United States Government Accountability Office

Report to Congressional Committees

September 2020

INFORMATION SECURITY AND PRIVACY

HUD Needs a Major Effort to Protect Data Shared with External Entities

Accessible Version

GAO-20-431

GAO Highlights

Highlights of GAO-20-431, a report to congressional committees

Why GAO Did This Study

To administer housing, community investment, and mortgage loan programs, HUD collects a vast amount of sensitive personal information and shares it with external entities, including federal agencies, contractors, and state, local, and tribal organizations. In 2016, HUD reported two incidents that compromised sensitive information.

House Report 115-237, referenced by the Consolidated Appropriations Act, 2018, included a provision for GAO to evaluate HUD's information security framework for protecting information within these programs. The objectives were to (1) assess the effectiveness of HUD's policies and procedures for overseeing the security and privacy of sensitive information exchanged with external entities; and (2) determine the extent to which HUD was able to identify external entities that process, store, and share sensitive information with applicable systems. GAO compared HUD's policies and practices for systems' security and privacy to four leading practices identified in federal legislation and guidance. GAO also assessed HUD's practices for identifying external entities with access to sensitive information.

What GAO Recommends

GAO is making five recommendations to HUD to fully implement the four leading practices and fully identify the extent to which sensitive information is shared with external entities.

HUD did not agree or disagree with the recommendations, but described actions intended to address them.

View GAO-20-431. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

September 2020

INFORMATION SECURITY AND PRIVACY

HUD Needs a Major Effort to Protect Data Shared with External Entities

What GAO Found

The Department of Housing and Urban Development (HUD) is not effectively protecting sensitive information exchanged with external entities. Of four leading practices for such oversight, HUD did not address one practice and only minimally addressed the other three in its security and privacy policies and procedures (see table). For example, HUD minimally addressed the first leading practice because its policy required federal agencies and contractors with which it exchanges information to implement risk-based security controls; however, the department did not, among other things, establish a process or mechanism to ensure all external entities complied with security and privacy requirements when processing, storing, or sharing information outside of HUD systems. HUD's weaknesses in the four practices were due largely to a lack of priority given to updating its policies. Until HUD implements the leading practices, it is unlikely that the department will be able to mitigate risks to its programs and program participants.

Extent to Which the Department of Housing and Urban Development (HUD) Policies and Procedures Address Leading Practices for Overseeing the Protection of Sensitive Information

Practice	Rating
Require risk-based security and privacy controls	minimally addressed
Independently assess implementation of controls	not addressed
Identify and track corrective actions needed	minimally addressed
Monitor progress implementing controls	minimally addressed

Legend: ◔=Minimally addressed—leading practice was addressed to a limited extent; ○=Not addressed—leading practice was not addressed.

Source: GAO analysis of HUD data. | GAO-20-431

HUD was not fully able to identify external entities that process, store, or share sensitive information with its systems used to support housing, community investment, or mortgage loan programs. HUD's data were incomplete and did not provide reliable information about external entities with access to sensitive information from these systems. For example, GAO identified additional external entities in system documentation beyond what HUD reported for 23 of 32 systems. HUD was further limited in its ability to protect sensitive information because it did not track the types of personally identifiable information or other sensitive information shared with external entities that required protection. This occurred, in part, because the department did not have a comprehensive inventory of systems, to include information on external entities. Its policies and procedures also focused primarily on security and privacy for internal systems and lacked specificity about how to ensure that all types of external entities protected information collected, processed, or shared with the department. Until HUD develops sufficient, reliable information about external entities with which program information is shared and the extent to which each entity has access to personally identifiable information and other sensitive information, the department will be limited in its ability to safeguard information about its housing, community investment, and mortgage loan programs.

Contents

Tables

Figure

Abbreviations

CIO	chief information officer
CSAM	Cybersecurity Assessment and Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
Ginnie Mae	Government National Mortgage Association
HUD	Department of Housing and Urban Development
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	personally identifiable information

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

September 21, 2020

The Honorable Susan M. Collins
Chairman
The Honorable Jack Reed
Ranking Member
Subcommittee on Transportation,
Housing and Urban Development, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable David E. Price
Chairman
The Honorable Mario Diaz-Balart
Ranking Member
Subcommittee on Transportation, and
Housing and Urban Development, and Related Agencies
Committee on Appropriations
House of Representatives

Federal agencies, including the Department of Housing and Urban Development (HUD), are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. This can include sensitive information—that is, information which, if released or otherwise involved in a security incident, could adversely impact the department's mission, assets, responsibilities, or functions.

Sensitive information includes, but is not limited to, personally identifiable information (PII). Any information that can be used to distinguish or trace an individual's identity is PII. For example, PII can include a 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. If PII is not protected, individuals could lose the privacy to which they are entitled to have protected under law.[1]

HUD programs manage financial information and other sensitive information pertaining to tens of millions of Americans. The department's Office of Inspector General has reported that HUD maintains over one billion records containing PII for American citizens.[2]

Further, HUD operates its programs with support from a variety of external business partners—referred to in this report as "external entities."[3] Among others, these external entities include federal agencies such as the Department of the Treasury and the Internal Revenue Service; private sector financial institutions and contractors; and state, local, and tribal government agencies, such as public housing agencies.

External entities process, store, and share with HUD's IT systems, specific types of sensitive information. This can include tenants' names, Social Security numbers, dates of birth, addresses, and telephone numbers, as well as sensitive information collected from grant program participants, such as names of owners, owners' racial and income characteristics, and locations of facilities operated with grant funds.

In 2016, the department reported two privacy incidents involving its IT systems used to manage HUD programs. According to HUD, these incidents compromised personal information of members of the public, including PII for approximately 50,000 employees of private businesses and about 420,000 public housing residents.[4]

[1] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974); and E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

[2] Department of Housing and Urban Development, Office of Inspector General, *HUD Privacy Program*, 2018-OE-0001 (Washington, D.C.: September 2018).

[3] External entities include organizations external to the department (e.g., external business partners, contractors, and other organizations that do business with HUD programs).

[4] HUD reported that it removed access to the associated web pages and links as soon as the disclosures were confirmed and stated that it had no evidence that any of the records had been used inappropriately. Details about the incidents are available at https://www.hud.gov/privacy.

Subsequent to the incidents, House Report 115-237 as incorporated by the Consolidated Appropriations Act, 2018 included a provision for GAO to evaluate HUD's information security framework for protecting information related to the housing, community investment, and mortgage loan programs.[5] The specific objectives for our review were to (1) assess the effectiveness of HUD's policies and procedures for overseeing the security and privacy of sensitive information exchanged with external entities; and (2) determine the extent to which HUD was able to identify the external entities that process, store, and share sensitive information with its systems used to help administer the housing, community investment, and mortgage loan programs.

To address the first objective, we reviewed Federal Information Security Modernization Act of 2014 (FISMA) requirements;[6] Office of Management and Budget (OMB) guidance on managing federal information;[7] National Institute of Standards and Technology (NIST) information security standards and guidance;[8] and work we have done previously to identify leading practices that would be relevant to protecting sensitive

[5] House Appropriations Committee report, H.R. Rep. No. 115-237, at 100 (2017), as approved by the joint explanatory statement of the conference, 164 Cong. Rec. H2697, H2872 (daily ed. Mar. 22, 2018) (statement of Chairman Frelinghuysen), specifically referenced in section 4 of the Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, § 4, 132 Stat. 348, 350 (Mar. 23, 2018).

[6] The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[7] Office of Management and Budget, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016).

[8] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199 (Gaithersburg, Md.: February 2004); *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006); *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 1 (Gaithersburg, Md.: December 2016); and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: April 2018).

information shared with external entities.[9] Based on our previous work, the guidance identified four leading practices: (1) require the implementation of risk-based security and privacy controls, (2) independently assess the implementation of security controls, (3) develop and implement corrective actions for weaknesses identified, and (4) monitor the implementation of controls on an ongoing basis.

For this review, we examined the guidance to associate at least one subpractice with each leading practice. For example, documenting a requirement for external entities to implement risk-based security controls is a subpractice of leading practice (1)—require the implementation of risk-based security and privacy controls. Across all four of the leading practices, we identified a total of 10 subpractices for our analysis.

We then collected and reviewed the policies and procedures that HUD had in place for protecting sensitive information for the housing, community investment, and mortgage loan programs that it shared with three different groups of external entities. These external entity groups were: (1) federal agencies with which HUD established agreements to share program information, (2) contractors, such as corporations that assist HUD in administering programs or developing or managing information systems, and (3) other government, for-profit, and nonprofit organizations, such as state and local public housing agencies, lending institutions, and grantees involved with HUD's housing, community investment, and mortgage loan programs.

We compared the policies and procedures that HUD had in place for the three groups of external entities to each of the identified subpractices. This comparison enabled us to determine whether the policies and procedures addressed or did not address each subpractice. We assigned a rating to HUD's policies and procedures based on the extent to which they addressed, for each entity, what the subpractice called for using a four-point scale:

- fully addressed indicated that HUD's policies and procedures addressed the subpractice;
- substantially addressed indicated that HUD's policies and procedures addressed the subpractice to a great extent;

[9] GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*, GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

- minimally addressed indicated that HUD's policies and procedures addressed the subpractice to a limited extent; and
- not addressed indicated that HUD's policies and procedures did not address the subpractice.

Finally, to determine the overall rating for each leading practice, we averaged their subpractice ratings. For example, for one leading practice, we assigned a rating of substantially addressed to the first subpractice (two points) and ratings of minimally addressed to the other three subpractices (one point each). The average point value for the four subpractices came out to roughly one point, which equated to a "minimally addressed" rating for the overall practice.

To further supplement our analyses of the department's policies and procedures, we collected and evaluated detailed plans and documentation (e.g., system security plans) for a nongeneralizable subset of the department's information systems. To identify this subset we used systems HUD had reported as containing sensitive information, sharing information with external entities, and representing the housing and mortgage loan programs. This list contained 32 systems. Then we randomly selected four systems from this list. Although HUD did not originally report any community investment systems as containing sensitive information and sharing information with external entities, we subsequently identified one community investment system as containing sensitive information and sharing information with external entities. We added that system to our subset of systems for review. We also interviewed HUD officials responsible for the security and privacy of the department's systems.

