



May 2020

CYBERSECURITY

Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States

Why GAO Did This Study

To protect data that are shared with state government agencies, federal agencies have established cybersecurity requirements and related compliance assessment programs. Specifically, they have numerous cybersecurity requirements for states to follow when accessing, storing, and transmitting federal data.

GAO was asked to evaluate federal agencies' cybersecurity requirements and related assessment programs for state agencies. The objectives were to determine the extent to which (1) selected federal agencies' cybersecurity requirements for state agencies varied with each other and federal guidance, and (2) federal agencies had policies for coordinating their assessments of state agencies' cybersecurity.

GAO reviewed four federal agencies that shared data with states and had assessment programs: CMS, FBI, IRS, and SSA. GAO compared, among other things, each agency's cybersecurity requirements to federal guidance and to other selected agencies' requirements; and reviewed federal agencies' policies for conducting assessments. In addition, GAO examined OMB's efforts to foster coordination among federal agencies. GAO also surveyed and received responses from chief information security officers in 50 out of 55 U.S. states, territories, and the District of Columbia to obtain their perspectives.

What GAO Recommends

GAO is making 12 recommendations to the four selected agencies and to OMB. Three agencies agreed with the recommendations and one agency (IRS) partially agreed or disagreed with them. OMB did not provide comments. GAO continues to believe all recommendations are warranted.

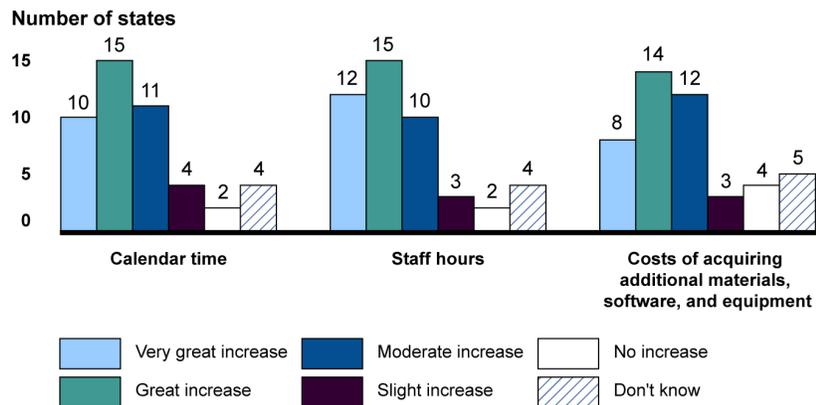
CYBERSECURITY

Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States

What GAO Found

Although the Centers for Medicare and Medicaid Services (CMS), Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), and Social Security Administration (SSA) each established requirements to secure data that states receive, these requirements often had conflicting parameters. Such parameters involve agencies defining specific values like the number of consecutive unsuccessful logon attempts prior to locking out the user. Among the four federal agencies, the percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent. Regarding variance with National Institute of Standards and Technology guidance, GAO found that the extent to which the four agencies did not fully address guidance varied from 9 percent to 53 percent of total requirements. The variances were due in part to the federal agencies' insufficient coordination in establishing requirements. Although the Office of Management and Budget's (OMB) Circular A-130 requires agencies to coordinate, OMB has not ensured that agencies have done so. Further, while federal agencies' variance among requirements may be justified in some cases because of particular agency mission needs, the resulting impact on states is significant, according to state chief information security officers (see figure).

Extent of Impacts Identified by State Chief Information Security Officers as a Result of Variances in Selected Federal Agencies' Cybersecurity Requirements



Source: GAO analysis of 2019 survey of state chief information security officers. | GAO-20-123

Note: Not all respondents answered all survey questions. The figure is based on 46 responses.

The four federal agencies that GAO reviewed either fully or partially had policies for coordinating assessments with states, but none of them had policies for coordinating assessments with each other. State chief information security officers that GAO surveyed reinforced the need to coordinate assessments by identifying impacts on state agencies' costs, including multiple federal agencies that requested the same documentation. Coordinating with state and federal agencies when assessing state agencies' cybersecurity may help to minimize states' cost and time impacts and reduce associated federal costs. Federal agencies reported spending about \$45 million for fiscal years 2016 through 2018 on assessments of state agencies' cybersecurity.

Contents

Letter		1
	Background	7
	Selected Federal Agencies Had a Significant Number of Variances in Cybersecurity Requirements for State Agencies	12
	Selected Federal Agencies' Policies Addressed a Majority of Activities for Coordinating with State Agencies When Assessing Cybersecurity, but Did Not Address Coordinating with Each Other	23
	Conclusions	33
	Recommendations for Executive Action	34
	Agency Comments and Our Evaluation	36
Appendix I	Methodology and Results of GAO's Survey of State Officials' Views	40
Appendix II	Detailed Assessment of Selected Federal Agencies' Policies	51
Appendix III	Breakdown of Selected Federal Agencies' Reported Spending for Fiscal Years 2016 through 2018	56
Appendix IV	Comments from the Department of Health and Human Services	57
Appendix V	Comments from the Federal Bureau of Investigation	62
Appendix VI	Comments from the Social Security Administration	64
Appendix VII	Comments from the Internal Revenue Service	65
Appendix VIII	GAO Contact and Staff Acknowledgements	68

Tables

Table 1: Types of Data That Selected Federal Agencies Share with State Agencies and the Cybersecurity Policies Established to Protect that Data	11
Table 2: Extent to Which Selected Federal Agencies' Cybersecurity Requirements for State Agencies Varied with Each Other and Federal Guidance	12
Table 3: Examples of Federal Agencies' Unique Cybersecurity Requirements for State Agencies	13
Table 4: Examples of Conflicting Parameters in Selected Federal Agencies' Cybersecurity Requirements for State Agencies	14
Table 5: Examples of Cybersecurity Requirements for State Agencies in Which Selected Federal Agencies Did Not Fully Address Guidelines from the National Institute of Standards and Technology (NIST)	16
Table 6: Extent to Which Selected Federal Agencies Established Policies for Coordinating When Assessing State Agencies' Cybersecurity	25
Table 7: Detailed Assessment of the Centers for Medicare and Medicaid Services's (CMS) Policies for Coordinating when Assessing State Agencies' Cybersecurity	51
Table 8: Detailed Assessment of the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services's (CJIS) Policies for Coordinating when Assessing State Agencies' Cybersecurity	52
Table 9: Detailed Assessment of the Internal Revenue Service's (IRS) Policies for Coordinating when Assessing State Agencies' Cybersecurity	53
Table 10: Detailed Assessment of the Social Security Administration's (SSA) Policies for Coordinating when Assessing State Agencies' Cybersecurity	54
Table 11: Selected Federal Agencies' Fiscal Years 2016-2018 Reported Spending for Assessing States' Compliance with Cybersecurity Requirements (expenditures in millions)	56

Figures

Figure 1: State Chief Information Security Officers' Perspectives on the Extent of Variation among Selected Federal Cybersecurity Requirements	18
--	----

Figure 2: Extent of Impacts Reported by State Chief Information Security Officers (CISO) as a Result of Variances in Selected Federal Agencies' Cybersecurity Requirements	19
Figure 3: Average State Staff Hours Expended Per Assessment across Selected Federal Agencies	31
Figure 4: Selected Federal Agencies' Fiscal Years 2016-2018 Reported Spending for Assessing State Compliance with Cybersecurity Requirements	32

Abbreviations

CISO	chief information security officer
CJIS	Criminal Justice Information Services
CMS	Centers for Medicare and Medicaid Services
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act of 2014
IRS	Internal Revenue Service
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SSA	Social Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



May 27, 2020

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Gary J. Palmer
House of Representatives

The federal government exchanges a large variety of personally identifiable and other sensitive information with states to implement key federal and state programs.¹ For example, federal and state agencies exchange taxpayer, law enforcement, and health care data, among many other types of information.

Because of the significant impact that such information can have on a broad array of government operations and assets, effective security controls to protect the information from growing and increasingly sophisticated cyber threats are essential. The Federal Information Security Modernization Act of 2014 (FISMA) and guidance from the Office of Management and Budget (OMB) emphasize that federal agencies are to use risk-based processes for information security.² FISMA provides a comprehensive framework for information security controls over information resources and requires each agency to develop, document, and implement an agency-wide information security program to provide

¹Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

²The Federal Information Security Modernization Act of 2014 (FISMA 2014) Pub. L. No. 113-283, 128 Stat. 3073 (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.

risk-based protections for the information and information systems that support the operations and assets of the agency.

To protect and secure the sensitive information exchanged with states, each federal agency that exchanges data has specific regulations, guidelines, or other requirements for states to follow when accessing, storing, and transmitting the data. Further, federal agencies have established assessment programs to ensure that the state agencies comply with their cybersecurity requirements.

At your request, we evaluated federal agencies' cybersecurity requirements and related assessment programs for state agencies. Our specific objectives were to determine the extent to which (1) selected federal agencies' cybersecurity requirements for state agencies varied with each other and federal guidance, and (2) federal agencies had policies for coordinating their assessments of state agencies' cybersecurity.

To accomplish the objectives, we first selected a sample of federal agencies for our review. To do so, we determined which of the 24 agencies covered by the Chief Financial Officers Act³ (1) shared data with state agencies; (2) had a standard, minimum set of cybersecurity requirements to protect these data;⁴ and (3) conducted regularly scheduled assessments of states' compliance with the requirements.⁵ We identified four agencies that met these criteria: the Centers for Medicare and Medicaid Services (CMS) within the Department of Health and Human Services, the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) within the Department of Justice, the Internal Revenue Service (IRS) within the Department of the Treasury,

³The 24 agencies covered by the Chief Financial Officers Act are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs as well as the U.S. Agency for International Development, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration.

⁴We defined standard cybersecurity requirements as a consistent, documented set of requirements to protect data that is shared between the federal and state agencies.

⁵We included agencies that reviewed cybersecurity control assessments conducted by third parties (e.g., a contractor selected by the state) as part of the federal agency's assessment of a states' compliance with its requirements.

and the Social Security Administration (SSA). The results of our review of these four agencies are not generalizable to other federal agencies.

For the first objective, we reviewed the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4),⁶ to identify cybersecurity controls and control enhancements⁷ that we could use as a basis for comparing federal agencies' cybersecurity requirements for state agencies. We specifically chose those controls and control enhancements where organizations, such as the federal agencies we selected, are to define specific values when tailoring their requirements.⁸ Based on this criterion, we identified a nonprobability sample of 616 (out of 1,682) cybersecurity controls and control enhancements for our review.

Then, for each of the four selected federal agencies, we identified its cybersecurity requirements that state agencies are to comply with when exchanging data with the federal agency. These requirements were documented in:

- IRS, Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information*;⁹

⁶National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013). NIST Special Publication 800-53 is the set of baseline controls which provide guidance to agencies on the selection and implementation of information security and privacy controls for systems.

⁷According to NIST, controls are safeguards and countermeasures that are necessary to protect an organization's confidentiality, integrity, and availability of its information; control enhancements are expansions of security controls to increase their effectiveness.

⁸For example, for the control related to unsuccessful logon attempts, an agency is to define the number of consecutive invalid logon attempts by a user during a given time period before a user's account is automatically locked (NIST control AC-7).

⁹Internal Revenue Service, *Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information* (September 2016).

-
- CMS, *MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*;¹⁰
 - Department of Justice, *Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Security Policy*;¹¹ and
 - SSA, *Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration*.¹²

We compared each selected federal agency's cybersecurity requirements for state agencies to the other three selected federal agencies' requirements, and to guidance associated with the 616 selected controls and control enhancements specified in NIST Special Publication 800-53. In doing so, we considered three specific instances in which the federal agencies' requirements could vary:

- When a federal agency had a requirement that the other three federal agencies did not have. We refer to such variances as unique requirements.
- When a federal agency had in its requirements, specific values that are to be defined by individual federal agencies that differed from at least one of the other three federal agencies. We refer to such variances as requirements with conflicting parameters.
- When a federal agency did not fully address in its requirements the guidelines from NIST for associated controls and control enhancements.¹³ We refer to such variances as requirements that did not fully address NIST guidelines.

¹⁰Centers for Medicare and Medicaid Services, *MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* (November 2015).

¹¹Department of Justice, Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.8 (June 2019).

¹²Social Security Administration, *Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration*, Version 8.0, (July 2019).

¹³We determined that agency's requirement did not fully address guidelines from NIST when the requirement addressed some, but not all, aspects of a control or control enhancement. For instance, an agency requirement may not have defined an agency-specific parameter or other aspects of the control as called for by NIST.

We also reviewed OMB Circular A-130, *Managing Information as a Strategic Resource*, which identifies requirements for federal agencies to coordinate when establishing cybersecurity requirements for nonfederal entities, such as state agencies.¹⁴ In addition, we reviewed practices that GAO recommended regarding ways that federal agencies may enhance and sustain coordination and collaboration with each other.¹⁵ We also reviewed practices that NIST recommended on ways that federal agencies may coordinate on their development of cybersecurity requirements to satisfy common security objectives.¹⁶ We then assessed whether the selected federal agencies were implementing the OMB requirements and recommended practices.

