that host FFM systems, and authorities to operate were granted, on November 23, 2012, and January 25, 2013, respectively. HHS also noted that FFM security controls were tested again in June 2014. We have updated the report to include the tests to which CMS referred. However, we continue to believe that while CMS took steps to address security at specific layers, it did not ensure that controls worked effectively for the entire system and did not adequately document the role of inherited controls in the security of the FFM. NIST guidelines on managing information security risk (Special Publication 800-39) note that security controls that are effective within one subsystem may be less adequate when interconnections with other subsystems are taken into account and that such controls must be mutually supporting and employed with realistic expectations for effectiveness. Thus we continue to believe that a comprehensive assessment of the security of the FFM is warranted to ensure that the security controls for the FFM are adequate.

We are sending copies of this report to the Departments of Defense, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs, as well as the Office of Personnel Management, the Peace Corps, and the Social Security Administration.

Should you or your staffs have questions on matters discussed in this report, 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. Contact points for our

Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Gregory C. Wilshusen
Director, Information Security Issues

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

The Honorable Ron Wyden
Chairman
The Honorable Orrin Hatch
Ranking Member
Committee on Finance
United States Senate

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Lamar Alexander
Ranking Member
Committee on Health, Education, Labor and Pensions
United States Senate

The Honorable Jon Tester
Chairman
Subcommittee on Efficiency and Effectiveness of Federal
Programs and the Federal Workforce
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Claire McCaskill
Chairman
Subcommittee on Financial and Contracting Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Darrell Issa
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Dave Camp
Chairman
The Honorable Sander M. Levin
Ranking Member
Committee on Ways and Means
House of Representatives

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Mike Coffman
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

The Honorable Charles Boustany, Jr.
Chairman
The Honorable John Lewis
Ranking Member
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

The Honorable Mark Begich
United States Senate

The Honorable Michael Bennet
United States Senate

The Honorable Richard Blumenthal
United States Senate

The Honorable Robert P. Casey, Jr.
United States Senate

The Honorable Al Franken
United States Senate

The Honorable Kay R. Hagan
United States Senate

The Honorable Tim Kaine
United States Senate

The Honorable Amy Klobuchar
United States Senate

The Honorable Mary Landrieu
United States Senate

The Honorable Joe Manchin III
United States Senate

The Honorable Jeffrey A. Merkley
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable Mark Pryor
United States Senate

The Honorable Jeanne Shaheen
United States Senate

The Honorable John Thune
United States Senate

The Honorable Mark Udall
United States Senate

The Honorable Mark R. Warner
United States Senate

The Honorable Ron Barber
House of Representatives

The Honorable John Barrow
House of Representatives

The Honorable Tulsi Gabbard
House of Representatives

The Honorable Pete P. Gallego
House of Representatives

The Honorable Duncan Hunter
House of Representatives

The Honorable Mike Kelly
House of Representatives

The Honorable Ann McLane Kuster
House of Representatives

The Honorable Daniel W. Lipinski
House of Representatives

The Honorable Patrick E. Murphy
House of Representatives

The Honorable Scott Peters
House of Representatives

The Honorable Kyrsten Sinema
House of Representatives

The Honorable Filemon Vela
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the planned exchanges of information between the Healthcare.gov website, supporting information technology (IT) systems, and the federal, state, and other organizations that are providing or accessing the 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 the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS) to protect the security and privacy of the information and the major IT systems used to support Healthcare.gov.

To address our first objective, we reviewed the Patient Protection and Affordable Care Act (PPACA) and other relevant laws to identify the responsibilities of CMS and other federal agencies for establishing and participating in healthcare coverage marketplaces. We reviewed and analyzed system and security documentation, including interagency agreements, with each partnering entity in order to identify interconnections between Healthcare.gov and other external partners that are providing or accessing information to support enrollment processes for Healthcare.gov. Further, we obtained documentation and interviewed officials at the following federal agencies that directly support implementation of Healthcare.gov: the Department of Defense (DOD), Homeland Security (DHS), and Veterans Affairs (VA), as well as CMS, Experian Information Solutions, the Internal Revenue Service (IRS), the Office of Personnel Management (OPM), the Peace Corps, and the Social Security Administration (SSA). We also received a demonstration of the online Healthcare.gov system, which we used to corroborate the information flow described to us by agency officials and in official documentation. Based on an analysis of the information we received, we described the major types of data connections that are currently in place or planned between systems maintained by CMS to support Healthcare.gov and other internal and external systems. We also reviewed requirements set forth in the Internal Revenue Code, PPACA, and implementing guidance regarding the handling of taxpayer data to describe how IRS and CMS policies and procedures for sharing tax data adhere to legal requirements.