For the second objective, we obtained from relevant HUD program offices and reviewed, information about the systems used to support the housing, community investment, and mortgage loan programs. Because HUD was not able to provide reliable data from its Cybersecurity Assessment and Management (CSAM) system[10]—the department's repository of information about its information systems' security and privacy—we also requested that the four program offices provide us with lists of the department's systems that they use which (1) contain sensitive information and (2) share information with external entities. We then compared this information to other sources of information, including the data analyzed for our first objective, HUD reports about the systems, and

[10] CSAM is a tool that was developed by the Department of Justice and offered to other agencies.

information posted on the department's websites. We found that the information the department provided was incomplete and not reliable for identifying the external entities with access to sensitive information in HUD's systems. We address these findings later in this report. In addition, we interviewed system owners about the extent to which selected systems contained sensitive information and shared information with external entities.[11] Appendix I provides a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from September 2018 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

HUD's mission is to create strong, sustainable, and inclusive communities, as well as quality, affordable homes for all. To help achieve this mission, the department operates a wide variety of programs, including those that provide rental assistance, mortgage insurance, and community development grants. For example:

- Rental housing assistance programs subsidize rents for low-income households and populations with special needs, such as older adults and persons with disabilities. Two program offices within HUD—the Office of Public and Indian Housing and the Office of Housing—carry out these programs.
- Community investment programs seek to develop viable communities by promoting integrated approaches that provide decent housing, a suitable living environment, and expanded economic opportunities for low and moderate income persons. The department's Office of Community Planning and Development operates the community investment programs.

[11] System owners are the individuals to whom HUD has assigned responsibility for the successful operation of information systems. According to the department's IT security policy, system owners are ultimately accountable for the security of their information systems.

- Mortgage loan programs are operated by the Federal Housing Administration—a component of HUD's Office of Housing—and the Government National Mortgage Association (Ginnie Mae). The Federal Housing Administration insures mortgages made by lenders to home buyers with low down payments and to developers of multifamily rental buildings containing relatively affordable units. Ginnie Mae provides an explicit federal guarantee of the performance of mortgage-backed securities that have been insured or guaranteed by federal agencies. Ginnie Mae programs incorporate borrower information about loans insured by the Federal Housing Administration, as well as information from other external entities, such as other federal mortgage organizations and private financial institutions.

The four program offices within HUD that manage the rental assistance, mortgage insurance, and community development programs account for a substantial portion of the department's operations and budgetary resources.[12] In fiscal year 2018, HUD's housing and community investment programs accounted for $50.6 billion (96 percent) of the department's total gross discretionary budget authority. For that fiscal year, HUD mortgage loan programs also generated more than $10 billion in offsetting receipts, which lowered the net budget authority needed to fund all of the department's programs and activities.[13]

HUD's housing, community investment, and mortgage loan program offices rely on PII to fulfill their missions. According to data reported from HUD, about half (96) of the department's 200 information systems support these three programs.[14]

[12] Throughout this report, we use the phrase "program offices" to refer to the offices managing relevant HUD programs, including the Office of Housing/Federal Housing Administration, the Office of Public and Indian Housing, the Office of Community Planning and Development, and Ginnie Mae.

[13] For example, the Federal Housing Administration generates offsetting receipts when it estimates that the present value of cash inflows (such as mortgage insurance premiums paid by borrowers) will exceed the present value of cash outflows (such as claim payments to lenders) for the loans insured in a fiscal year.

[14] We did not verify the accuracy of this information reported by HUD's Office of the Chief Information Officer.

HUD's Administrative Support Offices and Program Offices Have Responsibilities for Information Security and Privacy

Multiple HUD offices have responsibility for establishing and managing department-wide IT security and privacy requirements. HUD's administrative support offices provide department-wide management and support for information security and privacy, while program offices have responsibilities for information security and privacy for the programs and systems they manage.

The **Office of the Chief Information Officer (CIO)** sets policy and manages the department-wide IT security program. The Secretary of HUD has delegated responsibility for ensuring that the department's information and information systems are protected and for providing security-related support and resources to the CIO.

HUD's CIO serves as the department's cybersecurity risk executive[15] and is responsible for appointing the Chief Information Security Officer, providing security consulting assistance to HUD program offices, and evaluating the security program at least annually. The department established primary responsibility for security with the Chief Information Security Officer and the Office of IT Security.

The **Chief Information Security Officer** is responsible for directing and maintaining the HUD information security program.[16] The officer is charged with, among other things, interacting with internal and external resources; coordinating security compliance across HUD organizational elements; and serving as the CIO's primary liaison with authorizing officials, information system owners, and information security system officers.

The **Office of the CIO's Office of IT Security** is responsible for issuing department-wide information security policy and guidance for all HUD

[15] According to the department's IT security policy, roles of the risk executive include ensuring that management of information system-related security risks is consistent across HUD, reflects organizational risk tolerance, and is performed as part of a HUD-wide process that considers other organizational risks affecting mission and business success.

[16] Since December 2018, three different individuals have held the key position of Chief Information Security Officer. HUD hired a new officer in July 2019.

systems; providing oversight to ensure the policies are implemented; serving as the principal advisor on information system security matters; and reviewing and approving the processes, techniques, and methodologies planned for securing information systems. Specifically, the office has developed security policies and guidance, and implemented a system for managing security management reviews and records.

- The Office of IT Security has established department-wide security policy handbooks that replicate and closely align with guidance published by NIST.[17] The office has also established standard operating procedures (e.g., policy for managing plans of actions and milestones for identified weaknesses, performing vulnerability scanning, and responding to incidents and plans to establish additional security policy). In addition, the department's IT project planning and management process requires specific artifacts (e.g., system security plans, initial privacy assessments, and approvals of systems' authorities to operate) outlining plans for how IT security and privacy are to be addressed when developing new systems or enhancing or modernizing existing systems.
- The Office of IT Security primarily uses the CSAM system to store records on information system controls, sensitive information, and external entities that connect with HUD systems. For example, HUD program offices and system owners use CSAM to identify security controls to employ for information systems, track security reviews needed, and store security-related artifacts (e.g., system security plans, plans of actions and milestones for identified weaknesses, and the results of vulnerability scans). The Office of IT Security works with program offices and system owners to leverage CSAM to generate various reports that capture different details about the extent to which the department's systems incorporate sensitive information and exchange information with external entities.

The **Office of Administration's Privacy Office** is to protect the privacy of individuals and minimize the impact of the department's actions on privacy, while achieving HUD's mission. Since 2013, responsibility for

[17] HUD updated the security policy handbook in 2018 to align with NIST Special Publication 800-53, Revision 4 and plans to update the security procedures handbook, which was last revised in 2014.

privacy has changed twice, moving from the Office of Administration to the Office of the CIO, and then back to the Office of Administration.[18]

The office hired a Chief Privacy Officer in September 2019, to, among other things, manage the Privacy Office.[19] According to the security policy handbook, HUD's Privacy Officer is responsible for:

- establishing HUD's privacy policy and ensuring privacy compliance;
- assuring that IT services and service arrangements (e.g., contractual agreements with service providers and other external entities) meet privacy policies regarding the protection, dissemination, and disclosure of information; and
- reviewing program and system privacy analyses and assessments and system of records notices, and providing approval as appropriate.

The **Office of the Chief Procurement Officer** is responsible for ensuring that HUD's contracts for information systems and services include the appropriate information security requirements. To fulfill its responsibility, the office works with the Office of IT Security, other interested stakeholders (e.g., the program office sponsoring the acquisition), and the Office of General Counsel to develop and administer contracts. Specifically, the office develops IT security contract terms, as appropriate, based on current federal and HUD policies, regulations, and guidance.

The **Executive Risk Management Council** is composed of senior leaders from various offices to provide governance of enterprise risk management. As the department's cybersecurity risk executive, the department's CIO serves on this council. In addition, the CIO has initiated efforts to establish a new risk advisory committee designed to oversee the department's IT risk management framework, identify high-level risks

[18] In March 2020, the Office of IT Security and the Privacy Office announced plans to coordinate more closely to improve cybersecurity and privacy for the department. The Senior Agency Official for Privacy announced several planned improvement efforts, including requiring program offices to update privacy impact assessments for information systems and respond to a survey about the systems' sensitive data.

[19] From 2016 until September 2019, the department operated its privacy program with the acting Senior Agency Official for Privacy also acting as Chief Privacy Officer and overseeing operations of the Privacy Office. The new Chief Privacy Officer now reports to the Senior Agency Official for Privacy.

within the Office of the CIO programs, and coordinate with the department's risk management council.

In addition, HUD assigns certain roles and responsibilities for IT security and privacy to program offices and system owners. Programs establish requirements for external entities and oversee their compliance at the program level. Program offices vary in their approaches to overseeing external entities involved with programs. For example:

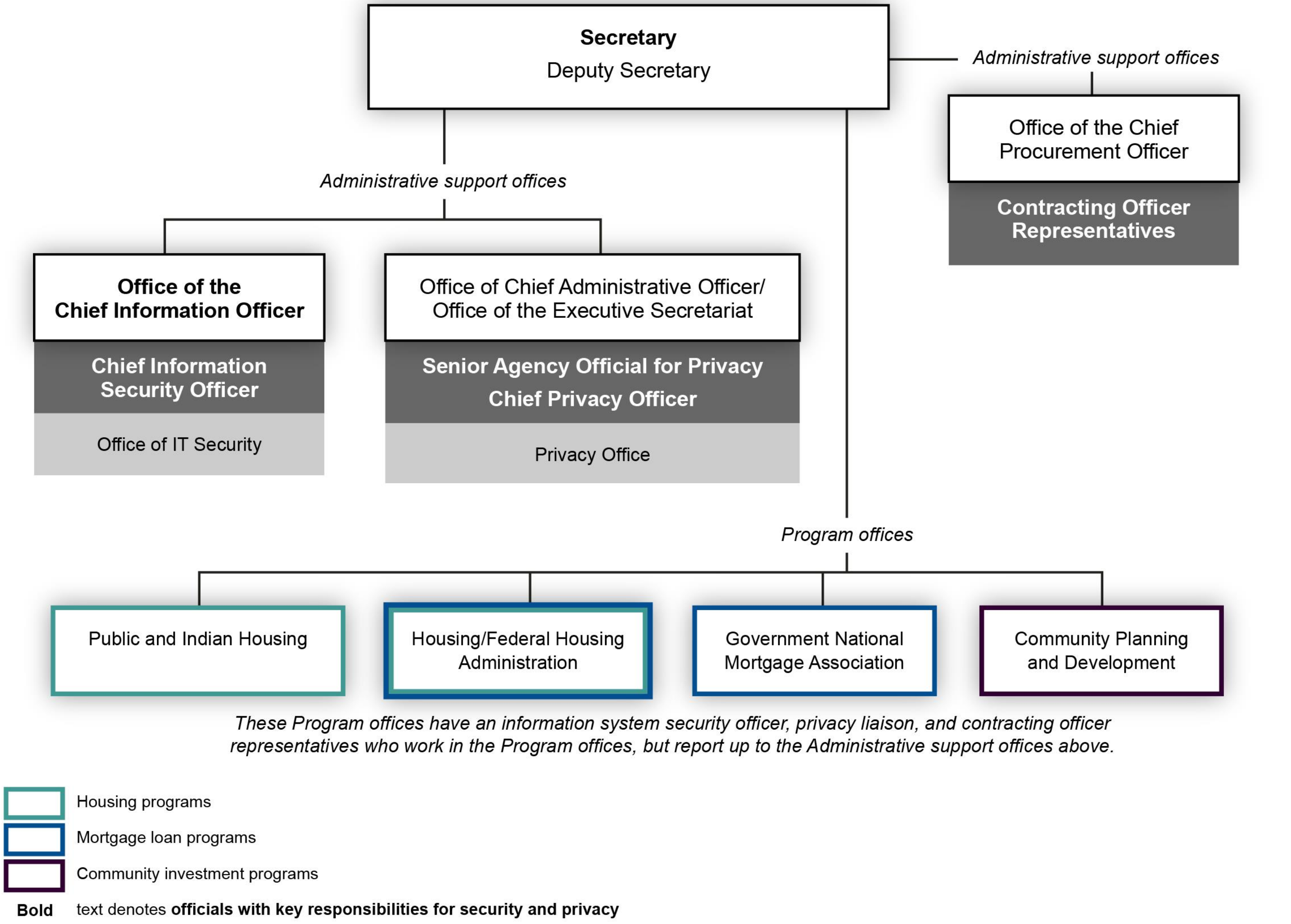
- Ginnie Mae's guidance mirrors the detail and content of HUD's guidance, but adds more than 60 supplemental policies and procedures for contractors managing Ginnie Mae systems and for the third-party contractor that reviews compliance with security and privacy policies.
- The Federal Housing Administration's guidance outlines security and privacy oversight roles and responsibilities for the program office's internal systems and defines time frames for conducting specific practices, including requiring and reviewing independent assessment reports from service providers annually.
- The Office of Public and Indian Housing issued guidance in 2015 for protecting the privacy of sensitive information shared with state and local public housing agencies.[20]