To address the second objective, we reviewed relevant requirements in OMB Circular A-130 that pertained to federal agencies' coordination on assessments of state agencies' cybersecurity. We also identified practices recommended by GAO for federal agencies to coordinate in an effort to better manage potential fragmentation, overlap, or duplication through coordination.¹⁷ In addition, we identified practices recommended by NIST related to federal agencies' coordination on assessments of cybersecurity.¹⁸

Based on our reviews of these guidance documents, we identified two broad areas of coordination that were relevant to federal agencies' assessments of state agencies' cybersecurity: (1) coordination with state agencies when assessing states' cybersecurity and (2) coordination with

¹⁴OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

¹⁵GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012); and *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

¹⁶National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

¹⁷GAO, *Fragmentation, Overlap and Duplication: An Evaluation and Management Guide* [GAO-15-49SP](#) (Washington, D.C.: April 2015).

¹⁸NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Special Publication 800-53A, Revision 4 (Gaithersburg, Md.: December 2014); and *Technical Guide to Information Security Testing and Assessment*, Special Publication 800-115 (Gaithersburg, Md.: September 2008).

other federal agencies on the assessments of state agencies' cybersecurity.

Using guidance from NIST that pertained to coordination on assessments of cybersecurity and practices recommended by GAO for enhancing coordination among federal agencies, we identified four supporting activities that were common to each of these two areas of federal agencies' coordination on cybersecurity assessments:¹⁹

- assessment schedules and time frames,
- meeting and document requests,
- security test plans, and
- the use of findings from prior assessments.

We then analyzed the selected federal agencies' policies and related procedures for conducting assessments of state agencies' cybersecurity, as discussed in relevant documentation, such as assessment methodologies, pre-evaluation questionnaires, and report templates. In doing so, we reviewed agencies' policies to identify whether there was discussion of the four activities supporting the two areas of coordination with state agencies and with other federal agencies.

We determined that an agency

- fully addressed an area of coordination if its policies included discussion about coordination on all of the four supporting activities;
- partially addressed an area of coordination if its policies included discussion of some, but not all, of the supporting activities; and
- did not address an area of coordination if its policies did not include any discussion of the supporting activities.

We supplemented our documentation review with interviews of cognizant officials from FBI's CJIS Information Technology Management Section and the CJIS Audit Unit; IRS's Office of Safeguards; CMS's Office of Information Technology; and SSA's offices of General Counsel; Analytics, Review, and Oversight; and Deputy Commissioner for Systems. We discussed with agency officials our observations of variances in agencies'

¹⁹NIST Special Publication 800-53A, NIST Special Publication 800-115, and [GAO-15-49SP](#).

cybersecurity requirements for state agencies, as well as their policies for coordinating with state agencies and other federal agencies when assessing state agencies' cybersecurity. We also interviewed officials from OMB's Office of E-Government and Information Technology to discuss the extent to which federal agencies have coordinated on their assessments of state agencies' cybersecurity.

In addition, for both objectives, we administered a survey to the offices of the Chief Information Officer and Chief Information Security Officer (CISO) in the 50 states, District of Columbia, American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands. We received survey responses from 50 of these 55 states and territories, and the District of Columbia.²⁰

The survey requested these officials' perspectives on the nature of any variances among federal cybersecurity requirements, the officials' experiences in implementing the requirements, and their views on oversight performed by federal agencies. Several questions from our survey requested that state CISOs provide their subjective views based on a range of alternatives. For example, regarding the question on the extent to which federal cybersecurity requirements varied, we asked state CISOs to identify the extent of variation for three scenarios as very great, great, moderate, slight, none, or unknown. See appendix I for a more detailed discussion of our survey methodology and results.

We conducted this performance audit from July 2018 to May 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

Federal agencies are dependent on information systems and electronic data to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out

²⁰Not all state CISOs who completed the survey responded to all questions. The number of responses received for each question varied.

their missions and account for their resources without these information assets.

Federal agencies exchange personally identifiable and other sensitive information with state agencies in the implementation of key federal and state programs.²¹ The security of systems and data involved in this exchange of information is vital to public confidence and the nation's safety, prosperity, and well-being.

Since federal agencies face computerized (cyber) threats that continue to grow in number and sophistication, it is imperative that such information is protected. In recognition of this growing threat, we designated information security as a government-wide high-risk area in 1997.²² We further expanded this area in 2015 to include protecting the privacy of personally identifiable information.²³

Federal Law and Policy Set Roles and Responsibilities for Protecting Federal Systems and Managing Cybersecurity Risk

Several federal laws and policies establish requirements for protecting federal systems and managing cybersecurity risks. Specifically, FISMA is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. The act requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or managed by another entity.

FISMA also assigns government-wide responsibilities to key agencies. For example, OMB is responsible for developing and overseeing implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national

²¹Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

²²GAO, *High-Risk Series: An Overview*, [GAO-HR-97-1](#) (Washington, D.C.: February 1997) and *High-Risk Series: Information Management and Technology*, [GAO-HR-97-9](#) (Washington, D.C.: February 1997).

²³GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

security systems.²⁴ NIST is also responsible for developing standards for categorizing information and information systems, security requirements for information and systems, and guidelines for detection and handling of security incidents. For example, NIST Special Publication 800-53 provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.²⁵

Further, OMB Circular A-130, *Managing Information as a Strategic Resource*, establishes minimum requirements for federal information security programs and assigns federal agency responsibilities for the security of information and information systems.²⁶ It requires agencies to implement a risk management framework to guide and inform the categorization of federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.

Circular A-130 also requires federal agencies to provide oversight of nonfederal entities—such as state agencies—that use or operate federal information systems, as well as nonfederal entities’ information systems that collect or maintain federal information. In doing so, federal agencies are to ensure that security and privacy controls for such information systems are effectively implemented and comply with NIST standards and guidelines and agency requirements.

Federal agencies may share data with one or more individual component agencies within a state, such as agencies that execute a state’s tax administration, law enforcement, or human services functions. The state’s responsibility for protecting data shared by federal agencies may reside within an individual state agency or it may be a shared responsibility with the state’s chief information officer and CISO. For example, a state CISO may help to manage the protections over centralized information

²⁴The Department of Homeland Security is responsible for certain operational aspects of agencies’ information security policies and practices, including assisting OMB in fulfilling its FISMA authorities, issuing binding operational directives, monitoring agencies’ security policies and practices, and assisting agencies with implementation.

²⁵National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

²⁶OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

technology (IT) resources that store, process, and transmit federal data for multiple component agencies within the state.

To protect federal data that are shared with state agencies in the implementation of key federal and state programs, federal agencies have developed cybersecurity requirements for state agencies to follow when accessing, storing, and transmitting federal data. Federal agencies are to obtain assurance that state agencies' security and privacy controls are effectively implemented through independent evaluations. These evaluations include tests and assessments of the effectiveness of state agencies' information security policies, procedures, and practices.²⁷ Such assessments are important inputs to decisions by federal officials to authorize or reauthorize a state agency's use of information systems that create, collect, use, process, store, maintain, disseminate, disclose, and dispose of federal information.²⁸

Selected Federal Agencies Have Established Policies and Compliance Assessment Programs to Protect Data Shared with State Agencies

To protect federal data that are shared with state agencies, each of the federal agencies in our review have established their own policies that articulate cybersecurity requirements, as well as related compliance assessment programs, based in part on guidance from NIST.²⁹

Table 1 identifies the types of data that the four selected federal agencies share with state agencies and the cybersecurity policies that they have established to protect that data.

²⁷Under FISMA, agencies are responsible for providing information security for the information and information systems that support the operations and assets of the agency, including those used or operated by another agency, contractor, or other source on behalf of the agency.

²⁸According to NIST, an authorization is the process by which a senior management official, the authorizing official, reviews security and privacy information describing the current security and privacy posture of information systems or common controls that are inherited by systems. The authorizing official uses this information to determine if the mission/business risk of operating a system or providing common controls is acceptable—and if it is, explicitly accepts the risk.

²⁹Officials from each of the four federal agencies that we reviewed (CMS, FBI's CJIS, IRS, and SSA) stated that they were planning to review and potentially update their existing security policies based on anticipated changes in NIST Special Publication 800-53 (Revision 5), which was in draft as of February 2020.

Table 1: Types of Data That Selected Federal Agencies Share with State Agencies and the Cybersecurity Policies Established to Protect that Data

Federal agency	Type of data shared with states	Agency security policy applicable to state agencies	Legal authorities and requirements referred to in agency policy
Centers for Medicare and Medicaid Services (CMS)	Certain health care information that have specified human services and health care related functions under the Patient Protection and Affordable Care Act.	Minimum Acceptable Risk Standards for Exchanges	Provides guidance to state administering entities and their contractors responsible for implementing privacy and security controls specified in regulations implementing the Patient Protection and Affordable Care Act (45 C.F.R. §§ 155.260, 155.280). ^a
Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS)	State criminal justice information—including biometric, biographic, property, criminal history, and case/incident data—for use by state agencies that perform law enforcement functions.	CJIS Security Policy	Incorporates presidential directives, federal laws, FBI directives, and criminal justice Advisory Policy Board decisions to provide guidance on minimum security controls and requirements needed to access FBI CJIS information. Further, 28 C.F.R. Part 20 provides regulatory guidance for the dissemination of criminal history records information, a subset of criminal justice information.
Internal Revenue Service (IRS)	Federal tax information used by state agencies that have financial and tax administration related functions.	Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information	Provides guidance about policies, practices, controls, and safeguards to be employed by recipient agencies in accordance with the Internal Revenue Code. For example, Internal Revenue Code Section 6103 protects the confidentiality of federal tax information and Section 7213 prescribes criminal penalties for illegal disclosure of federal tax information.
Social Security Administration (SSA)	Personally identifiable information used by Electronic Information Exchange partners, such as state agencies that rely on such data to perform their mission.	Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies for Exchanging Electronic Information with the Social Security Administration	Provides guidance to ensure Electronic Information Exchange partners adequately safeguard information provided to them by SSA in accordance with the Federal Information Security Modernization Act, National Institute of Standards and Technology standards, the Privacy Act of 1974, and Sections 453, 1106, and 1137 of the Social Security Act.

Source: GAO analysis of agencies' security policies. | GAO-20-123

^aAccording to CMS, administering entity means health insurance exchanges or marketplaces, whether federal or state, state Medicaid agencies, Children's Health Insurance Program agencies, or state agencies administering the Basic Health Program.

Selected Federal Agencies Had a Significant Number of Variances in Cybersecurity Requirements for State Agencies

The selected federal agencies' had a significant number of variances in the cybersecurity requirements that they had established for protecting data exchanged with state agencies. Specifically, our review identified hundreds of instances in which the four agencies either had (1) included a requirement in its cybersecurity policy that was not a requirement of the other three agencies (unique requirement); (2) established a requirement with specific, organization-defined technical thresholds that differed from at least one of the other three agencies for a related control (conflicting parameters); or (3) did not fully address in its requirements the guidelines from NIST for associated controls and control enhancements (did not fully address NIST guidelines).

Table 2 summarizes the total number of requirements that each agency had included in its security policy and the extent to which the four agencies' requirements varied from each other and from the NIST guidance.

Table 2: Extent to Which Selected Federal Agencies' Cybersecurity Requirements for State Agencies Varied with Each Other and Federal Guidance

	CMS	FBI's CJIS	IRS	SSA
Total number of requirements included in each agency's policy^a	281	118	220	61
Type of variance				
Unique requirements	54	24	5	3
Requirements included in agency policy that other agencies did not include	(19%)	(20%)	(2%)	(5%)
Conflicting parameters	139	72	131	48
Requirements with differences in technical thresholds from at least one of the other selected agencies for a related control	(49%)	(61%)	(60%)	(79%)
Did not fully address guidelines from National Institute of Standards and Technology (NIST) guidance	26	63	22	30
Agency requirements that did not fully address the guidelines from NIST for associated controls and control enhancements	(9%)	(53%)	(10%)	(49%)

Source: GAO analysis of selected federal agencies' data. | GAO-20-123

Note: CMS = Centers for Medicaid and Medicare Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

^aWe examined a nonprobability sample of 616 cybersecurity controls and control enhancements from NIST Special Publication 800-53. Of the 616 controls, each agency selected a number of these controls to include in its cybersecurity requirements policy. For example, for the control related to unsuccessful logon attempts, an agency is to define the number of consecutive invalid logon attempts by a user during a given time period before a user's account is automatically locked (NIST control AC-7).

Selected Federal Agencies Had Unique Cybersecurity Requirements for State Agencies

Collectively, the four selected federal agencies' policies included 86 unique cybersecurity requirements for state agencies with which they exchange data. Specifically, CMS's policy included 54 requirements that the other three agencies did not include. FBI's CJIS's policy included 24 unique requirements, IRS's policy included five unique requirements, and SSA's policy included three unique requirements. For example, CMS's security policy included a requirement that state agencies review their organization-wide information security program plan annually; however, the other three agencies did not have such a requirement in their security policies. As another example, IRS had a requirement for state agencies to employ automated mechanisms to alert security personnel of inappropriate activities, while the other agencies did not have this requirement.

Because each agency is addressing different legal requirements and risk management approaches for protecting information shared with states, certain requirements that are unique to an agency may be necessary. Nevertheless, agencies need to ensure that such requirements are necessary by documenting their decisions during the control selection process.

Table 3 provides examples of the unique requirements that each agency included in its cybersecurity policies.