To address our second objective, we reviewed relevant information security and privacy laws, guidance, and National Institute of Standards and Technology (NIST) standards and guidance to identify federal security and privacy control requirements. We compared CMS's security and privacy policies and procedures to determine their adherence to federal requirements. We then assessed the implementation of controls over Healthcare.gov and its supporting systems and interconnections by

reviewing risk assessments, security plans, system control assessments, contingency plans, and remedial action plans. To determine the effectiveness of the information security controls for the Federally Facilitated Marketplace (FFM), we analyzed the overall network control environment, identified interconnectivity and control points, and reviewed controls for the network and servers supporting the FFM. Specifically, we reviewed controls over the FFM application and its supporting software, the operating systems, network and computing infrastructure provided by the supporting platform as a service, and infrastructure as a service systems.

To evaluate CMS's controls over its information systems supporting Healthcare.gov, we used our Federal Information System Controls Audit Manual, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; NIST standards and guidelines; National Security Agency guidance; Center for Information Security guidance; and agency policies, procedures, practices, and standards.

Specifically, we

- reviewed network access paths to determine if boundaries had been adequately protected;
- reviewed the complexity and expiration of password settings to determine if password management was being enforced;
- analyzed users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewed software security settings to determine if modifications of sensitive or critical system resources had been monitored and logged;
- examined configuration settings and access controls for routers, network management servers, switches, and firewalls; and
- inspected the operating system and application software on key servers and workstations to determine if critical patches had been installed and/or were up-to-date.
- Aspects of our review of controls on the infrastructure supporting Healthcare.gov were limited because they involved shared system elements in a cloud environment. Regarding the CMS infrastructure as a service contract with its contractor, we only reviewed those elements of the environment that were dedicated to CMS's use. Consequently, it is possible our review may either have not identified

certain controls that would compensate for the weaknesses we
identified, that weaknesses remain in the system that we did not
identify, or both.

Using the requirements established by the Federal Information Security
Management Act of 2002 and associated NIST and agency guidelines,
we evaluated CMS's information security program, as it related to
Healthcare.gov, by:

- reviewing agency policies and procedures to determine the extent to
  which they addressed roles and responsibilities for information
  security, incident response, and flaw remediation;
- reviewing the system security plans for the FFM and the data hub to
  determine the extent to which they addressed elements
  recommended by NIST;
- reviewing the interconnection security agreements between CMS and
  DHS, DOD, IRS, SSA, and VA to determine the extent to which they
  addressed elements recommended by NIST;
- reviewing the security control assessments for the FFM to determine
  the extent to which they complied with NIST guidance;

We performed our work at CMS headquarters in Baltimore, Maryland; and
at contractor facilities in Dallas, Texas; and in Reston and Chantilly,
Virginia.

To determine the extent to which CMS had addressed privacy concerns
in the development and operation of Healthcare.gov and its supporting
systems, we compared the requirements of the Privacy Act of 1974 and
E-Government Act of 2002 and associated guidance with privacy
documentation, such as system of records notices and privacy impact
assessments, for the FFM, data hub, and other systems that support
Healthcare.gov. We also compared requirements of the Computer
Matching Act with computer matching agreements CMS established with
DHS, DOD, IRS, SSA, and VA, and the data transfer arrangements CMS
made with OPM and the Peace Corps.

We conducted this performance audit from December 2013 to September
2014 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.

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen and Dr. Barkakati,

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "HealthCare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls" (GAO-14-730).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

<u>**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "HEALTHCARE.GOV: ACTIONS NEEDED TO ADDRESS WEAKNESSES IN INFORMATION SECURITY AND PRIVACY CONTROLS" (GAO-14-730)**</u>

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on this draft report.

The privacy and security of consumers' personally identifiable information (PII) are a top priority for HHS and CMS. As part of that effort, and as noted in GAO's draft report, within HHS, CMS has taken many steps and implemented several security controls to secure PII related to the Federally-Facilitated Marketplace (FFM) and its supporting databases. CMS developed the Marketplace systems consistent with federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. Components of the website that are operational have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institute of Standards and Technology (NIST). Marketplace systems are also in compliance with all the relevant privacy and security statutes, including the Privacy Act. Additionally, the Internal Revenue Service accepted the CMS Safeguard Procedures Report as certification that the confidentiality of federal tax information disclosed to CMS would be adequately protected.