HUD system owners have primary responsibility for establishing system security and privacy controls and overseeing the extent to which they are implemented for the department's internal systems. Regarding information shared with external entities, system owners also work with the Office of the Chief Procurement Officer to establish requirements for systems in contracts, agreements with other federal agencies, and external business partners.

Figure 1 provides a simplified view of HUD's organization chart, identifying key department officials and administrative support and program offices with responsibility for IT security and privacy.

[20] This program office's guidance has not been updated to reflect revisions made to federal guidance since it was issued.

Figure 1: Simplified Department of Housing and Urban Development Organization Chart


Secretary
Deputy Secretary
Administrative support offices
Office of the Chief Procurement Officer
Contracting Officer Representatives
Administrative support offices
Office of the Chief Information Officer
Chief Information Security Officer
Office of IT Security
Office of Chief Administrative Officer/ Office of the Executive Secretariat
Senior Agency Official for Privacy
Chief Privacy Officer
Privacy Office
Program offices
Public and Indian Housing
Housing/Federal Housing Administration
Government National Mortgage Association
Community Planning and Development
These Program offices have an information system security officer, privacy liaison, and contracting officer representatives who work in the Program offices, but report up to the Administrative support offices above.
Housing programs
Mortgage loan programs
Community investment programs
Bold text denotes officials with key responsibilities for security and privacy

Source: GAO analysis of HUD data. | GAO-20-431

HUD's Housing, Community Investment, and Mortgage Loan Programs Share Sensitive Information with External Entities and Rely on Information Systems

HUD's housing, community investment, and mortgage loan program offices engage with thousands of external entities that process, store, and share information to manage their programs. Specifically, HUD engages with other federal agencies; contractors; and other government, for-profit, and nonprofit organizations in operating these programs.

- **Federal agencies** – HUD shares information with other federal agencies, often for the purpose of verifying the eligibility of program participants. This information can include names, addresses, loan amounts, and income. HUD enters into agreements with other federal agencies, including memorandums of understanding, computer matching agreements, and interconnection security agreements that specify requirements for how each agency is to protect data. The Office of the CIO has developed templates for such agreements for use by program offices and system owners.
- **Contractors** – The department works with contractors to manage programs; develop, manage, operate, and enhance information systems; collect information needed for HUD programs; and provide other services. Certain contractors are utilized by owner agents to act as administrators to help manage properties for rental housing programs. Those contactors collect sensitive information and PII from site visits of properties lived in by residents in housing programs and submit the required information to HUD on behalf of multiple property owners. Data collected can include, for example, household income and expenses, ethnicity, and race. The Office of the CIO or program offices work with the Office of the Chief Procurement Officer to establish the terms of contracts, incorporate appropriate requirements for managing and securing information systems, and ensure effective oversight of contractor performance.

In addition, service providers are one specific type of contractor supporting the department's programs and systems.[21] For example, mortgage loan programs involve service providers that collect sensitive and nonsensitive information from lending institutions and process it on the department's behalf. Another type of service provider supporting rental assistance programs involves property management agents that operate rental properties on behalf of property owners. These service providers employ commercial software or other

[21] HUD defines service providers as vendors, contractors, other federal government organizations, and entities that provide IT services, information systems, and facilities housing HUD information systems and makes service providers responsible for ensuring and maintaining security controls that are compliant with HUD security policy.

systems to collect information about properties and report to the department.

- **Other government, for-profit, and nonprofit organizations** – HUD also works with a variety of other government, for-profit, and nonprofit organizations in managing and operating the department's programs. HUD's program offices—not the Office of the CIO or the Privacy Office—typically approve the enrollment of these organizations in HUD programs, establish the requirements to be followed, and provide oversight of their participation and performance. External entities involved in HUD rental assistance housing programs include, among others, state, local, and tribal public housing or housing finance agencies and property owners. Some state and local housing agencies serve, for example, as contract administrators providing oversight for rental assistance programs. To perform oversight, the administrators need access to sensitive information, including financial statements for property owners. External entities for community investment include the grantees that manage programs and provide services through the department's grant programs. Lending institutions and other financial organizations comprise the external entities supporting HUD mortgage loan programs.

The housing, community investment, and mortgage loan program offices rely on information systems to exchange information—including sensitive information—with the external entities.

- To support HUD housing programs, the Office of Housing and the Office of Public and Indian Housing each manage three systems that contain sensitive information and share information with external entities. Specific types of external entities involved in one multifamily housing program include private firms and state and local agencies that administer rental assistance contracts. These external entities use one system to submit sensitive information to the Office of Housing to verify tenant eligibility for the program and to process rental assistance payments. Specific types of sensitive information processed, stored, and shared include tenant name, Social Security number, date of birth, address, and telephone number.

In another example, the Office of Public and Indian Housing uses a different information system to enable reporting by public housing agencies, tribes, tribal entities, and their hired management agents that administer other housing programs. System users submit sensitive information electronically to support the effective distribution of rental assistance to individuals and annual and interim reexaminations of tenants' family income and composition. The system collects sensitive information about tenants, including full name, date of birth, citizenship status, disability status, race, ethnicity, Social Security number, and alien registration number. Specific types of external entities connected to the systems that support this program office's mission include, among others, over 4,000 public housing agencies throughout the United States. These external entities collect and transmit tenant information used to verify rental assistance program eligibility.

- In addition, to manage community investment programs, the Office of Community Planning and Development uses one system that contains PII to support at least seven different programs. For that system, grantees submit certain sensitive information collected from grant program participants, including names of individuals, their racial and income characteristics, and locations of facilities operated with grant funds.[22]
- To support mortgage loan programs, the Federal Housing Administration manages 23 systems and Ginnie Mae manages two systems that contain sensitive information and share information with external entities. For example, with regard to one mortgage loan system, lenders report sensitive information about borrowers, such as case numbers, in order to process payments for premiums associated with loans insured by the Federal Housing Administration. Ginnie Mae operates another system that collects information about borrowers associated with mortgages that back securities with Ginnie Mae guarantees. Sensitive information collected by the system includes borrower name, Social Security number, loan address, and financial information (i.e., loan numbers and credit score).

Leading Practices to Protect Agencies' Sensitive Information

Federal laws and guidance specify requirements for federal agencies to protect systems and data, including systems used or operated by a

[22] According to a branch chief from the Office of Community Planning and Development's Systems Development and Evaluation Division, external entities that collect certain sensitive information to manage grant programs are responsible, under their contracts with HUD, for maintaining and safeguarding the information in their records.

contractor or other organization on behalf of a federal agency. The Privacy Act of 1974 and other statutes establish protections for personal information accessed or held by federal agencies.[23] These laws describe, among other things, agency responsibilities with regard to protecting individually identifiable information.

OMB directs agencies that share PII to use written agreements to require the implementation of security and privacy controls by contractors and other nonfederal entities that collect, use, process, store, maintain, and disseminate federal information on behalf of a federal agency. OMB guidance notes that agencies are ultimately responsible for ensuring that federal information is adequately protected, commensurate with the risk resulting from the unauthorized access, use, disclosure, modification, or destruction of such information. Accordingly, OMB guidance states that, when sharing PII with contractors or other nonfederal entities, agencies should establish requirements for the protection of their data in written agreements with these entities.[24] For specific technical direction, OMB requires agencies to implement standards and guidelines established by NIST.

NIST has developed a series of information security standards and guidelines for agencies to follow in managing information security risks.[25] NIST guidance provides steps that agencies can take to identify appropriate security and privacy controls and establish specific requirements for implementing those controls to ensure consistency, both internally and externally, to the agency. The guidance also outlines standards for protecting the confidentiality of controlled unclassified information (which includes PII) when it resides in a nonfederal system or organization.

As we have previously reported, guidance from OMB and NIST calls for agencies to oversee external entities with which they share PII to ensure that appropriate security and privacy controls are in place. This guidance

[23] Privacy Act of 1974, Pub. L. No. 93-579, §3, 88 Stat. 1896, 1897 (Dec. 31, 1974); codified at 5 U.S.C. §552a; 44 U.S.C. §§ 3571, 3572.

[24] Office of Management and Budget, Circular A-130: *Managing Information as a Strategic Resource,* Appendices I and II (July 2016).

[25] NIST, Special Publication 800-37, Revision 1; Special Publication 800-53, Revision 4; FIPS Publication 199; FIPS Publication 200; Special Publication 800-171, Revision 1; and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1.

identifies four leading practices along with others for overseeing the protection of data by external entities: (1) require the implementation of risk-based security and privacy controls, (2) perform independent assessments to ensure controls are implemented, (3) identify corrective actions needed, and (4) monitor progress implementing controls/corrective actions.[26] In addition, these practices are further defined by various subpractices, as detailed in table 1.