Table 3: Examples of Federal Agencies' Unique Cybersecurity Requirements for State Agencies

Agency	Examples of unique cybersecurity requirements
CMS	<ul style="list-style-type: none"> Review the organization-wide information security program plan annually. Employ automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system.
FBI's CJIS	<ul style="list-style-type: none"> Control physical access by authenticating visitors before authorizing escorted access to the physically secure location and escort visitors at all times to monitor visitor activity. Configure agency applications, services, or information systems to provide only essential capabilities and prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
IRS	<ul style="list-style-type: none"> Purge/wipe information from mobile devices (e.g., personal digital assistants, smartphones and tablets) based on 10 consecutive, unsuccessful device logon attempts. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications.
SSA	<ul style="list-style-type: none"> Authorize read-only access to audit information to authorized users with a need to know privilege. Review employees, contractors, and agent's system access periodically to determine if the same levels and types of access remain applicable. The senior management official's entity responsible for management oversight should consist of one or more management officials whose job functions include responsibility to ensure that only appropriate users and position types are granted access.

Source: GAO analysis of agency data. | GAO-20-123

Note: CMS = Centers for Medicare and Medicaid Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

Selected Federal Agencies Had Conflicting Parameters in Their Cybersecurity Requirements for State Agencies

In total, the four federal agencies had identified 390 requirements for state agencies in their policies, where the parameters conflicted with at least one of the other federal agencies. Across the four agencies, CMS had the largest number of requirements that had conflicting parameters, with 139 such requirements. This was followed by IRS with 131, FBI's CJIS with 72 requirements, and SSA with 48 requirements with conflicting parameters.

For example, each of the selected agencies identified a different time frame for the retention of audit logs related to audited events. As another example, CMS required state agencies to annually review and update their access control policies, whereas IRS required this review every 3 years. FBI's CJIS and SSA did not have this requirement in their policies.

Table 4 provides additional examples of cybersecurity requirements for state agencies that the four federal agencies identified in their policies, where the parameters conflicted with those of at least one other of the federal agencies.

Table 4: Examples of Conflicting Parameters in Selected Federal Agencies' Cybersecurity Requirements for State Agencies

Requirements	CMS	FBI's CJIS	IRS	SSA
Amount of time state agencies should retain audit records, ^a which are individual entries in an audit log related to an audited event	10 years	1 year	7 years	3 years, preferably 7 years
Frequency of assessments of security controls in the information system environment	Annually	Every 3 years	Annually	Did not define a frequency
Frequency of providing basic security awareness training to information system users	Annually	Within 6 months of assignment and biennially thereafter	Annually	Annually
Frequency of reviews and updates to access control policies	Annually	Not applicable ^b	Every 3 years	Not applicable ^b
Number of consecutive login attempts before user is locked out	3 attempts within 15 minutes	No more than five	No more than three within 120 minutes	No fewer than three and no more than five
Frequency of scans for vulnerabilities in the information system	Monthly	Did not specify a frequency	Monthly	Did not specify a frequency
Frequency of review and updates to agency risk assessment policies	Annually	Not applicable ^b	Every 3 years	Did not specify a frequency

Source: GAO analysis of agency data. | GAO-20-123

Note: CMS = Centers for Medicare and Medicaid Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

^aThe retention of audit records refers to records retained to ensure that there are sufficient controls to provide auditable evidence for system transactions. The retention of audit records does not refer to agency recordkeeping under the Federal Records Act.

^bThe agency did not select this requirement to include in its cybersecurity policy.

Selected Federal Agencies Did Not Always Fully Address NIST Guidelines in Their Cybersecurity Requirements for State Agencies

The four selected federal agencies did not always fully address guidelines in NIST Special Publication 800-53 (Revision 4) when establishing cybersecurity requirements for related controls, leading to additional differences among the four agencies' cybersecurity policies. In total, the four agencies did not fully address guidelines from NIST in 141 instances. FBI's CJIS had the most variances, with 63 requirements that did not fully address NIST guidelines, followed by SSA with 30 variances, CMS with 26 variances, and IRS with 22 variances.

For example, FBI's CJIS's requirement did not identify the time period to retain individual training records, as called for by NIST guidance. In addition, SSA did not define the frequency of how often agencies should assess the security controls in the information system and its environment of operation.

Table 5 provides examples of the cybersecurity requirements for state agencies in which selected federal agencies did not fully address NIST guidelines.

Table 5: Examples of Cybersecurity Requirements for State Agencies in Which Selected Federal Agencies Did Not Fully Address Guidelines from the National Institute of Standards and Technology (NIST)

Agency	NIST guidelines (control reference)	Agency variances
CMS	<ul style="list-style-type: none"> Specified that organizations take defined actions when privileged role assignments are no longer appropriate. (AC-2(7)(c)) Recommended that the information system implement multifactor authentication for remote access and that the device meets organization-defined strength of mechanism requirements. (IA-2(11)) 	<ul style="list-style-type: none"> Specified that agencies monitor privileged and application-specific role assignments, but did not identify actions to be taken when assignments are no longer appropriate. Did not include terminology to identify organization-defined strength of mechanism requirements.
FBI's CJIS	<ul style="list-style-type: none"> Identified that the information system should provide an alert in a specific time period to defined personnel when a specific audit failure event occurs. (AU-5(2)) Recommended that agencies retain individual training records for a specified time period. (AT-4(b)) 	<ul style="list-style-type: none"> Defined personnel that are to receive an alert when a specific audit failure occurs, but it did not identify a specific time period for the system to provide an alert. Specified that agencies retain individual training records, but did not identify the time period to retain them.
IRS	<ul style="list-style-type: none"> Identified the prohibition of password reuse for an organization defined number of generations. (IA-5(1)(e)) Recommended that the information system uniquely identify and authenticate organization-defined specific and/or types of devices before establishing a local, remote or network connection. (IA-3) 	<ul style="list-style-type: none"> Established minimum and maximum lifetime restrictions and reuse conditions for authenticators, but did not identify the prohibition of password reuse for an organization-defined number of generations. Did not specify devices or the type of connection allowed.
SSA	<ul style="list-style-type: none"> Recommended that agencies assess the security controls in the information system and its environment of operation at an organization-defined frequency. (CA-2b) Recommended that agencies move from online storage and store organization defined information offline in a secure location. (SC-28(2)) 	<ul style="list-style-type: none"> Did not define the frequency of how often agencies should assess the security controls. Did not identify the type of information to be moved to an offline secure location.

Source: GAO analysis of agency data. | GAO-20-123

Note: CMS = Centers for Medicare and Medicaid Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

Majority of State CISOs Reported Moderate to Very Great Variation in Selected Federal Agencies' Cybersecurity Requirements and Increased Impacts from the Variances

The perspectives of state CISOs³⁰ who responded to our survey reflected the variation we found among the selected federal agencies' cybersecurity requirements. The majority (at least 29 out of 50) of the state CISOs that responded to our survey question regarding the ways in which federal cybersecurity requirements vary and the extent of the variation reported moderate to very great variation in the selected federal agencies' cybersecurity requirements. Specifically, of the 50 state CISOs that responded to this question,

- 34 reported that the federal agencies had moderate to very great variation with respect to unique requirements,³¹
- 38 reported that the federal agencies had moderate to very great variation due to conflicting parameters that were established,³² and
- 29 reported that the federal agencies had moderate to very great variation with respect to addressing NIST guidelines for security controls and control enhancements.³³

Figure 1 represents state CISOs' perspectives on the extent of variation among selected federal cybersecurity requirements.

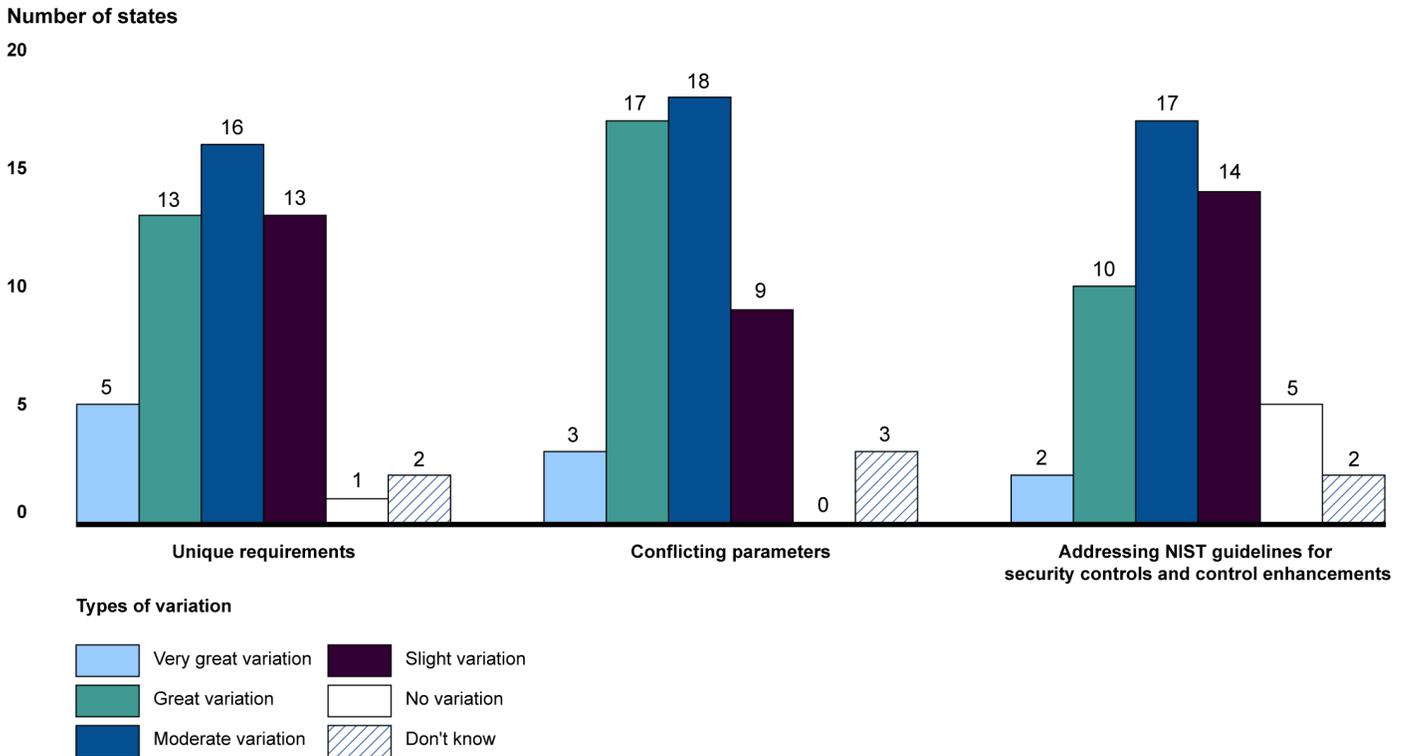
³⁰The use of the term state CISOs also includes territory CISOs or their equivalent.

³¹In our survey, we referred to this as "specific controls selected." See appendix I, question 4 for the question and responses.

³²In our survey, we referred to this as "parameters or thresholds." See appendix I, question 4 for the question and responses.

³³In our survey, we referred to this as "how agencies' requirement language matches NIST 800-53 control language." See appendix I, question 4 for the question and responses.

Figure 1: State Chief Information Security Officers' Perspectives on the Extent of Variation among Selected Federal Cybersecurity Requirements



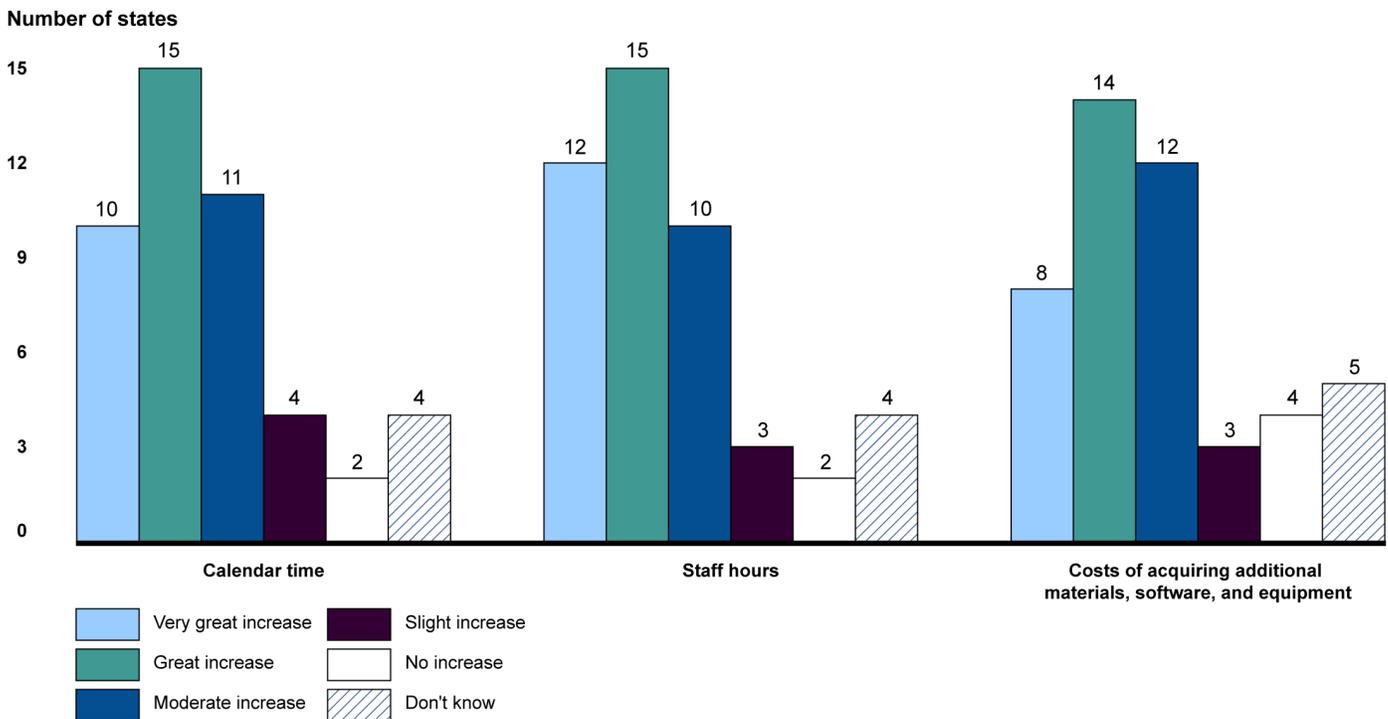
Source: GAO analysis of 2019 survey of state chief information security officers. | GAO-20-123

State agency officials that must comply with multiple federal agencies' cybersecurity requirements (and related compliance assessments) viewed variances as problematic and burdensome. For example, in responding to a survey question about challenges or impacts that state officials experienced regarding federal requirements and assessment processes, an official from one state agency explained that addressing variances in cybersecurity requirements reduced the ability of state officials to focus on their primary mission of securing data across their state enterprise. In response to the same survey question, another state official said that addressing the variances in federal agencies' cybersecurity requirements increased the complexity of automating the state's monitoring and reporting processes. In addition, the same state official commented that staff were burdened by reports and reviews to ensure that the full range of federal agencies' requirements were met.