In addition to the security controls examined by GAO in this report, CMS has implemented other measures to protect PII, including penetration testing, which happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. As part of the ongoing testing process, and in line with federal and industry standards, any open risk findings are appropriately addressed with risk mitigation strategies and compensating controls. The security of the system is also monitored by sensors and other tools to deter and prevent unauthorized access. CMS conducts continuous monitoring using a 24/7, multi-layer IT professional security team, added penetration testing, and a change management process that includes ongoing testing and mitigation strategies implemented in real time. These layered controls help protect the privacy and security of PII related to the FFM.

CMS acknowledges that risks exist inherently for every IT system, and appreciates GAO's suggestion of controls and processes that could be improved to further reduce or mitigate risk.

Government Accountability Office Findings

CMS does not concur with GAO's finding that CMS accepted significant security risks when it granted the FFM and the Hub an Authority to Operate (ATO) in September 2013 and allowed states to connect to the Hub. CMS does not concur for the following reasons:

The Hub completed its independent Security Controls Assessment with no high findings on August 23, 2013, and received an ATO on September 6, 2013. The completion of this testing confirms that the Hub complies with federal standards and that HHS and CMS have implemented the appropriate procedures and safeguards necessary for the Hub to operate securely beginning October 1, 2013.

1

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN
SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO)
DRAFT REPORT ENTITLED, "HEALTHCARE.GOV: ACTIONS NEEDED TO
ADDRESS WEAKNESSES IN INFORMATION SECURITY AND PRIVACY
CONTROLS" (GAO-14-730)**

Additionally, CMS leadership issued an ATO on September 27, 2013, to operate the FFM
application. The initial authorization was limited to six months and was conditioned on a
number of strategies to mitigate risks outlined in the ATO, including regular testing that exceeds
best practices. As GAO notes, the risk mitigation strategies and compensating controls that were
prescribed were implemented and executed as planned.

An independent security control assessor tested each piece of the FFM that went live October 1,
2013, prior to that date with no open high findings. All high, moderate, and low security risk
findings for the portions of the website that launched October 1 were either fixed or had
strategies and plans that met industry standards in place to fix the findings. The September 3,
2013, ATO identified in the report was only for the Qualified Health Plan and Dental Modules of
the website. This September 3, 2013, ATO is separate from the September 27, 2013, ATO for
the FFM and the parts of the website that launched on October 1.

Finally, in keeping with industry practice, CMS established strong security controls and
standards for each state to meet in order to connect to the Hub. These controls and standards are
based on federal security guidelines. Each state had to sign a Computer Matching Agreement, an
Interconnection Security Agreement, and an Information Exchange Agreement, all of which bind
the state to rules and operating procedures related to data security and privacy. Additionally,
each state was required to complete a security plan, a risk assessment which can either be a self-
assessment or a third-party assessment, and a corrective action plan to address risks. Every state
that was connected to the Hub adhered to these procedures.

CMS acknowledges that it accepted risk in authorizing the FFM to operate or authorizing states
to connect to the Hub. However, it disagrees with GAO's classification of the risk as
"significant." Every system operates under some level of risk. The purpose of an ATO, as
described in NIST 800-18, is to have a senior management official accept the associated risk of
authorizing a system to process information.

GAO Recommendation
Ensure that the system security plans for the FFM and Hub contain all the information
recommended by NIST.

CMS Response
CMS partially concurs with the recommendation. CMS notes that the CMS Master Security Plan
identifies all the agency-level common controls at CMS and these controls were tested on
September 6, 2013. Additionally, the Enterprise Information Security Group within the CMS
Office of Information Services owns and tests inheritable agency level controls. These are tested
on a regular basis as required by NIST. The system security plans of those systems inheriting the
common controls (FFM and Hub) did not adequately document those inherited controls, which
CMS will correct.

GAO Recommendation

2

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN
SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO)
DRAFT REPORT ENTITLED, "HEALTHCARE.GOV: ACTIONS NEEDED TO
ADDRESS WEAKNESSES IN INFORMATION SECURITY AND PRIVACY
CONTROLS" (GAO-14-730)

Ensure that all privacy risks associated with HealthCare.gov are analyzed and documented in
their privacy impact assessments (PIAs).