Table 1: Leading Practices and Subpractices for Overseeing the Protection of Sensitive Information by External Entities

Practice	Subpractice
Require risk-based security and privacy controls	• Document requirement for external entities to implement risk-based security controls. • Document rationale for categorizing the system and determining risk impact rating, including assessing risks associated with sharing sensitive information with external entities. • Document requirement for external entities to establish a plan or mechanisms for ensuring the privacy of agency information. • Establish processes or mechanisms to ensure that external entities comply with security and privacy requirements.
Independently assess implementation of controls	• Document requirement for third-party assessments of implemented security and privacy controls at a defined frequency. • Establish process for overseeing and tracking compliance of external entities with third-party assessments. • Establish process for obtaining access to assessments for external entities or reports, attestations, or other evidence that assessments were conducted. • Obtain evidence that third-party assessor for external entity controls was independent.
Identify and track corrective actions needed	• Document requirement for external entities to plan and manage corrective actions for weaknesses identified.
Monitor progress implementing controls	• Document requirement for external entities to monitor progress implementing technical, management, and operational security controls at a defined frequency.

[26] GAO-18-518; OMB, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016); and NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); Federal Information Processing Standards (FIPS) Publication: *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004); FIPS Publication: *Minimum Security Requirements for Federal Information and Information Systems,* FIPS Publication 200 (Gaithersburg, Md.: March 2006); *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 1 (Gaithersburg, Md.: December 2016); and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: April 2018).

Source: GAO analysis of relevant federal laws and guidance. | GAO-20-431

Previous Reports Have Highlighted the Importance of Cybersecurity and the Need for HUD to Improve Policies for Protecting Data

We first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of PII in 2015. Ensuring the cybersecurity of the nation remains a government-wide high-risk area, and we have identified protecting privacy and sensitive data among the nation's major cybersecurity challenges.[27]

In addition, we and the HUD Office of Inspector General have reported on weaknesses in HUD's practices for protecting the security and privacy of sensitive data.

[27] GAO, *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 16, 2019).

- In August 2018, we reported that HUD and other federal agencies had not fully addressed key responsibilities for effectively managing IT in accordance with federal law and guidance.[28] Specifically, HUD had not fully addressed the CIO's responsibility for establishing, implementing, and ensuring compliance with an agency-wide information security program. HUD neither agreed nor disagreed with our recommendation that the department address the CIO's role in its policies. According to the HUD CIO and Chief Information Security Officer, the department plans to update its IT security policies and procedures to address this recommendation. As of March 2020, the recommendation had not yet been implemented.
- In a July 2019 report on federal cybersecurity risk management, we reported that HUD had recently implemented an enterprise dashboard to aggregate system-level data and score the department's maturity in process areas based on the NIST cybersecurity framework, including scores for program offices and the department as a whole.[29] However, we also noted that HUD's documents and policies did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies. We recommended that the department develop a cybersecurity risk management strategy that includes key elements, and update the department's policies to require the use of risk assessments to inform the prioritization of plans of action and milestones for corrective actions. HUD concurred with the recommendations. In May 2020, HUD's CIO reported that the office had initiated efforts designed to address the recommendations. In addition to establishing a new advisory committee for IT risk management, the Office of the CIO stated that it plans to implement new guidelines designed to support the improved identification and protection of high-risk systems and data. HUD has also stated that it intends to finalize a risk management strategy by 2022.
- In September 2014, HUD's Office of Inspector General reported that a former public housing authority employee had improperly

[28] GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C., Aug. 2, 2018).

[29] GAO, *Cybersecurity*: *Agencies Need to Fully Establish Risk Management Programs and Address Challenges,* GAO-19-384 (Washington, D.C.: July 25, 2019).

released PII outside the department.[30] The employee had sent at least seven emails containing housing choice voucher holders' PII, including Social Security numbers and other personal information such as household income, to the employee's personal email address and the work email address of a friend who worked for one of the department's contractors. The office found that the former employee had obtained the PII from a state system.

- HUD's Office of Inspector General reported on the department's privacy policies in September 2018 and in June 2020.[31] Specifically, the office reported in 2018 that HUD had updated the department's privacy impact assessment processes, improved its incident response and reporting capabilities, and upgraded its privacy awareness training. However, HUD had not established a strategic plan for privacy or integrated privacy risks into the enterprise risk management process, and lacked a structured compliance program. Critically, HUD continued to lack the capability to fully identify and inventory the department's extensive holdings of PII. The Office of Inspector General made 24 recommendations for improving HUD's privacy program based on the findings from the 2018 privacy program evaluation and also recommended that HUD address 14 prior recommendations from a 2014 privacy program evaluation.[32] In June 2020, the office issued a new report on PII records protection and management. In that report, the office explained that HUD had begun addressing the 38 recommendations from the 2014 and 2018 reports but noted that five critical privacy-related recommendations from the reports had not yet been addressed. The office also issued nine additional privacy-related recommendations, including recommending that HUD designate a senior agency official for records management and issue a formal policy and requirements for managing controlled unclassified information.

[30] Department of Housing and Urban Development, Office of Inspector General, *A Former Employee of the Helena Housing Authority, Helena, MT, Improperly Released Personally Identifiable Information*, 2014-DE-1002 (Denver, Colo.: September 2014).

[31] Department of Housing and Urban Development, Office of Inspector General, *HUD Privacy Program*, 2018-OE-0001 (Washington, D.C.: Sept. 2018) and *HUD PII Records Protection and Management*, 2019-OE-0002a (Washington, D.C.: June 2020).

[32] Department of Housing and Urban Development, Office of Inspector General, *HUD Privacy Program Evaluation Report*, 2014-ITED-0001 (Washington, D.C.: April 2014).

- In March 2019, HUD's Office of Inspector General summarized the results of the department's 2018 FISMA review and noted that HUD had made improvements. However, the office also determined that key significant weaknesses in each of eight IT cybersecurity domains from 2017 remained and that HUD remained at the same level of maturity and effectiveness as in the prior fiscal year.[33] The Office of Inspector General made 30 recommendations for fiscal year 2018 and associated each with a FISMA metric to allow the department to better prioritize and work on continually maturing each component of the information security program. As of August 2020, HUD had implemented actions to address eight recommendations and had planned steps to address five additional recommendations. The department had not yet taken action to address the other 17 recommendations.

HUD's Security and Privacy Policies and Procedures Were Not Adequate for Overseeing the Protection of Sensitive Information Exchanged with External Entities

As previously discussed, federal guidance identifies four leading practices—and 10 related subpractices—that federal agencies should implement to protect sensitive information shared with external entities.[34] Specifically, agencies should (1) require the implementation of risk-based security and privacy controls, (2) perform independent assessments to ensure controls are implemented, (3) identify corrective actions needed, and (4) monitor progress in implementing controls/corrective actions.

Of the four leading practices, HUD did not address one and minimally addressed the other three practices in its security and privacy policies and procedures. In assessing the 10 subpractices that underpin those four practices, HUD minimally addressed six subpractices and did not

[33] Department of Housing and Urban Development, Office of Inspector General, *Semiannual Report to Congress for the period ending March 31, 2019*, 2018-OE-0003 (Washington, D.C.: March 2019).

[34] Office of Management and Budget, *Circular A-130: Managing Information as a Strategic Resource*, Appendices I and II (July 2016); NIST, Special Publication 800-37, Revision 1; Special Publication 800-53, Revision 4; FIPS Publication 199; FIPS Publication 200; Special Publication 800-171, Revision 1; and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1.

address three subpractices. The department substantially addressed only one of the 10 subpractices. As such, it lacked effective policies and procedures to ensure adequate protection of sensitive information exchanged with external entities (i.e., federal agencies and contractors, and other government, for-profit, and nonprofit organizations).

Among other things, the department lacked policies and procedures to verify that external entities have implemented the security controls necessary to protect sensitive HUD information (second practice). In addition, the department's policies and procedures related to external entities' implementation of risk-based security and privacy controls only minimally addressed the first leading practice. For example, while HUD required the federal entities with which it exchanges information to implement risk-based security controls, it did not have this same requirement for nonfederal entities (including state and local government, for-profit, and nonprofit organizations). Further, the department did not require external entities to have plans for protecting the privacy of sensitive HUD information. Table 2 depicts the extent to which the department's policies and procedures addressed the leading practices for overseeing the protection of sensitive information.

Table 2: Extent to Which the Department of Housing and Urban Development (HUD) Policies and Procedures Address Leading Practices for Overseeing the Protection of Sensitive Information

Practice	Rating
Require risk-based security and privacy controls	minimally addressed
Independently assess implementation of controls	not addressed
Identify and track corrective actions needed	minimally addressed
Monitor progress implementing controls	minimally addressed

Legend: ◔=Minimally addressed—leading practice was addressed to a limited extent; ○=Not addressed—leading practice was not addressed.

Source: GAO analysis of HUD data. | GAO-20-431

HUD Minimally Addressed the Leading Practice of Requiring External Entities to Implement Risk-Based Security and Privacy Controls

HUD minimally addressed the first leading practice for protecting sensitive information that is shared with external entities. This practice focuses on requiring external entities to implement risk-based security and privacy controls. In particular, for the four subpractices associated with this area, HUD substantially addressed one subpractice and minimally addressed three (for an average overall rating of “minimally addressed”).

- **Document requirement for external entities to implement risk-based security controls.** HUD substantially addressed this subpractice. Specifically, it required federal agencies with which it exchanges information to implement risk-based security controls. More specifically, HUD’s Office of the CIO provided templates for memorandums of agreement with other agencies and for documenting interconnection security agreements. The templates included fields for the agencies to document and describe data sensitivity, security policies, and expectations for trusted behavior. For example, one template called for the agreements to specify the sensitivity or classification level of the information to be exchanged.

HUD also incorporated guidance in its own contracts requiring contractors to comply with “applicable federal and HUD statutes, regulations, policies, and procedures governing the security of the system(s).” Further, the Office of the CIO’s IT policies stated that all security policies are to apply to external information systems operated on behalf of the department by contractors, vendors, and agents of HUD.

However, the department had not clearly defined the extent to which its contractual agreements with nonfederal entities (including state and local government, for-profit, and nonprofit organizations) are to address the leading practices for protecting sensitive information they process, store, or share with HUD systems. Specifically, the department's IT policies did not include requirements for entities outside the federal government to implement HUD requirements, including to what extent the external entity organizations were to establish risk-based IT security and privacy controls at the organizational level. In addition, HUD's acquisition policies did not address IT security aside from outlining requirements for personnel security and the return or destruction of its data after contracts were complete.

- **Document rationale for categorizing the system and determining risk impact rating, including assessing risks associated with sharing sensitive information with external entities.** HUD minimally addressed this subpractice. Specifically, its policy required that all systems and information under the department's control (including systems that contractors operated for HUD) were to be categorized in accordance with federal standards and called for annual review and validation of their categorization decisions and supporting rationale.