In responding to our survey, 46 state CISOs reported the extent to which they had experienced a very great, great, moderate, slight, or no increase in calendar time; staff hours; and costs of acquiring additional materials, software, and equipment to address variances in selected federal agencies' cybersecurity requirements. The majority (at least 34 out of 46) of the state CISOs that responded to this question in our survey reported moderate to very great increases in these types of impacts.

Figure 2 represents the extent of impacts that state CISOs reported as a result of variances in selected federal cybersecurity requirements.

Figure 2: Extent of Impacts Reported by State Chief Information Security Officers (CISO) as a Result of Variances in Selected Federal Agencies' Cybersecurity Requirements



Source: GAO analysis of 2019 survey of state chief information security officers. | GAO-20-123

Note: Forty-six of the 50 state CISOs that responded to our survey answered this question.

Selected Federal Agencies' Insufficient Coordination Contributed to Variances in Cybersecurity Requirements for State Agencies

OMB Circular A-130 requires federal agencies to coordinate with nonfederal entities, such as state agencies, as well as other federal agencies as appropriate, to ensure that security and privacy requirements pertaining to these nonfederal entities are consistent to the greatest extent possible. In addition, GAO and NIST have identified practices that can help federal agencies limit potential variation in security control selection and requirements, such as coordinating to develop compatible policies, procedures, and other means to operate across agency boundaries.³⁴ For example, according to NIST, agencies can establish a tailored set of baseline requirements to satisfy common security objectives.³⁵ In addition, by applying practices recommended by GAO for enhancing and sustaining coordination and collaboration, federal agencies could work towards establishing shared requirements with consistent terminology and parameters.

However, the four selected federal agencies have not ensured that their cybersecurity requirements for state agencies are consistent to the maximum extent possible through coordination with each other. Officials from IRS, FBI, and SSA acknowledged that they had not coordinated with other federal agencies in establishing their current cybersecurity requirements for state agencies. The agencies had not coordinated, in part, because they have prioritized addressing agency-specific responsibilities from relevant laws and agency policies as well as the needs of relevant communities of interest.

CMS officials stated that the agency coordinated with other federal agencies in 2015 when CMS originally established requirements for its security policy, the *Minimum Acceptable Risk Standards for Exchanges Document Suite 2.0, Volume III: Minimum Acceptable Risk Standards for Exchanges*. CMS officials noted that the agency added controls that IRS and SSA deemed essential to protecting data for which these agencies

³⁴GAO, *Managing for Results: Key Considerations for Implementing Key Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012); *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005); and National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

³⁵NIST refers to a tailored set of baseline requirements for community-wide use to satisfy common security objectives as overlays. According to NIST Special Publication 800-53 (Revision 4), tailored baselines such as these can be developed and provided to large communities of interest to achieve standardized security capabilities, consistency of implementation, and cost-effective security solutions.

were responsible. Nevertheless, we found variances between CMS's requirements and those established by IRS and SSA. Further, CMS last updated its security policy in September 2015 and IRS, SSA, and FBI's CJIS have each since updated their policies.

In addition to the insufficient coordination, the selected federal agencies identified two additional explanations for variances in their cybersecurity requirements for state agencies: (1) agencies' determination that selected requirements were necessary and therefore, that resulting variances are warranted and (2) agencies' requirements review processes that resulted in deviations from NIST guidance.

- Each of the selected agencies noted that they determined the unique controls and competing parameters in their requirements were necessary and warranted. For example, SSA noted that it has been conducting data exchanges with states since the late 1970s, predating NIST Special Publication 800-53. According to SSA officials, the agency's security requirements retained certain legacy language that state agencies were already familiar with to reduce disruption to them. IRS officials also noted that their security controls incorporate disclosure restrictions from the Internal Revenue Code and internal IRS directives.
- Agency processes for reviewing their cybersecurity requirements have resulted in deviations from NIST guidance. For example, FBI's CJIS officials stated that they started with NIST terminology when developing their policy. However, CJIS's Advisory Policy Board—which recommends the final CJIS policy to the FBI Director—suggested modifications to the wording of requirements during subsequent reviews. As another example, CMS noted that during the review process for its requirements, in certain instances it deviated from NIST guidance to use terminology that would be more familiar to state agency users.

Federal agencies may have legitimate reasons for having variances in their cybersecurity requirements. For instance, agencies may need to apply different information security controls, a greater number of controls, or more stringent technical parameters to protect data for which they are responsible in a manner consistent with various security requirements originating in federal laws, executive orders, directives, policies, regulations, standards, or guidelines as well as the agency's risk assessments. However, according to NIST, organizations should document the relevant decisions taken during the control selection

process, and provide a sound rationale for those decisions that is based on agency mission and business needs.³⁶

Both FBI's CJIS and IRS had documented the agency's rationale for unique requirements. SSA stated that their controls were developed before NIST standards were created and they have mapped their current controls to NIST. However, SSA was unable to produce this documentation. CMS officials noted that the rationale for the requirements identified in the agency's Minimum Acceptable Risk Standards for Exchanges security policy was documented in CMS's Acceptable Risk Standards.³⁷ However, the Acceptable Risk Standards did not include all requirements that were included in CMS's security policy. For example, CMS's requirements for organizations to review and re-evaluate privileges at least quarterly and for the information system to allocate resources by priority and/or quota were included in the security policy without a defined rationale and were also not included in CMS's Acceptable Risk Standards.

While agencies have identified various reasons for not coordinating on their cybersecurity requirements for state agencies, OMB has not taken steps to evaluate whether agencies are coordinating. OMB officials acknowledged that they could encourage additional coordination among the selected agencies, but said that it is ultimately up to the agencies to set their requirements and determine how best to assess states' compliance with those requirements. However, without OMB's involvement and encouragement that federal agencies collaborate to make their cybersecurity requirements for state agencies consistent to the greatest extent possible, federal agencies are less likely to prioritize such efforts.

The selected federal agencies will soon have an opportunity to harmonize to the extent possible their requirements as they revisit and potentially update their existing security policies based on anticipated changes in NIST guidance. Until these agencies coordinate, where feasible, to address the variances in their cybersecurity requirements, officials from state agencies may continue to experience cost, time, and other burdens resulting from these variances. Further, without documentation of the rationale for having requirements that are unique or parameters that

³⁶NIST 800-53, Rev. 4.

³⁷Centers for Medicare and Medicaid Services, *Acceptable Risk Standards*, Version 3.1 (November 2017).

conflict in comparison to other agencies, it will be more difficult for these agencies to achieve consistent requirements.

Selected Federal Agencies' Policies Addressed a Majority of Activities for Coordinating with State Agencies When Assessing Cybersecurity, but Did Not Address Coordinating with Each Other

As previously discussed, OMB Circular A-130 requires federal agencies to assess whether state agencies have implemented effective security and privacy controls on information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of federal information. The circular also encourages federal agencies to coordinate on their approaches to authorizing the use of such systems whenever practicable.

For example, the circular notes that multiple agencies are encouraged to jointly plan and execute tasks in NIST's Risk Management Framework, which includes conducting security assessments.³⁸ According to the circular, agencies can also leverage information generated by another agency based on the need to use the same information resources (e.g., information system or services provided by the system) by choosing to accept some or all of the information in an existing authorization package, including completed security assessments.³⁹

As previously stated, NIST and GAO have recommended practices that federal agencies can implement to help with their coordination on cybersecurity assessments, such as assessments of state agencies'

³⁸NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, Md.: December 2018). There are seven steps in the Risk Management Framework. One of these steps is to assess whether controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

³⁹According to OMB, agencies using leveraged authorization information from other (owning) agencies shall ensure that such information is included as part of their own Risk Management Framework to provide the appropriate context for managing risk within the leveraging organizations. The leveraging agency should consider risk factors, such as the time elapsed since the authorization results were produced; differences in environments of operation (if applicable); the impact of the information to be processed, stored, or transmitted; and the overall risk tolerance of the leveraging agency. The leveraging agency may determine that additional security measures are needed and negotiate with the owning agency to provide such measures.

compliance with federal cybersecurity requirements.⁴⁰ Those practices fall in two broad areas: (1) coordination with state agencies when assessing states' cybersecurity and (2) coordination with other federal agencies on the assessment of state agencies' cybersecurity.

In addition, based on the guidance from NIST that pertained to coordination on assessments of cybersecurity and practices recommended by GAO for enhancing coordination among federal agencies,⁴¹ four supporting activities are common to each of these two areas of federal agencies' coordination on cybersecurity assessments:

- assessment schedules and time frames;
- meeting and document requests;
- security test plans—including testing techniques,⁴² location, and tools; and
- the use of findings from prior assessments.

With regard to coordinating with state agencies when assessing their cybersecurity, two of the selected federal agencies—CMS and IRS—had policies that addressed all four of the activities supporting this area of coordination. The two other agencies—FBI's CJIS and SSA—had policies that addressed some, but not all, of the supporting activities for such coordination. With regard to coordinating with other federal agencies on the assessment of state agencies' cybersecurity, none of the four federal

⁴⁰GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP (Washington, D.C.: Apr. 14, 2015). NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (Gaithersburg, Md.: December 2014), and *Technical Guide to Information Security Testing and Assessment*, Special Publication 800-115 (Gaithersburg, Md.: September 2008).

⁴¹NIST Special Publication 800-53A, NIST Special Publication 800-115, and GAO-15-49SP.

⁴²According to NIST, dozens of security testing and examination techniques exist that organizations can use to assess the security posture of systems and networks. Commonly used techniques include review of documentation and other artifacts to passively examine systems, applications, networks, policies, and procedures to discover security vulnerabilities; target identification and analysis to identify potential vulnerabilities in active devices and their associated ports and services; and target vulnerability validation, such as penetration testing and social engineering to further explore the existence of potential vulnerabilities based on information produced from target identification and analysis.

agencies had policies that addressed the activities supporting this area of coordination.

Table 6 summarizes the extent to which selected agencies established policies for coordinating with state agencies and other federal agencies when assessing cybersecurity. See appendix II for details on the extent to which selected agencies addressed individual activities supporting the two areas of coordination.

Table 6: Extent to Which Selected Federal Agencies Established Policies for Coordinating When Assessing State Agencies' Cybersecurity

Policies	Agency	Rating
1. Policies for coordinating with state agencies.	CMS	●
	FBI's CJIS	◐
	IRS	●
	SSA	◐
2. Policies for coordinating with other federal agencies.	CMS	○
	FBI's CJIS	○
	IRS	○
	SSA	○

Legend: ● = Addressed all of the activities supporting coordination. ◐ = Addressed some, but not all, of the activities supporting coordination. ○ = Did not address any of the activities supporting coordination.

Source: GAO analysis of agency data. | GAO-20-123

Note: CMS = Centers for Medicare and Medicaid Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

Federal Agencies' Policies Addressed a Majority of Activities for Coordinating with State Agencies When Assessing Cybersecurity

Each of the selected federal agencies addressed at least three of the four activities for coordinating with state agencies when assessing cybersecurity. CMS and IRS fully established policies for coordinating with state agencies by addressing all of the activities supporting such coordination. However, FBI's CJIS and SSA partially established policies for coordinating with state agencies by addressing some—but not all—of the supporting activities. Specifically, FBI's CJIS and SSA fully addressed three of the activities: coordinating (1) assessment schedules and time frames, (2) meeting and document requests, and (3) security test plans. For example,

- FBI's CJIS policy included instructions for providing the date and time of assessment along with a schedule for the assessment process.

Further, the policy stated that assessors should lay out the meetings that need to occur and documentation that state agencies need to provide CJIS, including specifics about the state's network.