CMS Response
CMS partially concurs with the recommendation. As GAO notes, CMS developed and
documented PIAs for the FFM and the Hub and will have the MIDAS PIA completed before the
next open enrollment period begins. The PIAs for the FFM and the Hub were created using the
HHS PIA template, which contains a series of questions that must be answered in the PIA to
meet the requirements under Section 208 of the eGov Act. The HHS PIA template, which is
used for the FFM and the Hub, asks for additional information, going beyond the requirements
set by the Office of Management and Budget (OMB) Guidance on privacy impact assessments
(M-03-22).

GAO Recommendation
Develop separate computer matching agreements with Office of Personnel Management (OPM)
and the Peace Corps to govern the data that is being compared with CMS data for the purposes of
verifying eligibility for advance premium tax credits and cost-sharing reductions.

CMS Response
CMS concurs with this recommendation and will commence discussions with OPM and Peace
Corps.

GAO Recommendation
Perform a comprehensive security assessment of the FFM including the infrastructure, platform,
and all deployed software elements.

CMS Response
CMS concurs that comprehensive security assessments are important, and CMS will continue to
test functionality as they become operational through quarterly Security Control Assessments
(SCA). CMS disagrees that the infrastructure, platform, or software elements were not tested.
An SCA was completed separately for the Infrastructure as a Service and Platform as a Service
that host FFM systems, and ATOs were granted, on November 23, 2012, and January 25, 2013,
respectively. Another SCA for the infrastructure and platform will be conducted in October
2014. Additionally, in June 2014, the FFM security controls were tested for the fifth time. This
test included the application servers and gateway and border devices.

CMS conducts end-to-end comprehensive SCAs in the FFM that are above industry standards.
In December 2013, there was a comprehensive FFM SCA that met all industry standards, was an
end-to-end test and was conducted in a stable environment with no open high findings. Another
comprehensive end-to-end test will be conducted in September 2014, which will test security for
open enrollment and plan year functionality.

GAO Recommendation

3

<u>**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN
SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO)
DRAFT REPORT ENTITLED, "HEALTHCARE.GOV: ACTIONS NEEDED TO
ADDRESS WEAKNESSES IN INFORMATION SECURITY AND PRIVACY
CONTROLS" (GAO-14-730)**</u>

Ensure that the planned alternate processing site for the systems supporting HealthCare.gov is
established and made operational in a timely fashion.

<u>**CMS Response**</u>
CMS concurs with this recommendation. Under a contract with Hewlett-Packard, the backup site
is being developed and will be operational by next year. Until then, there is a limited disaster
management site.

<u>**GAO Recommendation**</u>
Establish detailed security roles and responsibilities for contractors, including participation in
security controls reviews, to better ensure that communications between individuals and entities
with responsibility for the security of the FFM and its supporting infrastructure are effective.

<u>**CMS Response**</u>
CMS concurs with this recommendation. The CMS Chief Information Officer and Chief
Information Security Officer have a unified and comprehensive view of the security of the
Marketplace, and work to better ensure that the individuals and entities responsible for the
security of the FFM and its supporting system are managed and informed as appropriate. CMS
ensured a shared understanding of FFM security when appropriate by using the same security
contractor and testing team member for all related security testing including for infrastructure,
platform, and cyclical audits. Additionally, the independent test team had a shared knowledge of
the development of the system and application. CMS balanced the shared understanding with
the FISMA-identified fundamental principles of "need to know" and "separation of duties."

<u>**GAO Recommendation**</u>
In a separate report, GAO made 22 technical recommendations.

<u>**CMS Response**</u>
CMS concurred with all of the technical recommendations. Of the 22 technical
recommendations, 19 have been resolved, fully mitigated, or will be further reviewed prior to
open enrollment. The remaining open findings are being remediated and will be closed by the
middle of September.

4

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

September 3, 2014

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, *"HEALTHCARE.GOV: Actions Needed to Address Weaknesses in Information Security and Privacy Controls"* (GAO-14-729SU). VA generally agrees with GAO's conclusions.

The enclosure provides technical comments to the draft report. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Jose D. Riojas
Chief of Staff

Enclosure

Appendix IV: GAO Contacts and Staff Acknowledgements

GAO Contacts	Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov Gregory C. Wilshusen (202) 512-6244, wilshuseng@gao.gov
Staff Acknowledgments	In addition to the contacts named above, John de Ferrari, Lon Chin, West Coile and Duc Ngo (assistant directors), Mark Canter, Marisol Cruz, Sandra George, Nancy Glover, Torrey Hardee, Tammi Kalugdan, Monica Perez-Nelson, Justin Palk, and Michael Stevens made key contributions to this report.