However, HUD's policy did not specifically require program offices or system owners that are establishing contracts to include provisions requiring their contractors to provide the department with the rationale for categorizing system risk or evidence that they had assessed or documented risks associated with sharing its information. In addition, the department's template for interconnection security agreements[35] with federal agencies provided a section for categorizing data sensitivity or specifying the classification level for categorizing risk associated with the information HUD and other federal agencies exchange. However, the template did not provide guidance on documenting the rationale for categorizing the HUD or federal agency systems or assessing the risk associated with the information

[35] HUD defines this agreement as a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. This agreement supports the memorandum of understanding or agreement governing information sharing between the organizations.

exchanged by the agencies. Further, HUD's IT policies did not require agreements with other state and local government, for-profit, and nonprofit organizations to require those external entities to document their rationale for categorizing their systems and determine their risk impact rating.

- **Document requirement for external entities to establish a plan or mechanisms for ensuring the privacy of agency information.** HUD minimally addressed this subpractice. HUD's policy called for the Chief Privacy Officer to establish mechanisms for ensuring privacy, such as developing privacy roles, responsibilities, and access requirements for contractors. However, the department's contracts did not require contractors to establish plans or mechanisms for ensuring the privacy of its information. Further, HUD's Office of the CIO developed templates for memorandums of agreement with other external entities, such as federal agencies, that required the agencies to identify within the agreement the highest sensitivity of the information (e.g., Privacy Act, Trade Secrets Act, or if the information had been classified as confidential, secret, or top secret). However, the templates did not require the other federal agencies to do more than state the sensitivity level for the information. The templates did not require the other federal agencies to describe plans or mechanisms for ensuring the privacy of HUD information. In addition, the department's IT policies did not state that HUD's agreements with other government, for-profit, and nonprofit organizations are to require those external entities to develop privacy plans or mechanisms for ensuring the privacy of information for HUD programs.
- **Establish processes or mechanisms to ensure that external entities comply with security and privacy requirements.** HUD minimally addressed this subpractice. The department required its staff or other individuals authorized who use HUD systems to be trained on security and privacy requirements. The department also established processes for overseeing compliance with training and other requirements for accessing and using its systems. In addition, HUD policy stated that contractors are required to provide copies of their internal IT security plans to the Chief Information Security Officer for review upon request.[36]

[36] We did not review the extent to which the Chief Information Security Officer requested that contractors provide plans for review.

HUD's policy also required its Office of the CIO and procurement staff to perform annual reviews of contractors. However, the department did not establish a process or mechanism to ensure all external entities complied with security and privacy requirements when processing, storing, or sharing information for the department's programs outside of its systems. Specifically, HUD's policies that called for annual reviews of contractors lacked detail about how this was to occur. Further, HUD IT policies did not prescribe security requirements to be implemented by other government, for-profit, and nonprofit organizations processing, storing, or sharing information for HUD programs.

Regarding privacy, HUD's policy stated that the Chief Privacy Officer was to establish, among other things, privacy roles, responsibilities, and access requirements for contractors. However, the department did not establish an oversight process to ensure that contractors, federal agencies, or other government, for-profit, and nonprofit organizations implemented privacy requirements.

HUD Did Not Address the Leading Practice of Ensuring Independent Assessments of External Entity Controls

HUD did not address the second leading practice of protecting sensitive information shared with external entities. This practice focuses on ensuring independent assessments of external entity controls. Specifically, HUD minimally addressed the first subpractice and did not address the other three practices (for an average overall rating of "not addressed").

- **Document requirement for external entities to have third-party assessments of implemented security and privacy controls at a defined frequency.** HUD minimally addressed this subpractice. Specifically, its policies called for system owners to obtain independent assessments for the department's internal moderate- and high-impact systems. In addition, HUD required certain contractors who manage systems on its behalf to conduct independent assessments. However, the department's policies and procedures did not address requirements for independent assessments by other contractors, and HUD did not require such assessments for federal agencies or other government, for-profit, and nonprofit organizations at a defined frequency.
- **Establish process for the agency to oversee and track compliance of external entities with third-party assessments.**

HUD did not address this subpractice. Specifically, HUD did not establish a process for the agency to oversee or track whether contractors—other than those responsible for managing HUD's internal systems—and other external entities complied with requirements for third-party assessments. In providing guidance to agencies, NIST calls for agencies to assign primary responsibility for tasks to ensure that they are completed.[37] However, HUD's policy did not clearly assign responsibility for oversight of assessments. Instead, its guidance discussed the responsibility for assessments as being among the responsibilities of multiple, disparate parties, including program offices, information system security officers, the procurement office, contracting officers, and contracting officers' representatives, leaving primary responsibility unclear. In addition, because HUD did not require evidence of third-party assessments for federal agencies and other government, for-profit, and nonprofit organizations, the department did not establish practices for overseeing assessments for those external entities.

- **Establish process for obtaining access to assessments for external entities or reports, attestations, or other evidence that assessments were conducted.** HUD did not address this subpractice. The department's policy did not establish practices for IT staff to obtain access to assessments for its contractors or attestations (or other evidence) that independent assessments of security controls had been completed. The department also lacked practices for HUD or its program offices to obtain access to assessments for other federal agencies or other state and local government, for-profit, and nonprofit organizations.
- **Obtain evidence that third-party assessors of external entity controls were independent.** HUD did not address this subpractice. The department did not define criteria or other guidance that external entities could use to ensure that assessors were independent.

[37] NIST Special Publication 800-37 states that the roles with primary responsibility may complete a task or may delegate completion of a task to one or more supporting roles except where delegation is specifically prohibited.

HUD Minimally Addressed the Leading Practice of Identifying and Tracking External Entity Corrective Actions Needed

HUD minimally addressed the third leading practice for protecting sensitive information shared with external entities (which is comprised of one subpractice).

- **Document requirement for external entities to plan and manage corrective actions for weaknesses identified.** HUD minimally addressed this subpractice. Its standard language for contracts called for contractors to comply with federal requirements such as those developed pursuant to FISMA and OMB Circular A-130; however, the contract language did not address planning or managing corrective actions for weaknesses identified. Similarly, the department's templates for agreements with federal agencies did not include a requirement for federal agencies to plan and manage corrective actions for weaknesses identified for HUD programs. Moreover, the department did not address whether other government, for-profit, or nonprofit organizations were to plan and manage corrective actions.

HUD Minimally Addressed the Leading Practice of Monitoring External Entity Progress in Implementing Controls

HUD minimally addressed the fourth leading practice for protecting sensitive information shared with external entities (which is comprised of one subpractice).

- **Document a requirement for external entities to monitor progress in implementing technical, management, and operational security controls at a defined frequency.** HUD minimally addressed this subpractice. Specifically, the department's policy documented a requirement for monitoring contractors' progress in implementing controls and assigned responsibility for monitoring progress to the department's procurement staff. However, HUD's policy did not define how this is to occur, including whether results are to be made available to department IT staff responsible for overseeing security and privacy. In addition, its templates for agreements with federal agencies documented a requirement for the agreements to be reviewed annually to ensure that security controls were operating properly but did not provide additional direction for oversight over the agreements. Further, the department did not document a requirement for other government, for-profit, and nonprofit organizations to monitor progress implementing security at a defined frequency.

HUD's Failure to Prioritize Updating Policies and to Establish Stable Leadership Contributed to Weaknesses in Protecting Sensitive Information

HUD's weaknesses in implementing the four leading practices for protecting sensitive information shared with external entities were due largely to a lack of priority given to updating its policies and a lack of stable leadership. For example:

- The department has not updated its privacy handbook since 1995 and has not updated one of its key security policies since 2014.
- Since 1998, HUD has experienced extremely high CIO turnover and has continued to experience frequent turnover and vacancies in additional critical IT security and privacy roles.[38] Notably, HUD operated without a Chief Privacy Officer from 2016 until September 2019. HUD has experienced turnover in key privacy positions. Specifically, since December 2018, three different HUD officials have served as acting secretary in the Office of the Executive Secretariat—the office within the Office of Administration charged with overseeing privacy. In addition to the Privacy Office's staff, privacy liaison officers within each HUD program office coordinate with system owners to establish and update privacy assessments and to obtain responses to questions about privacy matters.
- HUD has transferred the responsibility for the department's IT privacy program to different parts of the organization on multiple occasions. In 2014, the Office of the CIO managed the department's privacy program. In 2015, both the Office of the CIO and the Office of Administration had offices responsible for

[38] The current CIO took office in August 2018. The average tenure of the 14 appointed and acting CIOs since 1998 is about 1.6 years; appointed CIOs have averaged about 2.9 years in the position. Since December 2018, three different individuals have held the key position of Chief Information Security Officer and two individuals have acted in the Executive Secretariat position overseeing privacy functions.

privacy. The Office of Administration took over the privacy program in 2015. In March 2020, the Office of IT Security and the Privacy Office announced plans to coordinate more closely to improve cybersecurity and privacy for the department. Specifically, the Senior Agency Official for Privacy announced a requirement for program offices to update privacy impact assessments for information systems and respond to a survey about the systems' sensitive data.

HUD's CIO and Chief Information Security Officer acknowledged that HUD has room to improve how it (1) identifies and defines requirements for external entities to be included in contractual agreements, (2) ensures that the requirements are to protect the security and privacy of information, and (3) provides oversight to these external entities. They also reported actions the office has planned to improve IT security practices.

As of May 2020, the Office of the CIO had initiated efforts to review its IT security practices and revise, streamline, and enhance the policies and procedures. For example, the office had drafted an updated IT security policy and a revised set of security control procedures. The CIO had begun planning and implementing changes designed to fulfill his office's responsibility for remediating weaknesses in HUD's IT security program. However, the CIO asserted that the ultimate success of those efforts would be contingent upon the efforts and collaboration of all HUD offices—administrative support offices and program offices—as well as system owners in working to secure the department's systems and protect the sensitive information shared with external entities.

According to HUD's Senior Agency Official for Privacy, the department's privacy protection practices have been ad hoc and not mature. The official added that the Privacy Office relies heavily on the Office of the CIO's oversight of the privacy-related security controls for systems and has relied more heavily on recent OMB guidance since its privacy handbook is out of date. The official also stated that the lack of input and oversight from a chief privacy officer limited the department's progress in developing a strategic plan for privacy and revising privacy guidance.

To begin addressing these weaknesses, the Privacy Office published a new privacy program plan in March 2020 describing the roles of key privacy officials and outlining strategic goals and objectives for improving privacy protection for the department. The plan assigns the Senior Agency Official for Privacy with responsibility for, among other things, communicating HUD's privacy vision, principles, and policies internally and externally.

Nevertheless, until HUD implements leading practices for protecting sensitive information exchanged with external entities, it cannot be assured that it is appropriately addressing risks to the department's programs and program participants. Further, unless HUD expands beyond internal security and privacy controls to plan for controls required for the protection of data by external entities, the department may be limited in its ability to manage and improve its security posture. Extending security and privacy practices to ensure departmental oversight over whether those entities obtain independent assessments of controls, identify and track corrective actions needed, and monitor progress in implementing controls could aid the department in working with external entities to strengthen the protection of information for HUD programs.