- SSA's policy laid out each step of the assessment process, including the anticipated time frames. Further, SSA's policy identified certain meetings that should be held during the process and documentation to be provided before the assessment.

However, FBI's CJIS and SSA did not fully establish policies for coordinating with state agencies because they did not address the activity associated with coordinating the use of findings from prior assessments. Specifically, while these two agencies' policies addressed using findings from prior assessments conducted by their individual agency, their policies did not address whether or how assessors should use findings from other security assessments conducted within the state.

Officials from FBI stated that in practice they consider findings from independent security assessments conducted within a state, but had not documented this practice in their assessment policies due to the limited instances in which this information is available. Officials from SSA believed that their policy addressed how its assessors were to consider findings from other security assessments that are conducted within a state. However, based on our review of SSA's policy, this information was not yet addressed.

Federal Agencies' Policies Did Not Address Activities for Coordinating with Other Federal Agencies When Assessing State Agencies' Cybersecurity

None of the four agencies established policies for coordinating with other federal agencies when assessing state agencies' cybersecurity. Officials from the four selected agencies reported that this is because their priority is to assess compliance with their own security requirements and they are not comfortable relying solely on other federal agencies' assessments.

Officials from each of the selected agencies provided additional perspectives on coordination with other federal agencies. Specifically:

- CMS officials stated that while they do not coordinate with other federal agencies in conducting compliance assessments, they did coordinate with other federal agencies when establishing their cybersecurity requirements. In addition, CMS officials stated that they do not conduct assessments of compliance with their security policy and that states engage contractors to perform the assessments. Therefore, CMS officials believed that the agency does not have a need to coordinate with other federal agencies. However, CMS did not include, where feasible, additional and detailed guidance to the state

that it could use to inform its assessment contractors about coordination with other federal agencies. CMS guidance to the states could encourage additional coordination with other federal agencies such as planning the assessment, leveraging related efforts by other federal agencies, and sharing the state's documentation and findings with other federal agencies, as appropriate. By not doing so, CMS is not maximizing coordination with other federal agencies to the greatest extent practicable.

- FBI's CJIS officials stated that they schedule their security assessments 6 months ahead of time, but would be willing to reschedule the assessment if the state was unavailable due to another assessment being conducted. In addition, CJIS officials noted that while they test for security controls that other federal agencies are testing, they are not assessing the same information as other agencies because the FBI specifically requires criminal justice data to be logically separated from other data. Further, CJIS officials stated their assessment results and audit findings cannot be shared and that other federal agencies would need to refer to a state's criminal justice agency for such information.
- IRS officials stated that they previously attempted to review assessment findings from other agencies, but since IRS was not looking at the same systems, the findings were not helpful. IRS officials stated that they would be willing to review recent assessments conducted by other federal agencies to see if information can be leveraged.
- SSA officials noted that it is their practice to reschedule an assessment if another federal agency has an assessment scheduled around the same time, but acknowledged that this was not in their policies. Further, according to SSA officials, they do not currently examine or consider findings from independent security assessments conducted within a state.

While agencies cited various reasons for not coordinating when assessing state agencies' cybersecurity, taking steps to coordinate, such as leveraging other agencies' assessments or conducting joint assessments whenever practicable, would be consistent with practices encouraged by OMB. However, OMB has not taken steps to ensure that they do so. OMB officials noted that they believed several of the agencies had begun to coordinate on their own and acknowledged that they could take additional steps to encourage and promote coordination among the agencies. OMB officials further noted that it is ultimately the responsibility of the agencies to determine how they conduct their assessments.

Nevertheless, federal agencies may be placing unnecessary burdens on state officials' time and resources in responding to similar requests and inquiries. Several state CISOs told us that they have identified various instances in which multiple federal agencies' lack of coordination resulted in requests for similar documentation and interviews with IT officials. For example, according to three state CISOs, the selected federal agencies have asked them to address similar questions regarding physical security controls, network configurations, and password policies in separate interviews. Three state CISOs also noted that they have provided to multiple federal agencies documentation—such as network diagrams and incident response policies—related to the same IT environment and have facilitated multiple federal assessments of the same physical environment.

State CISOs Identified Opportunities for Federal Agencies to Further Coordinate and Impacts Related to Federal Cybersecurity Assessments

State CISOs identified additional opportunities for further coordination among federal agencies and impacts in dealing with federal cybersecurity assessments. For instance, in response to our survey, 16 states' officials commented that the four federal agencies in our review could leverage additional opportunities to coordinate on their assessments within their states, particularly where the states had a consolidated data center or other centrally managed IT infrastructure. Further, four state CISOs noted that federal agencies could potentially leverage security compliance assessments and internal audits performed at the state or local level because they included reviews of controls from NIST Special Publication 800-53.

In addition, 11 states mentioned “duplication” in their response to a survey question about challenges or impacts related to federal cybersecurity requirements and assessment processes, while two states mentioned “overlap,” and one state mentioned “fragmentation.”⁴³ For example:

⁴³Our definition of “fragmentation” refers to circumstances in which more than one federal agency (or more than one organization within an agency) is involved in the same broad area of national need and there may be opportunities to improve how the government delivers these services. The term “overlap” refers to when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. The term “duplication” refers to when two or more agencies or programs are engaged in the same activities or provide the same services to the same beneficiaries. See [GAO-15-49SP](#). State CISOs were not provided these definitions and therefore may have been thinking about these concepts differently than we do.

-
- One state identified that assessors from different federal agencies generally ask for the same items from the state, requiring state agency officials to reproduce the same response.
 - Another state identified that multiple federal agencies have been assessing the same state agencies with different scope, tools, and documentation requests.
 - In another example, a state concluded that federal assessors' interpretation of many technical controls was inconsistent and varied from one federal agency to another and across audit cycles. The state noted that there were opportunities for the federal government to streamline how each agency applied different interpretations.

State CISOs also identified impacts on their time and costs from responding to federal agencies' assessments. Seventeen respondents reported impacts to their time and six reported cost impacts.

Further, in responding to questions in our survey and an in-depth interview, state CISOs provided additional insights regarding impacts. For example:

- One state mentioned that, due to the varying requirements from the selected federal agencies, the state is required to stand up multiple virtual and physical environments. In doing so, the state is required to purchase additional software and hardware to maintain such environments.
- Another state explained that staff manage various state agencies' data in one central location and spend a considerable amount of time responding to each of the four selected federal agencies' assessments.
- Twenty-four states estimated that the four selected federal agencies conducted at least 188 assessments between calendar years 2016 and 2018 and that the states' best estimates of the total expenditures

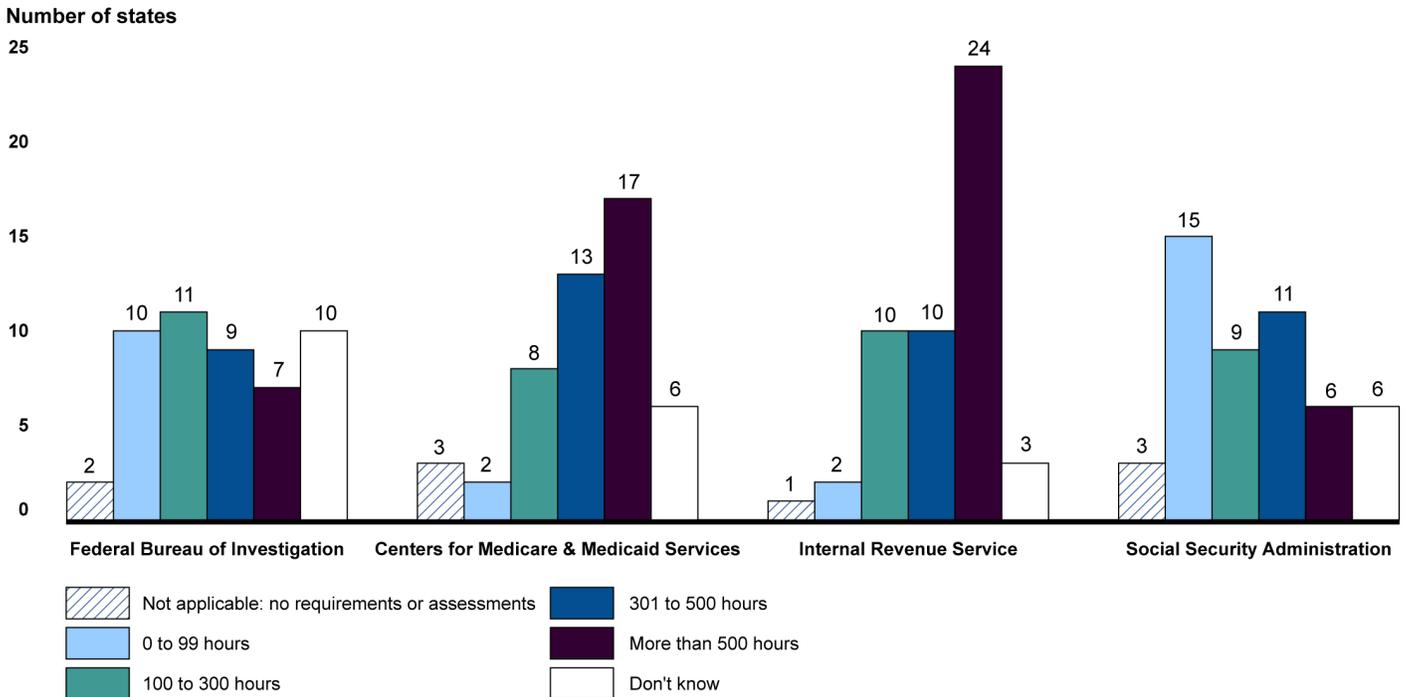
associated with those assessments ranged from \$43.8 million to \$67 million.⁴⁴

- Of 164 instances where states reported an average time spent on assessments by one of the four selected agencies between calendar years 2016 and 2018, in 97 instances the average time expenditure per assessment was reported to be 301 staff hours or more, and in 67 instances it was less than 301 staff hours. Additionally, there were 34 instances in which the state did not know what its average staff hour expenditure was for a particular agency's assessment or said that it was not applicable to the state.

Figure 3 represents the responses from 50 state CISOs on the average state staff hours expended per assessment from across the four selected federal agencies as reported by state CISOs.

⁴⁴We asked state CISOs to consider up to the last three assessments each of the four federal agencies performed between 2016 and 2018 and to provide their best estimate of the range of cost in dollars (including staff hour labor, travel, materials, and contract costs) the states expended per assessment, on average, to comply. Specifically, we asked state CISOs to provide a lower end and upper end estimate of dollar cost per assessment. We also asked states to provide a lower end and upper end estimate of the number of assessments each federal agency performed during the same period. For the 24 state CISOs that provided a range of estimates of dollar costs per assessment, we multiplied their lower end and upper end estimate of dollar cost for each federal agency by the lower end estimate of the number of assessments performed by the same federal agency. We chose the lower end estimate of the number of assessments in order to calculate a conservative estimate of the range of costs. We then calculated the sum total of states' lower end estimated costs and the sum total of states' upper end of estimated costs to identify an aggregate range of total expenditures made by the 24 states.

Figure 3: Average State Staff Hours Expended Per Assessment across Selected Federal Agencies



Source: GAO analysis of 2019 survey of chief information security officers. | GAO-20-123

Note: While chief information security officers from 50 states responded to this question, one state that responded did not provide information regarding average staff hours associated with assessments for the Federal Bureau of Investigation and the Centers for Medicare and Medicaid Services.

While state agencies could benefit from additional coordination among federal agencies in conducting their security assessments, increasing coordination may also save the federal government money. For instance, federal agencies may be able to reduce the number of assessments or the scope of the assessment conducted by each agency, the amount of time multiple federal agencies must spend reviewing state systems, and contractor services acquired to assist in performing assessments. The selected federal agencies reported spending close to \$45 million in fiscal years 2016 through 2018 on assessments of state agencies' cybersecurity. Figure 4, an interactive figure, provides the selected federal agencies' reported spending for fiscal years 2016 through 2018 for assessing state compliance with cybersecurity requirements. (See appendix III for the cost breakdown of selected federal agencies' reported spending).

Figure 4: Selected Federal Agencies' Fiscal Years 2016-2018 Reported Spending for Assessing State Compliance with Cybersecurity Requirements

^aCMS's expenditures for contractors are based on a project contract from July 2015 through July 2018. CMS uses contractors to review final assessments submitted by a state. State agencies bear the cost of using contractors to perform security assessments against the CMS requirements.

Until FBI's CJIS and SSA fully develop policies for coordinating with state agencies and all of the selected agencies develop policies for coordinating with other federal agencies when assessing state agencies' cybersecurity, as appropriate, they run the risk of spending more than necessary to assess the security of state systems and networks. Further, federal agencies may be placing unnecessary burdens on state officials' time and resources in responding to overlapping or duplicative requests and inquiries, retesting controls that have already been evaluated, or reporting similar findings multiple times throughout a state. In addition, until OMB takes steps to ensure agencies coordinate on assessments of state agencies' cybersecurity, it will not have reasonable assurance federal agencies are leveraging compatible assessments where practicable.

Conclusions

Given that the federal government exchanges personally identifiable and other sensitive information with state agencies, it is critical to have effective coordination across the federal and state agencies to protect this information. While the selected federal agencies have taken steps to secure information exchanged between federal and state agencies, they have not coordinated with each other in establishing cybersecurity requirements for state agencies. The selected agencies' insufficient coordination has contributed to variances in the agencies' control selection, terminology, and technical parameters across hundreds of cybersecurity requirements imposed on states. Further, OMB requires agencies to coordinate to ensure consistency among cybersecurity requirements for state entities, but it has not ensured that agencies have done so.

While federal agencies may have legitimate reasons for having variances in their cybersecurity requirements, states' compliance with multiple federal agencies' cybersecurity requirements has resulted in increased costs. Coordinating to address variances in federal agencies' cybersecurity requirements could help to significantly reduce these costs. The selected agencies will soon have an opportunity to coordinate on any planned updates of their security policies that affect state agencies when reviewing their security policies against expected revisions in NIST guidance. Accordingly, it is important that OMB ensures that selected federal agencies coordinate with state agencies and each other to establish cybersecurity requirements that are consistent to the greatest extent possible.

Selected federal agencies had partially established policies to coordinate with state agencies when assessing their cybersecurity, but did not have

policies for coordinating with other federal agencies. Federal agencies have not been coordinating with each other on assessments of state agencies' cybersecurity, in part, because this has not been a priority for them. Further, federal agencies have been less likely to coordinate in their assessments of state agencies' cybersecurity without additional involvement from OMB. The lack of coordination among federal agencies has been a concern among state CISOs who described instances of duplication and overlap in their cybersecurity assessments. As with the cybersecurity requirements, coordinating with both state and federal agencies when assessing state agencies' cybersecurity may help to minimize additional cost and time impacts on state agencies, and reduce federal resources associated with implementing state-based cybersecurity assessments. Until OMB takes steps to ensure federal agencies coordinate on assessments of state agencies' cybersecurity, it will not have reasonable assurance federal agencies are leveraging compatible assessments to the greatest extent possible.

Recommendations for Executive Action

We are making a total of 12 recommendations, including two to OMB, two to CMS, three to FBI, two to IRS, and three to SSA.

- The Director of OMB should ensure that CMS, FBI, IRS, and SSA are collaborating on their cybersecurity requirements pertaining to state agencies to the greatest extent possible and direct further coordination where needed. (Recommendation 1)
- The Director of OMB should take steps to ensure that CMS, FBI, IRS, and SSA coordinate, where feasible, on assessments of state agencies' cybersecurity, which may include steps such as leveraging other agencies' security assessments or conducting assessments jointly. (Recommendation 2)
- The Administrator of CMS should, in collaboration with OMB, solicit input from FBI, IRS, SSA, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible and document CMS's rationale for maintaining any requirements variances. (Recommendation 3)
- The Administrator of CMS should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. (Recommendation 4)
- The FBI Director should, in collaboration with OMB, solicit input from CMS, IRS, SSA, and state agency stakeholders on revisions to its

security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible. (Recommendation 5)

- The FBI Director should fully develop policies for coordinating with state agencies on the use of prior findings from relevant cybersecurity assessments conducted by other organizations. (Recommendation 6)
- The FBI Director should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. (Recommendation 7)
- The IRS Commissioner should, in collaboration with OMB, solicit input from CMS, FBI, SSA, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible. (Recommendation 8)
- The IRS Commissioner should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. (Recommendation 9)
- The Commissioner of SSA should, in collaboration with OMB, solicit input from CMS, FBI, IRS, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible and document the SSA's rationale for maintaining any requirements variances. (Recommendation 10)
- The Commissioner of SSA should fully develop policies for coordinating with state agencies on the use of prior findings from relevant cybersecurity assessments conducted by other organizations. (Recommendation 11)
- The Commissioner of SSA should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. (Recommendation 12)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB and the four other selected federal agencies for their review and comment. In response, three of the agencies (Department of Health and Human Services, FBI, and SSA) stated that they agreed with the recommendations; and one agency (IRS) stated that it partially agreed with one recommendation and disagreed with one recommendation. OMB did not provide comments on our report.

The following three agencies agreed with the recommendations.

- The Department of Health and Human Services provided written comments, in which it agreed with our recommendations and identified steps it said CMS had taken or intends to take to address them. For example, the department stated that CMS intends to solicit input from the other federal agencies identified in this report and from state agency stakeholders when making updates to its MARS-E security policy and when updating its assessment guidance to states on how to maximize coordination with other federal entities.

The department noted that CMS had developed and implemented its suite of guidance and requirements, known as MARS-E, based on the Patient Protection and Affordable Care Act, FISMA, and NIST. According to the department, variances in security requirements are to be expected because of the flexibility that NIST allows in its guidance. The department added that CMS tailored some of the controls to allow flexibilities for states while keeping the overall intent of the NIST guidance.

The department stated that it collaborated with federal agencies, including FBI's CJIS, in developing MARS-E and during subsequent updates of that security policy. However, CMS did not provide us with documentation as evidence of its collaboration with FBI's CJIS on the development of MARS-E. In addition, as noted in this report, CMS had not collaborated with the other agencies included in our review after the development of the most recent version of MARS-E. It is important that federal agencies collaborate to address variances in their cybersecurity requirements; doing so could help to significantly reduce state agencies' costs in complying with multiple federal agencies' requirements.

The department's comments are reprinted in appendix IV. The department also provided technical comments, which we incorporated as appropriate.

- In written comments, FBI's CJIS agreed with our three recommendations to the agency. Among other things, the agency stated that it would, to the greatest extent possible, collaborate with OMB and solicit input from the other federal agencies identified in this

report, as well as from state agency stakeholders, on revisions to its security policy.

With regard to our recommendation that FBI's CJIS develop policies for coordinating with state agencies on the use of prior findings, the agency stated that it had implemented this recommendation and updated its security policy to include coordinating with state agencies on the use of prior findings from relevant cybersecurity assessments conducted by other organizations. However, the agency did not provide documentation showing that it had updated the security policy. As a result, we did not change our assessment of this practice. We will continue to monitor the agency's progress in implementing the recommendation.

The agency's comments are reprinted in appendix V. The agency also provided technical comments, which we incorporated as appropriate.

- In its written comments, SSA stated that it agreed with our recommendations. SSA's comments are reprinted in appendix VI. The agency also provided technical comments, which we incorporated as appropriate.

One agency partially agreed with one recommendation and disagreed with one recommendation. Specifically, IRS partially agreed with our recommendation to, in collaboration with OMB, solicit input from the four federal agencies identified in this report and state agency stakeholders on revisions to its security policy. Specifically, the agency agreed to participate in collaborative working sessions with OMB and interested stakeholders to discuss the impact of inconsistent standards and the extent to which the standards might be harmonized. However, IRS stated that it must follow Treasury Directives and internal standards for systems that process tax data and, as a result, its ability to harmonize requirements may be limited.

As noted in this report, federal agencies may have legitimate reasons for variances in their cybersecurity requirements, such as applying different information security controls and more stringent technical parameters to protect data for which the agencies are responsible in a manner consistent with various security requirements originating in federal laws, directives, and regulations. Nevertheless, we continue to believe that it is important for all of the agencies in our review to identify opportunities where requirements can be streamlined or made more consistent while still achieving each agency's desired security outcomes because doing so may reduce potential burdens on state agencies, as discussed in this report. Thus, we maintain that our recommendation is still warranted.

IRS disagreed with our recommendation to revise its assessment policies to maximize coordination with other federal agencies to the greatest extent possible. Specifically, IRS stated that it has sole statutory oversight authority and enforces requirements for agencies subject to Internal Revenue Code § 6103. As such, IRS cannot solely rely on an assessment conducted by another agency. However, as noted in this report, OMB encourages federal agencies to coordinate on their assessments whenever practicable.⁴⁵ Doing so would not necessarily require IRS to solely rely on another agency's assessment nor conflict with its authority to conduct statutory oversight because IRS could leverage and share relevant information and artifacts with other federal agencies while continuing to conduct its own required assessments and oversight.

Further, as discussed in this report, state chief information officers identified a number of areas where federal agencies requested similar information through documentation requests and interviews, such as network configurations, password policies, and incident response policies. Leveraging and sharing relevant information that is collected by federal agencies could help those agencies, including IRS, reduce some of their data collection needs while also helping to minimize burdens on state officials' time and resources. We acknowledge that complete alignment of assessment policies may not be feasible in light of unique statutory responsibilities and requirements; however, agency coordination and simplification of certain assessment logistics may be possible and could result in gained efficiencies from the perspective of the federal government. Thus, we maintain that our recommendation is still warranted.

IRS's comments are reprinted in appendix VII.

We are sending copies of this report to the appropriate congressional requesters, the Director of OMB, the Administrator of CMS, the Assistant Attorney General for Administration for the Department of Justice, the FBI Director, the IRS Commissioner, and the Commissioner of SSA. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

⁴⁵OMB, Circular A-130, Managing Information as a Strategic Resource (July 2016).

If you or your staff have any questions about this report, please contact me at (202) 512-6240 or at dsouzav@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 VIII.



Vijay A. D'Souza
Director,
Information Technology and Cybersecurity

Appendix I: Methodology and Results of GAO's Survey of State Officials' Views

We administered a survey to the offices of the Chief Information Officer and Chief Information Security Officer (CISO) in the 50 states, District of Columbia, American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands.¹ To administer the survey, we emailed each state a fillable PDF questionnaire. We fielded the survey from February 19, 2019, through April 24, 2019. We received usable survey responses from 50 of the 55 states and territories, for a response rate of 91 percent.

In developing, administering, and analyzing the survey, we took steps to minimize the five types of errors that may affect survey results—population coverage, sampling, measurement, nonresponse, and data processing. Our results are not subject to either of the first two types of errors—population coverage (under- or over-coverage) error of the study population or sampling error—because we defined all states and five territories as our study population, and sent each a questionnaire.

To minimize the third type of error (measurement error), we pretested the questionnaire with CISOs (or their delegates) in four states that varied over two characteristics related to our questions: whether or not the state took a “federated” or “consolidated” management approach to data center and other information technology (IT) infrastructure, and the relative size of the state’s IT budget. Using cognitive interviewing techniques, such as nondirective probing of answers and asking respondents to think aloud when formulating answers, we determined whether (1) the questions were clear and unambiguous, (2) terminology was used correctly, (3) the questionnaire did not place an undue burden on state officials, (4) the information could feasibly be obtained, and (5) the survey was comprehensive and unbiased. Based on the pretests and interviews with external subject matter experts on questionnaire subjects, we modified the questionnaire.² During the survey, we also followed up by email or phone with some respondents to clarify unclear answers and edit them if necessary. Additionally, after the survey, our in-depth interviews with four responding states confirmed their answers to selected questions, or resulted in edits to those answers.

¹State CISO’s may have obtained input for the survey from other officials in relevant state agencies.

²We interviewed staff from the National Association of State Chief Information Officers to gain insight into (1) states that manage agency data in a consolidated versus deconsolidated environment and (2) states’ annual IT budget expenditures.

To minimize the potential for the fourth type of error (nonresponse error), we emailed or called states that did not respond to the initial notice multiple times to encourage survey participation or provide technical assistance, as appropriate. Also, the follow up contacts made to clarify answers resulted in obtaining some answers to questions that had been left blank in returned questionnaires. While the four states and one territory not returning questionnaires may have differed to an unknown extent in what their answers would have been, compared to the aggregate answers of those who did respond, the overall impact on our results from only five missing members of the population is unlikely to be material. To minimize the possibility for the fifth type of error (data processing error), all data entry, edits, and analysis were verified by a second, independent analyst on the engagement team.

To further understand the states' experiences with and views of selected federal agencies' cybersecurity assessments, we conducted in-depth interviews with four states. In selecting the four states for in-depth interviews, we considered responses from 44 states that had submitted surveys prior to April 11, 2019. From these states, we analyzed responses to survey questions 4, 7, 9, 10, 11, 12, 13, 14, 15, 16, and 17, and identified whether states' responses reflected a generally favorable opinion or a generally unfavorable opinion of federal cybersecurity requirements and assessments. Based on this information, we selected two states to interview that had a generally favorable opinion and two states that had a generally unfavorable opinion toward federal cybersecurity assessments and requirements. In selecting states to interview from states that had favorable and unfavorable opinions, we chose to interview states that provided different responses about increases in costs and/or coordination with federal and nonfederal agencies.

We sent an email to each of the four states to ask for their participation and conducted follow up interviews with officials from the offices of the state CIO and state CISO, state audit entities, and mission agencies from four states. Our interview questions concerned topics such as challenges states may have faced in complying with federal cybersecurity requirements, the impacts federal requirements and assessments may have had on states, the efficiency and effectiveness of assessments performed by each federal agency, and the nature and extent of any duplication in federal agencies' cybersecurity requirements. Although the results of these in-depth interviews are not generalizable to all of the states and territories that responded to our survey, they provide richer insight into some of the information we collected through our survey, such

as the reasons for certain questionnaire responses or the sources of variation in states' perspectives.

The following identifies the survey questionnaire that we administered and the aggregated results from the responses are below under each question. Not all state CISOs who completed the survey responded to all questions, and some questions were not discussed in the body of our report.

Federal Requirements

These questions ask about the federal agency cybersecurity requirements that set standards in any of the related general security control categories, and your experiences with those applicable to your state.