HUD Was Not Fully Able to Identify External Entities That Process, Store, and Share Sensitive Information with Its Systems for Housing, Community Investment, and Mortgage Loan Programs

Federal guidance promulgated by OMB and NIST calls for agencies to maintain an inventory of the agency's information systems and to provide oversight of systems' sensitive information. Such guidance also outlines standards for protecting the confidentiality of controlled unclassified information (which includes PII) when it resides in a nonfederal system or organization (e.g., when information is processed, stored, or shared with external entities).[39] Maintaining comprehensive data about systems that process, store, and share sensitive information and external entities with access to sensitive information can support an agency in making informed decisions about the risks to and protection needed for sensitive information shared outside the organization, and ensure that records

[39] GAO-18-518; OMB, *Circular A-130: Managing Information as a Strategic Resource,* Appendices I and II (July 2016); NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171 (Gaithersburg, Md.: December 2016); and NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

containing sensitive information are accurate, relevant, timely, and complete.

NIST guidance also outlines requirements for protecting the confidentiality of controlled unclassified information (which includes PII) when it resides in a nonfederal system or organization. Identifying the external entities that process, store, or share sensitive federal information is one way agencies can take action to help ensure the protection of the data accessed by those entities. Regarding privacy, HUD's IT security policy handbook assigns the Chief Privacy Officer responsibility for an inventory of all programs and information systems using PII.

HUD was not fully able to identify the external entities that process, store, or share sensitive information with its systems used to support the housing, community investment, or mortgage loan programs. Specifically, the data that HUD provided about systems supporting the three program areas was incomplete and did not provide reliable information about the external entities with access to sensitive information from these systems. For example, we identified additional external entities in system documentation beyond what HUD reported for 23 of the 32 systems. Also, we were able to confirm the entities that HUD reported for only seven of 32 systems identified in its data.

For 23 of the 32 systems, the information on external entities that HUD reported differed from what we found in privacy assessments and other documents. For example, for one Federal Housing Administration mortgage program system, HUD reported the Department of the Treasury was the only external entity that interfaced with the system. By reviewing other documents, however, we determined that the system's external entities also included recorders' offices responsible for recording legal documents or responding to child support income offsets, as well as contractors, grantees, other experts, and consultants. Further, HUD lacked current privacy assessments or other documentation of external entities for two of the systems, so we could not verify the external entities for those systems.

Table 3 shows the differences in what HUD reported regarding the external entities that share information with its systems and what we identified in the department's system documentation.

Table 3: Assessment of the Department of Housing and Urban Development (HUD)-Reported Data Regarding External Entities That Share Information with HUD Systems That Store Sensitive Information

Program area	Total number of HUD-reported systems with sensitive information that share data with external entities	Number of HUD-reported systems with external entities confirmed	Number of HUD-reported systems with incorrect external entities[a]
Housing: Office of Housing	**3**	1	2
Housing: Office of Public and Indian Housing	**3**	1	2
Community investment	**1**	N/A[b]	1
Mortgage loans: Federal Housing Administration	**23**	5	16 (2 missing information)
Mortgage loans: Ginnie Mae	**2**	0	2
Total	**32**	**7**	**23** **(2 missing information)**

Source: GAO analysis of HUD data. | GAO-20-431

[a] We identified additional external entities for the systems or fewer than what HUD had reported.

[b] HUD did not report information about external entities with access to personally identifiable information (PII) for this system that stores sensitive information because the department had not identified this system as containing PII and exchanging it with external entities prior to our review.

HUD was further limited in its ability to protect sensitive information because it did not track the types of sensitive information shared with external entities that required protection. Specifically, neither the Office of the CIO nor the Privacy Office tracked whether information systems contain specific types of PII (e.g., disability status) or sensitive information other than PII (e.g., financial information or proprietary information).

HUD was unable to identify the external entities that process, store, or share sensitive information with its systems, in part, because it does not have a comprehensive inventory of its systems, to include information on external entities. This is due, in part, to HUD's guidance lacking specificity about how program offices and system owners were to ensure that all types of external entities protected information they collected, processed, or shared with HUD programs.

Further, HUD IT officials were not required to collect comprehensive information about whether all external entities were implementing the leading practices for protecting sensitive information shared with external entities described in this report. HUD's CIO stated that his office is responsible for the quality of the data entered in CSAM and expects to work with program offices and system owners to evaluate and improve the reliability of the data.

Until HUD develops comprehensive data that incorporates sufficient, reliable information about the external entities with which program information is shared and the extent to which each has access to PII and other sensitive information, the department will be limited in its ability to ensure information about its housing, community investment, and mortgage loan programs is being effectively safeguarded. Moreover, the department's ability to effectively manage the risks associated with sharing sensitive information and PII with external entities will be impaired.

Conclusions

HUD had minimally addressed the leading practices for requiring the implementation of risk-based security and privacy controls, identifying and tracking corrective actions, and monitoring progress in implementing controls when sharing information with external entities. Moreover, the department had not taken steps to make sure that independent assessments are performed to ensure controls are implemented by external entities. Among the reasons for these weaknesses was HUD's failure to make it a priority to update and improve IT security and privacy policies. Without leading practices for protecting sensitive information shared with external entities in place, HUD lacks assurance that sensitive information shared with external entities is being protected.

Further, HUD had a limited ability to identify external entities that process, store, or share sensitive information with its systems. Until the department has access to better quality information and takes action to improve its inventory of systems that share sensitive information with external entities, HUD will face greater risk that it is falling short in working to protect privacy and sensitive data.

Recommendations for Executive Action

We are making the following five recommendations to HUD.

- The Secretary of Housing and Urban Development should direct the Chief Information Officer, Senior Agency Official for Privacy, and Chief Privacy Officer to review and revise department-level security and privacy policies to ensure that they require the implementation of risk-based security and privacy controls for external entities that process, store, or share sensitive information with HUD. (Recommendation 1)

- The Secretary of Housing and Urban Development should direct the Chief Information Officer, Senior Agency Official for Privacy, and Chief Privacy Officer to review and revise department-level security and privacy policies to ensure that they require independent assessments of external entities that process, store, or share sensitive information with HUD to ensure controls are implemented. (Recommendation 2)
- The Secretary of Housing and Urban Development should direct the Chief Information Officer, Senior Agency Official for Privacy, and Chief Privacy Officer to review and revise department-level security and privacy policies to ensure that they require identifying and tracking corrective action needed by external entities that process, store, or share sensitive information with HUD. (Recommendation 3)
- The Secretary of Housing and Urban Development should direct the Chief Information Officer, Senior Agency Official for Privacy, and Chief Privacy Officer to review and revise department-level security and privacy policies to ensure that they require monitoring of progress in implementing controls/corrective actions by external entities that process, store, or share sensitive information with HUD. (Recommendation 4)
- The Secretary of Housing and Urban Development should direct the Chief Information Officer, Senior Agency Official for Privacy, and Chief Privacy Officer to develop and maintain a comprehensive systems inventory that incorporates sufficient, reliable information about the external entities with which HUD program information is shared and the extent to which each external entity has access to PII and other sensitive information. (Recommendation 5)

Agency Comments

HUD provided written comments on a draft of this report, which are reproduced in appendix II. In is comments, HUD did state whether it agreed or disagreed with our recommendations; however, the department noted actions that it has begun taking to address the recommendations.

For example, HUD stated that the Office of the CIO has developed revised contract requirements designed to improve the protection of the department’s data and intends to incorporate them in new agreements. In addition, HUD said it developed a draft cybersecurity supply chain risk management strategy to identify, assess, and monitor risks associated with external entities. According to the department, the strategy is designed to include, among other things, an evaluation of security and privacy controls and the identification of external entities that present higher risk based on the type of services or products supplied and the data transmitted.

Further, HUD stated that it had developed new updates for the privacy handbook and IT security policy handbook; however, the department had not obtained approval to finalize and implement the updated policies. HUD also provided updated information about the status of the department’s efforts to address 30 recommendations made by HUD’s Office of Inspector General in its 2018 FISMA review. According to the department, HUD has—as of August 2020—closed eight recommendations, planned steps to address five additional recommendations, and is actively working on the other 17. We updated the report to reflect this new information.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Department of Housing and Urban Development, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions about information discussed in this report, please contact me at (202) 512-4456 or HarrisCC@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 key contributions to this report are listed in appendix III.

CCHarris

Carol C. Harris
Director, Information Technology Management Issues

Appendix I: Objectives, Scope, and Methodology

House Report 115-237 as incorporated by the Consolidated Appropriations Act, 2018 included a provision for GAO to evaluate the Department of Housing and Urban Development's (HUD) information security framework for protecting information related to housing, community investment, and mortgage loans.[1] The specific objectives for this review were to (1) assess the effectiveness of HUD's policies and procedures for overseeing the security and privacy of sensitive information exchanged with external entities; and (2) determine the extent to which HUD was able to identify external entities that process, store, and share sensitive information with its systems used to help administer the housing, community investment, and mortgage loan programs.

To address the first objective, we reviewed Federal Information Security Modernization Act of 2014 requirements;[2] Office of Management and Budget (OMB) guidance on managing federal information;[3] National Institute of Standards and Technology information security standards and

[1] House Appropriations Committee report, H.R. Rep. No. 115-237, at 100 (2017), as approved by the joint explanatory statement of the conference, 164 Cong. Rec. H2697, H2872 (daily ed. Mar. 22, 2018) (statement of Chairman Frelinghuysen), specifically referenced in section 4 of the Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, § 4, 132 Stat. 348, 350 (Mar. 23, 2018).

[2] The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[3] Office of Management and Budget, Circular A-130: *Managing Information as a Strategic Resource*, Appendices I and II (July 2016).

guidance;[4] and work we have done previously[5] that identified four leading practices relevant to protecting sensitive information shared with external entities. The leading practices are: (1) require the implementation of risk-based security and privacy controls, (2) independently assess the implementation of security controls, (3) develop and implement corrective actions for weaknesses identified, and (4) monitor the implementation of controls on an ongoing basis.

For this review, we examined the guidance and associated at least one subpractice with each leading practice. For example, documenting a requirement for external entities to implement risk-based security controls is a subpractice of leading practice (1)—require the implementation of risk-based security and privacy controls. Across all four of the leading practices, we identified a total of 10 subpractices for our analysis.