1. For how long has the current CISO of your state been in that role? (check one box)

	States
Less than 1 year	16
1 to up to 2 years	14
2 to up to 5 years	13
5 to up to 10 years	4
10 years or more	2

2. Please provide some background on your state's governance model for cybersecurity. Specifically, how is the responsibility for managing the following aspects of cybersecurity primarily assigned within your state? (check the one box in each row which best represents your answer)

	Statewide	Individual agencies	Don't know
Budget and/or funding	24	25	1
Developing policies and regulations	40	10	0
Enforcing policies and regulations	31	19	0
Data management	12	38	0
Infrastructure management	36	14	0
Application management	12	38	0

**Appendix I: Methodology and Results of
GAO's Survey of State Officials' Views**

3. Is your state currently required to meet any security requirements by any of the following federal agencies in order to obtain and use federal data?

	Yes	No	Don't know
Federal Bureau of Investigation (FBI) (Criminal Justice Information Services (CJIS) Security Policy CJISD-ITS-DOC-08140-5.7, Version 5.7)	49	1	0
Centers for Medicare & Medicaid Services (CMS) (Minimum Acceptable Risk Standards for Exchanges, Version 2.0)	49	1	0
Internal Revenue Service (IRS) (IRS Publication 1075, Tax Information Security Guidelines For Federal, State, and Local Agencies, September 2016)	50	0	0
Social Security Administration (SSA) (Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information, Version 8.0)	49	1	0
Any other federal agency(s) and its requirements	31	2	6

4. Federal security requirements applicable to states may vary in a number of ways. Considering as a whole all of the federal agencies' requirements that your state is currently required to meet, how much do you think they vary from each other in each of the following ways?

	Very great variation	Great variation	Moderate variation	Slight variation	No variation	Don't know
The specific controls selected by agencies for states to implement	5	13	16	13	1	2
How agencies' requirement language matches NIST 800-53 control language	2	10	17	14	5	2
The technical parameters or thresholds of controls specified by agencies	3	17	18	9	0	3
Other types of variation in agency requirements	6	6	2	3	1	12

5. Consider again all the applicable federal cybersecurity requirements required of your state. Do one or more federal agencies have any requirements that most vary from other agencies?

Within each of the following families of security controls, check all boxes that apply to tell us in what ways requirements vary, and which agency(s) vary the most from others.

(If "Other(s)" varying agencies selected, list in Question 6.)

NIST Control Family	Controls Selected	Matching NIST Control Language	Parameters or Thresholds	Other Variation
Access Control (AC)	33	33	36	7
Awareness and Training (AT)	29	25	33	7
Audit and Accountability (AU)	30	29	37	8
Security Assessment and Authorization (CA)	28	29	29	8
Configuration and Management (CM)	30	29	31	8
Contingency Planning (CP)	26	29	30	6
Identification and Authentication (IA)	29	28	31	7
Incident Response (IR)	25	27	34	8
Media Protection (MP)	24	26	28	3
Physical and Environmental Protection (PE)	30	26	35	5
Planning (PL)	24	25	26	6
Personnel Security (PS)	27	29	36	7
Risk Assessment (RA)	26	29	29	7
System and Services Acquisition (SA)	28	28	31	7
System and Communications Protection (SC)	28	29	29	6
System and Information Integrity (SI)	28	27	28	7
Program management (PM)	26	24	24	4

6. If you indicated above that any other federal agencies have requirements that most vary from others, what are those other agencies and the control categories and way(s) they vary?

(Narrative answers not displayed)

**Appendix I: Methodology and Results of
GAO's Survey of State Officials' Views**

7. If you identified any variation in the requirements of multiple Federal agencies in question 5 above, what is your overall estimation of the degree of that variation in each of the following families of controls?

Families of controls (Based on NIST 800-53)	Very great variation	Great variation	Moderate variation	Slight variation	Not applicable: no variation	Don't know
Access control (AC)	6	9	15	11	0	4
Awareness and training (AT)	2	8	19	9	3	4
Audit and accountability (AU)	4	12	17	9	0	4
Security assessment and authorization (CA)	7	10	15	5	4	4
Configuration management (CM)	5	11	14	8	2	5
Contingency planning (CP)	4	5	18	5	6	5
Identification and authentication (IA)	4	9	16	10	1	4
Incident response (IR)	4	8	19	7	2	4
Maintenance (MA)	4	4	18	4	8	5
Media protection (MP)	4	6	15	10	5	4
Physical and environmental protection (PE)	5	7	18	7	3	5
Planning (PL)	3	5	16	10	5	5
Personnel security (PS)	6	12	17	5	1	4
Risk assessment (RA)	5	5	20	7	4	4
System and services acquisition (SA)	6	5	17	7	3	5
System and communications protection (SC)	4	11	18	4	3	4
System and information integrity (SI)	5	7	17	5	5	4
Program management (PM)	5	7	11	8	7	5
Any other security area(s) with conflicts	3	0	1	0	1	2

8. Do you have any comments on or explanations of your answers to the question above that would help us appropriately interpret those answers? (itemize your comments by the row letters above, to the extent possible, in the box below)

(Narrative answers not displayed)

9. Has your state taken any of the following actions specifically to address variation(s) across agency requirements?

Check here if no variation and skip to Question 11

	Yes	No	Don't know
Increased coordination with federal agencies	24	18	3
Increased coordination with NASCIO and other non-federal agencies outside your state	37	6	1
Increased coordination with other agencies within your state	40	5	1
Any other action(s)	14	0	4

10. Have the variations increased any of the following types of costs and/or challenges?

Costs and challenges	Very great increase	Great increase	Moderate increase	Slight increase	No increase	Don't know
Calendar time to meet requirements	10	15	11	4	2	4
Staff hours for meeting requirements	12	15	10	3	2	4
Costs of acquiring additional materials, software, and equipment	8	14	12	3	4	5
Costs of additional contractor services	9	10	11	4	7	5
Other costs of meeting requirements	6	9	11	4	5	11
Challenges to meeting state missions	7	12	14	5	3	5
Challenges to IT reform efforts	12	11	7	2	6	6
Any others	4	1	0	0	1	3

Federal Assessments

The following questions ask about assessments performed by federal agencies on your state on its compliance with the federal cybersecurity requirements covered above.

For the purposes of this survey, an "assessment" includes only the activities in the period between the date the state is notified of the assessment and the date the federal agency or entity carrying out the assessment (e.g., contractor) completes its on-site work.

Appendix I: Methodology and Results of
GAO's Survey of State Officials' Views

11. Approximately how many assessments did each of the following federal agencies perform on your state's efforts to comply with its requirements in calendar years 2016-2018? (When counting assessments performed by one federal agency on more than one state mission agency or operational entity at the same time, please count each assessment individually.)

	Not applicable: no requirements	0	1-2	3-4	5 or more	Don't know
FBI	1	1	24	4	12	7
CMS	1	3	21	13	4	7
IRS	0	1	20	16	12	1
SSA	1	1	22	14	8	4
Any other federal agency(s)	0	2	8	1	0	3

12. Considering up to the last 3 assessments a federal agency performed in 2016-2018, approximately how long in calendar time was taken per assessment, on average, to perform?

	Not applicable: no requirements or assessments	Less than 1 month	1 to 2 months	3 to 5 months	6 months or more	Don't know
FBI	2	19	12	6	1	9
CMS	3	5	19	8	7	7
IRS	1	12	13	16	5	3
SSA	3	18	16	6	1	6
Any other federal agency(s)	1	4	2	2	0	3

13. Considering up to the last 3 assessments a federal agency performed in 2016-2018, approximately how many of your state's staff hours were expended per assessment, on average, to comply?

	Not applicable: no requirements or assessments	0 to 99 hours	100 to 300 hours	301 to 500 hours	More than 500 hours	Don't know
FBI	2	10	11	9	7	10
CMS	3	2	8	13	17	6
IRS	1	2	10	10	24	3
SSA	3	15	9	11	6	6
Any other federal agency(s)	1	3	4	3	0	4

14. And considering up to the last 3 assessments a federal agency performed in 2016-2018, what is your best estimate of the range of cost in dollars (including staff hour labor, travel, materials, and contract costs) your state expended per assessment, on average, to comply?

	Not applicable: no requirements or assessments	Estimated lower end of dollar cost (mean value)	Estimated upper end of dollar cost (mean value)	Don't know
FBI	3	\$77,103 (17 responses)	\$155,059 (17 responses)	28
CMS	3	\$623,650 19 responses)	\$840,472 (19 responses)	24
IRS	2	\$211,574 (21 responses)	\$418,238 (21 responses)	25
SSA	4	\$33,822 (16 responses)	\$61,719 (16 responses)	28

**Appendix I: Methodology and Results of
GAO's Survey of State Officials' Views**

15. Considering all the federal assessments performed on your state's implementation of requirements in 2016-2018, how would you rate those assessments, overall, on the following factors?

	Excellent	Very good	Good	Fair	Poor	Don't know
Timeliness – the speed of completing on-site assessment work and issuing reports	2	8	23	11	2	3
Relevance – to federal agencies' efforts for ensuring compliance with IT security objectives	2	12	19	13	0	4
Usefulness – to federal agencies' abilities for ensuring compliance with IT security objectives	1	11	20	9	4	4
Any other factors	0	1	0	1	7	5

16. In summary, how would you rate the efficiency of assessments performed by each federal agency on your state's implementation of requirements?

	Extremely efficient	Very efficient	Moderately efficient	Slightly efficient	Not at all efficient	Don't know
CMS	0	11	14	7	4	12
FBI	1	13	13	7	1	13
IRS	0	10	24	6	5	5
SSA	2	14	18	6	2	7
Any other agency(s)	0	3	2	1	0	6

17. In summary, how would you rate the effectiveness of assessments performed by federal agencies on your state's implementation of requirements?

	Extremely effective	Very effective	Moderately effective	Slightly effective	Not at all effective	Don't know
CMS	1	11	17	5	2	11
FBI	1	8	18	8	1	12
IRS	1	13	21	5	4	5
SSA	1	11	19	8	3	7
Any other agency(s)	0	1	4	1	0	3

18. Considering the issues covered in this questionnaire, what challenges or impacts, if any, has your state experienced regarding the federal requirements and assessment processes? (list and describe up to 5)
(Narrative answers not displayed)

Additional Information

19. Do you have any additional explanations of your answers or comments on any of the issues in this questionnaire?
(Narrative answers not displayed)

20. Who is the person primarily responsible for completing this questionnaire whom we can contact in case we need to clarify a response? If the state CISO did not complete this questionnaire, we recommend that the CISO review these answers.

Name: _____

Title _____

Office: _____

Phone: _____

Email: _____

Appendix II: Detailed Assessment of Selected Federal Agencies' Policies

The tables below identify the extent to which each of the four selected federal agencies established policies that addressed individual activities supporting two areas of coordination: (1) coordination with state agencies when assessing states' cybersecurity and (2) coordination with other federal agencies on the assessment of state agencies' cybersecurity.

Table 7: Detailed Assessment of the Centers for Medicare and Medicaid Services's (CMS) Policies for Coordinating when Assessing State Agencies' Cybersecurity

Policies	Supporting activities	Rating	Description
1. Policies for coordinating with state agencies.	Assessment schedules and time frames	●	CMS's security assessment guidance addressed coordinating with state agencies on schedules and time frames by providing a detailed time frame on when the required Minimum Acceptable Risk Standards for Exchanges documentation, such as an annual controls attestation and authority to connect package, are due to CMS.
	Meeting and document requests	●	CMS's Framework for Independent Assessment of Security and Privacy Controls stated that state agencies are responsible for and have control over scheduling meetings and the completion of deliverables. In addition, the Minimum Acceptable Risk Standards for Exchanges Timeline and Artifacts document detailed how state agencies should coordinate with CMS in submitting required artifacts.
	Security test plans including testing techniques, location, and tools	●	CMS's security policy provided a template for the security test plan, which included steps for selecting testing techniques such as observation of system users, identifying the testing location, and identifying testing tools to be used in the assessment such as system scanning tools.
	Use of prior findings	●	CMS's Framework for Independent Assessment of Security and Privacy Controls communicated that state agencies can reuse information from prior assessments to meet CMS's requirements as long as the assessment was independent and the scope covered all or a portion of the Minimum Acceptable Risk Standards for Exchanges controls. In addition, this framework directed assessors to coordinate with the state agencies to determine if any internal state audits had been conducted and use the results as appropriate.
2. Policies for coordinating with other federal agencies.	Assessment schedules and time frames	○	CMS did not establish policies that facilitate coordination with other federal agencies regarding assessment schedules and time frames.
	Meeting and document requests	○	CMS did not establish policies to coordinate with other federal agencies in scheduling meeting and document requests.
	Security test plans including testing techniques, location, and tools	○	CMS did not establish policies to coordinate with other federal agencies on security test plans.
	Use of prior findings	○	CMS did not establish policies with respect to how assessors are to consider prior findings from other federal assessments when assessing state agencies' cybersecurity.

Appendix II: Detailed Assessment of Selected Federal Agencies' Policies

Legend: ● = Established policies that addressed all aspects of this activity. ◐ = Established policies that addressed some, but not all, aspects of this activity. ○ = Did not establish policies that addressed any aspects of this activity.