We then collected and reviewed the policies and procedures that HUD had in place for protecting the sensitive information for the housing, community investment, and mortgage loan programs that it shared with three different groups of external entities. These external entity groups were: (1) federal agencies with which HUD established agreements to share program information; (2) contractors, such as corporations that assist HUD in administering programs or developing or managing information systems; and (3) other government, for-profit, and nonprofit organizations, such as state and local public housing agencies, lending institutions, and grantees involved with HUD's housing, community investment, and mortgage loan programs.

We compared the policies and procedures that HUD had in place for the three groups of external entities to each of the identified subpractices.

[4] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); Federal Information Processing Standards (FIPS) Publication: *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004); *Minimum Security Requirements for Federal Information and Information Systems,* FIPS Publication 200 (Gaithersburg, Md.: March 2006); *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 1 (Gaithersburg, Md.: December 2016); and *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: April 2018).

[5] GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*, GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

This comparison enabled us to determine whether the policies and procedures addressed or did not address each subpractice. We assigned a rating to HUD's policies and procedures based on the extent to which they addressed, for each entity, what the subpractice called for using a four-point scale:

- fully addressed indicated that HUD's policies and procedures addressed the subpractice;
- substantially addressed indicated that HUD's policies and procedures addressed the subpractice to a great extent;
- minimally addressed indicated that HUD's policies and procedures addressed the subpractice to a limited extent; and
- not addressed indicated that HUD's policies and procedures did not address the subpractice.

Finally, to determine the overall rating for each leading practice, we averaged their subpractice ratings. For example, for the first leading practice, we had assigned a rating of substantially addressed to the first subpractice (two points) and ratings of minimally addressed to the other three subpractices (one point each). The average point value for the four subpractices came out to roughly one point, which equated to a "minimally addressed" rating for the overall practice. The average point value for the four subpractices came out to roughly one point, which equated to a "minimally addressed" rating for the overall practice.

To further supplement our analyses of the department's policies and procedures, we collected and evaluated detailed system plans and documentation (e.g., system security plans) for a nongeneralizable subset of the department's information systems. To identify this subset, we used systems HUD had reported as containing sensitive information, sharing information with external entities, and representing the housing and mortgage loan programs. This list contained 32 systems. Then we randomly selected four systems from this list. Although HUD did not originally report any community investment systems as containing sensitive information and sharing information with external entities, we subsequently identified one community investment system as containing sensitive information and sharing information with external entities. We added that system to our subset of systems for review. We also interviewed HUD officials responsible for the security and privacy of the department's systems.

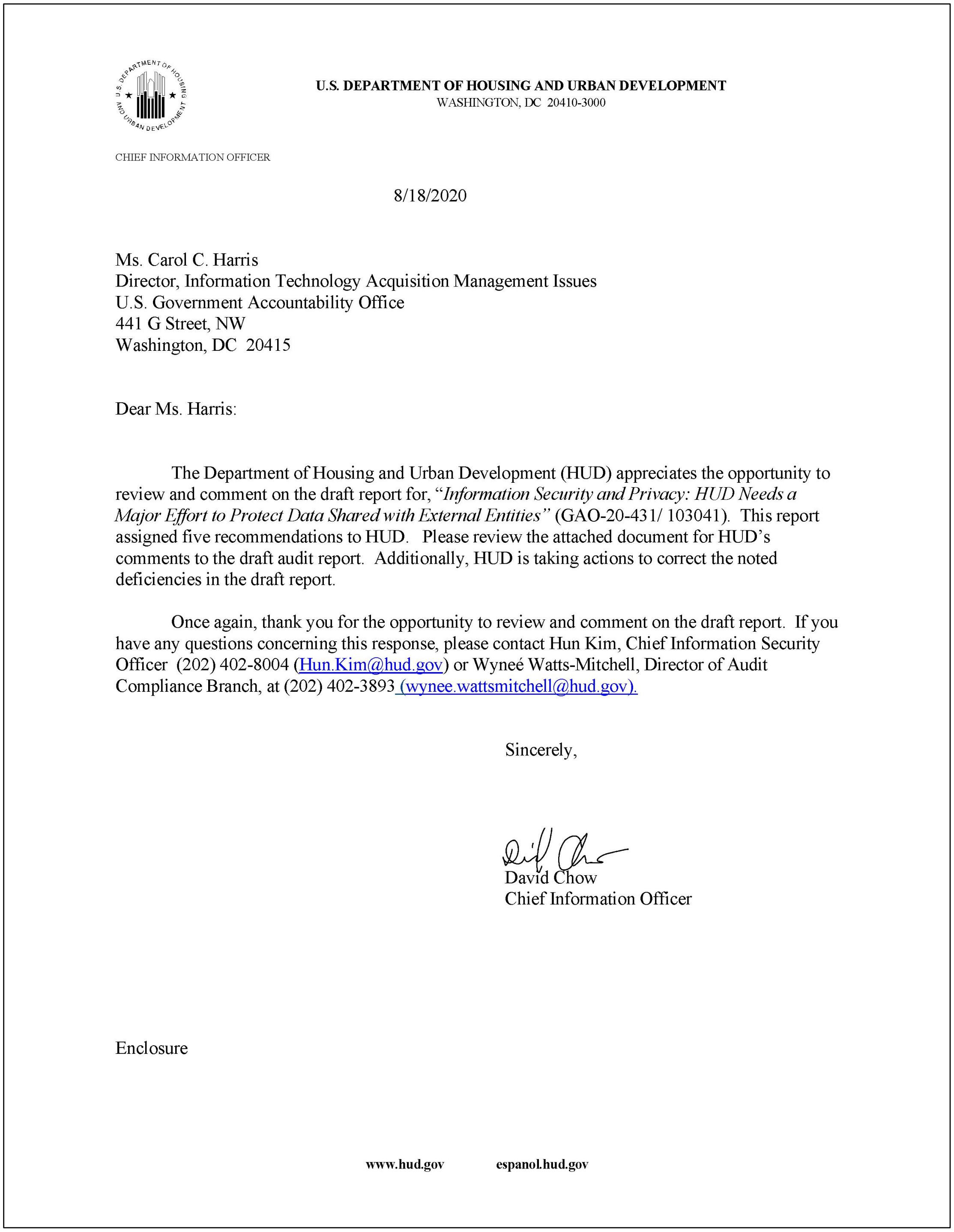
We used information about the selected systems as illustrative examples of how HUD's policies and procedures did or did not address subpractices. Results from nongeneralizable samples cannot be used to make inferences about a population. The systems that we reviewed included two housing systems—the Federal Housing Administration's Tenant Rental Assistance Certification System and the Office of Public and Indian Housing's Inventory Management System/Public and Indian Housing Information Center system; one community investment program system—the Office of Community Planning and Development's Integrated Disbursement Information System Online; and two mortgage loan program systems—the Government National Mortgage Association's Reporting Feedback System and the Federal Housing Administration's Single Family Premium Collections Subsystem-Upfront system. The community investment system was not randomly selected because the Office of Community Planning and Development had reported no systems that met our criteria for selection. Upon discovering that the system met the criteria above, we added that system to our subset of systems for review since it was the only system reported to meet our criteria for selection.

For the second objective, we obtained information from relevant HUD program offices and reviewed information about the systems used to support the housing, community investment, and mortgage loan programs. Because HUD was not able to provide reliable data from its Cybersecurity Assessment and Management (CSAM) system—the department's repository of information about its information systems' security and privacy—we also requested that these program offices provide us with lists of the department's systems that they use that (1) contain sensitive information and (2) share information with external entities. We then compared this information to other sources of information, including the data analyzed for our first objective, HUD reports about the systems, and information posted on the department's websites. We found that the information the department provided was incomplete and not reliable for identifying the external entities with access to sensitive information in HUD's systems. We address these findings in this report. In addition, we interviewed program office officials responsible for the security and privacy of the housing, community investment, and mortgage loan systems and system owners for the subset of systems selected for the first objective about the extent to which systems contained sensitive information and shared information with external entities.

We conducted this performance audit from September 2018 to September 2020 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.

Appendix II: Comments from the Department of Housing and Urban Development

Appendix II: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

8/18/2020

Ms. Carol C. Harris
Director, Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20415

Dear Ms. Harris:

The Department of Housing and Urban Development (HUD) appreciates the opportunity to review and comment on the draft report for, "*Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities*" (GAO-20-431/ 103041). This report assigned five recommendations to HUD. Please review the attached document for HUD's comments to the draft audit report. Additionally, HUD is taking actions to correct the noted deficiencies in the draft report.

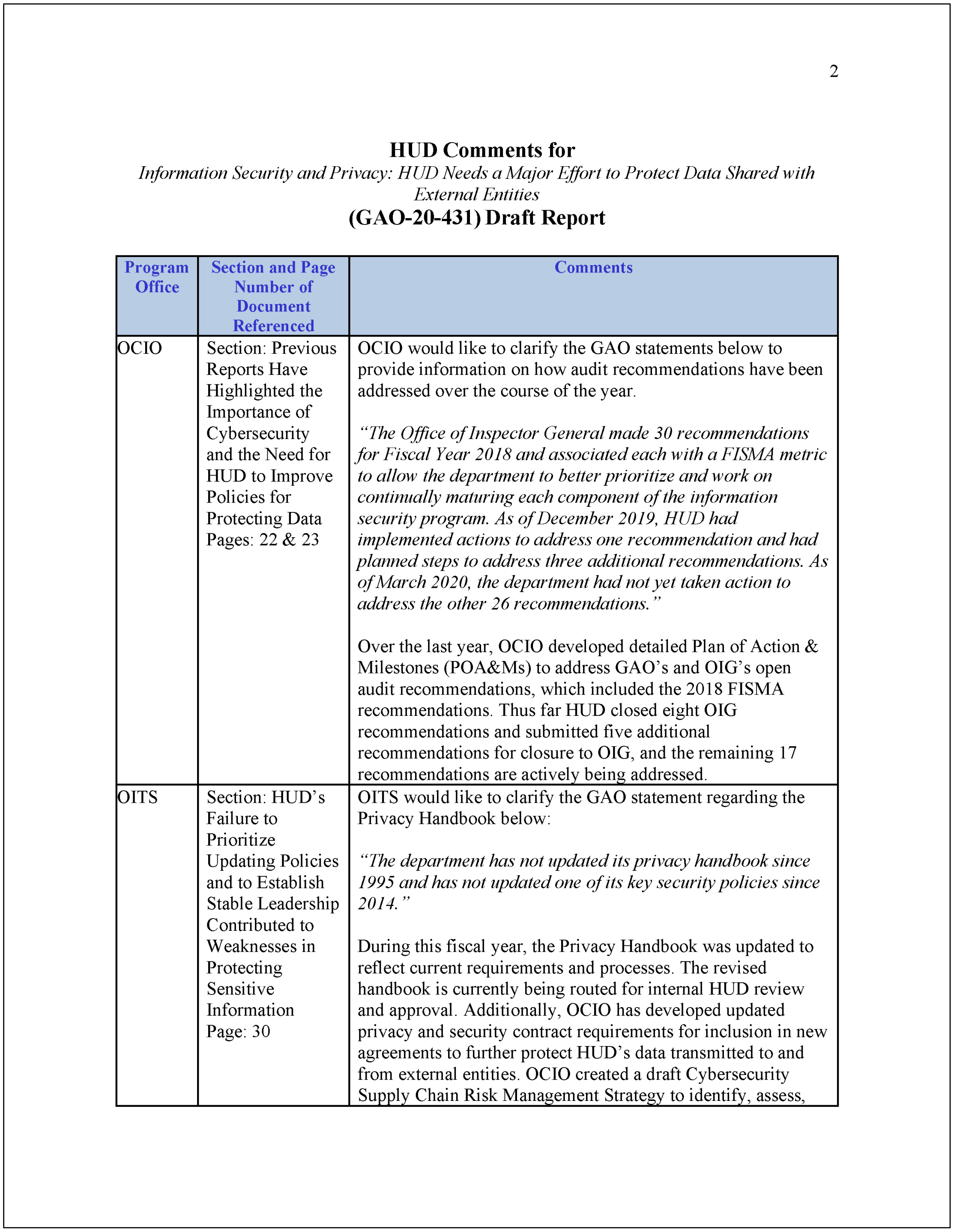
Once again, thank you for the opportunity to review and comment on the draft report. If you have any questions concerning this response, please contact Hun Kim, Chief Information Security Officer (202) 402-8004 (Hun.Kim@hud.gov) or Wyneé Watts-Mitchell, Director of Audit Compliance Branch, at (202) 402-3893 (wynee.wattsmitchell@hud.gov).

Sincerely,

David Chow
Chief Information Officer

Enclosure

www.hud.gov espanol.hud.gov

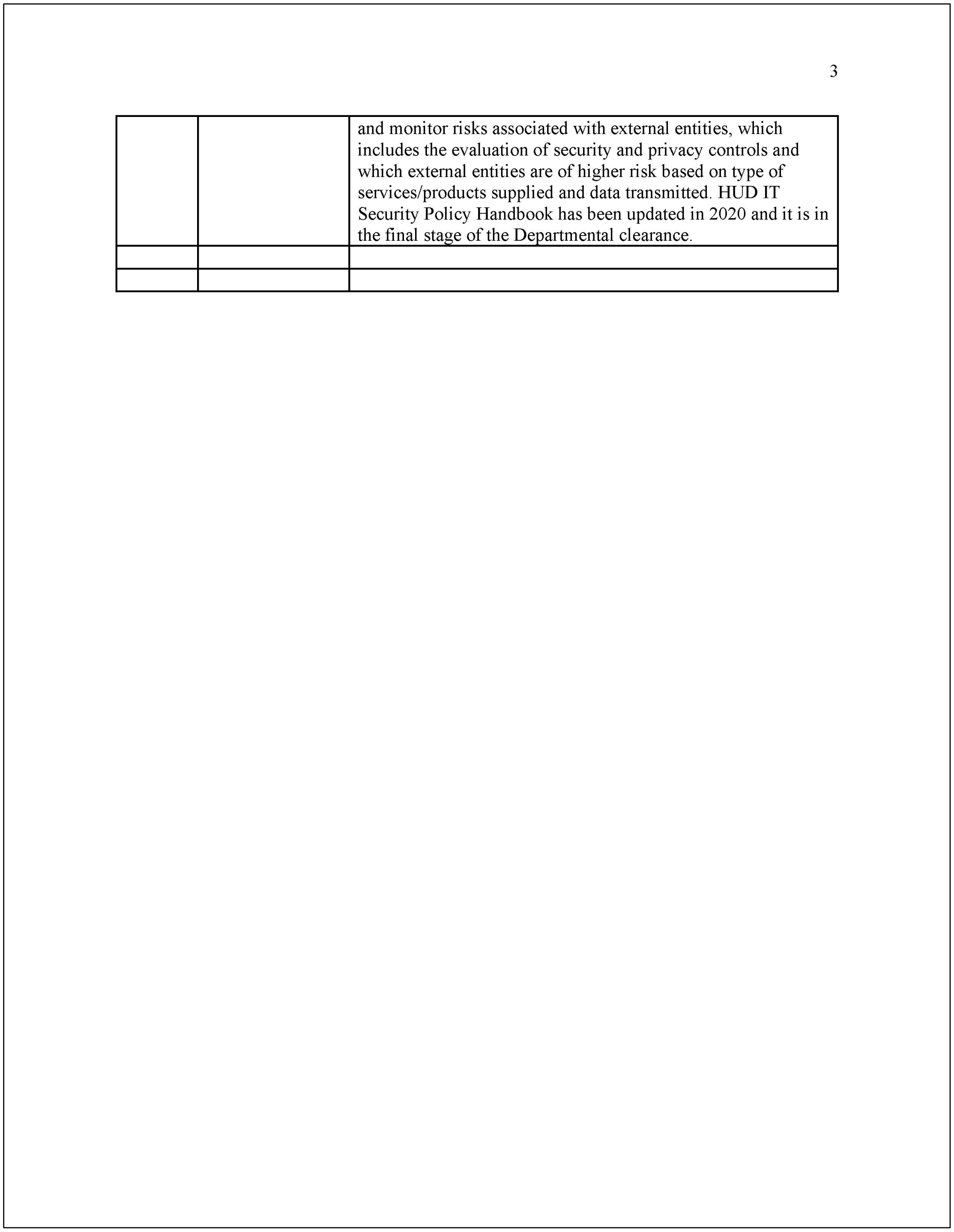


HUD Comments for

Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities

(GAO-20-431) Draft Report

Program Office	Section and Page Number of Document Referenced	Comments
OCIO	Section: Previous Reports Have Highlighted the Importance of Cybersecurity and the Need for HUD to Improve Policies for Protecting Data Pages: 22 & 23	OCIO would like to clarify the GAO statements below to provide information on how audit recommendations have been addressed over the course of the year. *"The Office of Inspector General made 30 recommendations for Fiscal Year 2018 and associated each with a FISMA metric to allow the department to better prioritize and work on continually maturing each component of the information security program. As of December 2019, HUD had implemented actions to address one recommendation and had planned steps to address three additional recommendations. As of March 2020, the department had not yet taken action to address the other 26 recommendations."* Over the last year, OCIO developed detailed Plan of Action & Milestones (POA&Ms) to address GAO's and OIG's open audit recommendations, which included the 2018 FISMA recommendations. Thus far HUD closed eight OIG recommendations and submitted five additional recommendations for closure to OIG, and the remaining 17 recommendations are actively being addressed.
OITS	Section: HUD's Failure to Prioritize Updating Policies and to Establish Stable Leadership Contributed to Weaknesses in Protecting Sensitive Information Page: 30	OITS would like to clarify the GAO statement regarding the Privacy Handbook below: *"The department has not updated its privacy handbook since 1995 and has not updated one of its key security policies since 2014."* During this fiscal year, the Privacy Handbook was updated to reflect current requirements and processes. The revised handbook is currently being routed for internal HUD review and approval. Additionally, OCIO has developed updated privacy and security contract requirements for inclusion in new agreements to further protect HUD's data transmitted to and from external entities. OCIO created a draft Cybersecurity Supply Chain Risk Management Strategy to identify, assess,



		and monitor risks associated with external entities, which includes the evaluation of security and privacy controls and which external entities are of higher risk based on type of services/products supplied and data transmitted. HUD IT Security Policy Handbook has been updated in 2020 and it is in the final stage of the Departmental clearance.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol Harris, (202) 512-4456, harriscc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Eric Winter (assistant director), Andrew Avery, Donald Baca, Chris Businsky, Caitlin Cusati, John deFerrari, Amanda Gill, Rebecca Eyler, Franklin Jackson, Duc Ngo, Cassaundra Pham, Teresa Smith, and Adam Vodraska made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Accessible Text for Appendix II: Comments from the Department of Housing and Urban Development

Page 1

8/18/2020

Ms. Carol C. Harris

Director, Information Technology Acquisition Management Issues

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20415

Dear Ms. Harris:

The Department of Housing and Urban Development (HUD) appreciates the opportunity to review and comment on the draft report for, “Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities” (GAO-20-431/ 103041). This report assigned five recommendations to HUD. Please review the attached document for HUD’s comments to the draft audit report. Additionally, HUD is taking actions to correct the noted deficiencies in the draft report.

Once again, thank you for the opportunity to review and comment on the draft report. If you have any questions concerning this response, please contact Hun Kim, Chief Information Security Officer (202) 402-8004 (Hun.Kim@hud.gov) or Wyneé Watts-Mitchell, Director of Audit Compliance Branch, at (202) 402-3893 (wynee.wattsmitchell@hud.gov).

Sincerely,

David Chow

Chief Information Officer

Enclosure

Page 2

Program Office	Section and Page Number of Document Referenced	Comments
OCIO	Section: Previous Reports Have Highlighted the Importance of Cybersecurity and the Need for HUD to Improve Policies for Protecting Data Pages: 22 & 23	OCIO would like to clarify the GAO statements below to provide information on how audit recommendations have been addressed over the course of the year. *"The Office of Inspector General made 30 recommendations for Fiscal Year 2018 and associated each with a FISMA metric to allow the department to better prioritize and work on continually maturing each component of the information security program. As of December 2019, HUD had implemented actions to address one recommendation and had planned steps to address three additional recommendations. As of March 2020, the department had not yet taken action to address the other 26 recommendations."* Over the last year, OCIO developed detailed Plan of Action & Milestones (POA&Ms) to address GAO's and OIG's open audit recommendations, which included the 2018 FISMA recommendations. Thus far HUD closed eight OIG recommendations and submitted five additional recommendations for closure to OIG, and the remaining 17 recommendations are actively being addressed.
OITS	Section: HUD's Failure to Prioritize Updating Policies and to Establish Stable Leadership Contributed to Weaknesses in Protecting Sensitive Information Page: 30	OITS would like to clarify the GAO statement regarding the Privacy Handbook below: *"The department has not updated its privacy handbook since 1995 and has not updated one of its key security policies since 2014."* During this fiscal year, the Privacy Handbook was updated to reflect current requirements and processes. The revised handbook is currently being routed for internal HUD review and approval. Additionally, OCIO has developed updated privacy and security contract requirements for inclusion in new agreements to further protect HUD's data transmitted to and from external entities. OCIO created a draft Cybersecurity Supply Chain Risk Management Strategy to identify, assess, and monitor risks associated with external entities, which includes the evaluation of security and privacy controls and which external entities are of higher risk based on type of services/products supplied and data transmitted. HUD IT Security Policy Handbook has been updated in 2020 and it is in the final stage of the Departmental clearance.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548