Source: GAO analysis of agency data. | GAO-20-123

Table 8: Detailed Assessment of the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services's (CJIS) Policies for Coordinating when Assessing State Agencies' Cybersecurity

Policies	Supporting activities	Rating	Description
1. Policies for coordinating with state agencies.	Assessment schedules and time frames	●	CJIS established an agency contact sheet that provided the date and time of audit, along with a schedule of the assessment process and a time frame for how the assessment is expected to be carried out. In addition, CJIS's email contact template laid out the time and date of the assessment and the completion date for pre-assessment questionnaire.
	Meeting and document requests	●	CJIS's pre-audit questionnaire discussed documentation that states need to provide for the audit and specific information about the network infrastructure. In addition, the email contact template provided a time frame for returning required documents and for when the assessment would occur. In addition, the audit task list provides a checklist of tasks CJIS must complete during the audit, including meetings with the state.
	Security test plans including testing techniques, location, and tools	●	The CJIS questionnaire for the assessment listed specific tests to be performed at state agencies such as validation testing on access points and password testing. In addition, the Audit Program Methodology stated that an onsite network inspection is conducted to assess, evaluate, and verify physical and technical security. Testing tools were not applicable to CJIS's assessment because, according to CJIS officials, the agency does not perform scanning or testing of state systems.
	Use of prior findings	◐	CJIS partially established policies and procedures for coordinating with state agencies on the use of prior findings. Specifically, the audit task list calls for CJIS to review previous results from its past assessments when planning the assessment. However, CJIS's policy did not address whether or how assessors should use prior findings from other security assessments conducted within the state.
2. Policies for coordinating with other federal agencies.	Assessment schedules and time frames	○	CJIS did not establish policies that facilitate coordination with other federal agencies regarding assessment schedules and time frames.
	Meeting and document requests	○	CJIS did not establish policies to coordinate with other federal agencies in scheduling meeting and document requests.
	Security test plans including testing techniques, location, and tools	○	CJIS did not establish policies on coordinating with other federal agencies on security test plans.

**Appendix II: Detailed Assessment of Selected
Federal Agencies' Policies**

Policies	Supporting activities	Rating	Description
	Use of prior findings	○	CJIS did not establish policies with respect to how assessors are to consider prior findings from other federal assessments when assessing state agencies' cybersecurity.

Legend: ● = Established policies that addressed all aspects of this activity. ◐ = Established policies that addressed some, but not all, aspects of this activity. ○ = Did not establish policies that addressed any aspects of this activity.

Source: GAO analysis of agency data. | GAO-20-123

Table 9: Detailed Assessment of the Internal Revenue Service's (IRS) Policies for Coordinating when Assessing State Agencies' Cybersecurity

Policies	Supporting activities	Rating	Description
1. Policies for coordinating with state agencies.	Assessment schedules and time frames	●	IRS Publication 1075 and the agency's assessment policy provided an overview of the time frame for when assessment teams are expected to coordinate with state agencies on scheduling meetings. Additionally, IRS's assessment training directed the assessors to create schedules in coordination with the state agency prior to the assessment.
	Meeting and document requests	●	IRS's assessment policy provided a detailed outline of the agency's coordination with state agencies on meeting and document requests, including when these should be sent and their respective time frames. Additionally, the IRS's assessment training provided further details on coordinating with state agencies on the types of documents that should be delivered to the IRS.
	Security test plans including testing techniques, location, and tools	●	IRS established policies for coordinating with state agencies for security test plans, including testing techniques, location, and tools. Specifically, the agency's security assessment matrix identifies the tests assessors are to run on state systems to determine if they are in compliance. In addition, the assessment matrix describes the test plan and the expected results of the test. As part of the assessment process, a preparation email is to be included to coordinate with states on the location of the test. Further, IRS is to coordinate with states via memorandums that outline the testing tools and techniques it will be using to conduct the assessment.
	Use of prior findings	●	IRS's assessment policy included a provision that assessors should examine previous assessments as part of the background gathering process. Additionally, IRS's Safeguard Review Preparation procedures directed assessors to coordinate with the state agencies to determine internal state audits that had been conducted and use the results as appropriate.
	Assessment schedules and time frames	○	IRS did not establish policies that facilitate coordination with other federal agencies regarding assessment schedules and time frames.

Appendix II: Detailed Assessment of Selected Federal Agencies' Policies

Policies	Supporting activities	Rating	Description
2. Policies for coordinating with other federal agencies.	Meeting and document requests	○	IRS did not establish policies to coordinate with other federal agencies in scheduling meeting and document requests.
	Security test plans including testing techniques, location, and tools	○	IRS did not establish policies to coordinate with other federal agencies on security test plans.
	Use of prior findings	○	IRS did not establish policies with respect to how assessors are to consider prior findings from other federal assessments when assessing state agencies' cybersecurity.

Legend: ● = Established policies that addressed all aspects of this activity. ○ = Established policies that addressed some, but not all, aspects of this activity. ◐ = Did not establish policies that addressed any aspects of this activity.

Source: GAO analysis of agency data. | GAO-20-123

Table 10: Detailed Assessment of the Social Security Administration's (SSA) Policies for Coordinating when Assessing State Agencies' Cybersecurity

Policies	Supporting activities	Rating	Description
1. Policies for coordinating with state agencies.	Assessment schedules and time frames	●	SSA's certification process document, which is shared with states, detailed each step of the agency's assessment process as well as the anticipated number of days that are required to complete each step. The engagement letter is to coordinate with state officials specific dates and time frames for the assessment.
	Meeting and document requests	●	SSA's Security Evaluation Questionnaire directed states to attach documents that address information required by SSA. The Electronic Information Exchange Requirements coordinated meeting requests by providing examples to states of who SSA may request to meet with during the compliance review.
	Security test plans including testing techniques, location, and tools	●	SSA's Security Evaluation Questionnaire and Electronic Information Exchange Requirements provided for coordination with states on security test plans to include testing techniques and location. Testing tools were not applicable to SSA's assessments.
	Use of prior findings	◐	SSA partially developed policies for coordinating with states on the use of prior findings. Specifically, the Electronic Information Exchange Requirements stated that a state's prior performance from a past SSA review determined whether an assessment will be conducted on site or remotely and also determined the risk level for each state agency. However, SSA's policy did not address whether or how assessors should use prior findings from other security assessments conducted within the state.
2. Policies for coordinating with other federal agencies.	Assessment schedules and time frames	○	SSA did not establish policies that facilitate coordination with other federal agencies regarding assessment schedules and time frames.
	Meeting and document requests	○	SSA did not establish policies to coordinate with other federal agencies in scheduling meeting and document requests.

**Appendix II: Detailed Assessment of Selected
Federal Agencies' Policies**

Policies	Supporting activities	Rating	Description
	Security test plans including testing techniques, location, and tools	○	SSA did not establish policies to coordinate with other federal agencies on security test plans.
	Use of prior findings	○	SSA did not establish policies with respect to how assessors are to consider prior findings from other federal assessments when assessing the overall effectiveness of state agencies' cybersecurity.

Legend: ● = Established policies that addressed all aspects of this activity. ○ = Established policies that addressed some, but not all, aspects of this activity. ○ = Did not establish policies that addressed any aspects of this activity.

Source: GAO analysis of agency data. | GAO-20-123

Appendix III: Breakdown of Selected Federal Agencies' Reported Spending for Fiscal Years 2016 through 2018

The following table provides the breakdown of selected agencies' reported spending during fiscal years 2016 through 2018 associated with assessing states' compliance with cybersecurity requirements.

Table 11: Selected Federal Agencies' Fiscal Years 2016-2018 Reported Spending for Assessing States' Compliance with Cybersecurity Requirements (expenditures in millions)

Agency	IRS	SSA	FBI's CJIS	CMS ^a	Total
Staff and travel	\$12.3	.58	3.2	1.3	—
Contractors and travel	\$15.0	.21	—	8.4	—
Others	\$3.7	—	—	—	—
Total	\$31	.79	3.2	9.7	44.7

Legend: — = Agency did not report costs for this category.

Source: GAO analysis of agency data. | GAO-20-123

Note: CMS = Centers for Medicare and Medicaid Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

^aCMS's expenditures for contractors are based on a project contract from July 2015 through July 2018. CMS uses contractors to review final assessments submitted by a state. State agencies bear the cost of hiring contractors to perform security assessments against the CMS requirements.

Appendix IV: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

April 14, 2020

Vijay D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. D'Souza:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, *"Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States"* (GAO-20-123).

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

Sincerely,

Sarah C.
Arbes -S

Digitally signed by
Sarah C. Arbes -S
Date: 2020.04.14
14:32:01 -04'00'

Sarah C. Arbes
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: SELECTED FEDERAL AGENCIES NEED TO COORDINATE ON REQUIREMENTS AND ASSESSMENTS OF STATES (GAO-20-123)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report. HHS takes its responsibility to protect and secure beneficiary data seriously, and has established strong cybersecurity requirements for states to follow when accessing, storing, and transmitting federal data.

As part of GAO's review, they compared cybersecurity requirements for programs at four federal agencies—the Centers for Medicare & Medicaid Services' (CMS), Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), and Social Security Administration (SSA). For CMS, GAO specifically reviewed CMS' state cybersecurity requirements relating to data shared as part of provisions in the Patient Protection and Affordable Care Act (PPACA). In 2010, PPACA established Health Insurance Exchanges, also known as Marketplaces, through which consumers could submit applications and enroll in health coverage. Under the law, states have the authority to establish a state exchange. CMS works with all states to address the specific needs of their consumers while also meeting the requirements and responsibilities set by statute.

The Federal Information Security Management Act of 2002 (FISMA 2002) requires each Federal agency to develop, document, and implement an agency-wide information and information system security program that supports the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA 2014) amends FISMA 2002, recognizing evolving security concerns by focusing on issues caused by security incidents, by strengthening the use of continuous monitoring, and by increasingly focusing on compliance.

FISMA 2002 and 2014 require the National Institute of Standards and Technology (NIST) to develop security standards and guidance, including minimum requirements for federal systems. NIST also developed an integrated *Risk Management Framework* which brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies. HHS utilizes a risk-based approach to implementing NIST standards across the department through policies and procedures such as the *HHS Information Security and Privacy Policies* and has an enterprise-wide information security and privacy program, known as the HHS Cybersecurity Program, to protect against potential information technology threats and vulnerabilities. In addition, CMS provides guidance to both CMS staff and its contractors in the *CMS Information Security Acceptable Risk Safeguards (ARS)* as to the minimum acceptable level of required security controls that must be implemented by CMS and its contractors to protect information and information systems.

CMS has developed, assembled, and implemented a document suite of guidance, requirements, and templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0, in accordance with the agency's Information Security and Privacy programs. The guidance is founded upon PPACA, CMS regulations implementing PPACA, FISMA 2002, amended by FISMA 2014 requirements of the federal government, and the NIST Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems*

**Appendix IV: Comments from the Department
of Health and Human Services**

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: SELECTED FEDERAL AGENCIES NEED TO COORDINATE ON REQUIREMENTS AND ASSESSMENTS OF STATES (GAO-20-123)

and Organizations, and NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. The guidance in the MARS-E document suite applies to all PPACA Administering Entities. “Administering Entity” includes newly established Exchanges, whether federal or state, state Medicaid agencies, Children’s Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program.

Even though state-based Administering Entities need not comply with FISMA, CMS has chosen NIST guidance as the basis for the standards for Administering Entities because it is the de facto method for specifying security and privacy control requirements throughout the Information Technology (IT) industry. However, variances are to be expected. Per NIST SP 800-53A Rev 4, “the procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security control assessments and privacy control assessments that support organizational risk management processes and that are aligned with the stated risk tolerance of the organization.” State systems run in diverse environments developed and maintained by the states themselves, so in applying NIST guidance, CMS tailored some of the controls to allow flexibilities for states, while still keeping the overall intent of the guidance. In addition, controls mentioning “organization-defined” actions, were passed on to the states to define based on their organizational structure.

In developing the MARS-E document suite for states, and during subsequent updates, CMS solicited feedback and approval from Federal partners, including the IRS, SSA, and FBI Criminal Justice Information Services (CJIS). Based on feedback from Federal partners of controls deemed essential in protecting data for which these agencies were responsible, CMS made updates to the requirements. These controls are tailored to the specific data being provided to states and their IT environment boundaries, so requirements would not be expected to align with requirements other agencies have for distinct data and IT environments. For example, CMS chose to include a requirement that state agencies review their organization-wide information security program plans annually, since many states were standing up new systems which needed continuous review as they matured.

While some of the CMS selected controls may be unique when viewed in comparison with other agency security control selections, they are not unique to the standard moderate baseline as documented in NIST, SP 800-53; Rev. 4 or the CMS ARS 3.1, which was the rationale for including these controls. As the CMS ARS controls change, CMS anticipates similar changes would be made to future versions of MARS-E. The overall rationale for controls selection is documented in MARS-E, Ver. 2.0; Volume I. In addition, CMS security requirements must align with CMS policy, which goes through public comment and rulemaking. For example, CMS finalized the 10-year record retention standard through this process.

The state-based Administering Entities are custodians of sensitive information such as Personally Identifiable Information (PII) for millions of US citizens. As such, they have a unique responsibility for ensuring its ultimate protection. Through continuous monitoring and regular security and privacy control testing, the Administering Entities demonstrate that they meet this responsibility. CMS requires all security and privacy controls attributable to a state system or application be assessed over a 3-year period. Additionally, this assessment is to be conducted by an “independent assessor,” sometimes referred to as a “third-party” assessor. CMS does not

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: SELECTED FEDERAL AGENCIES NEED TO COORDINATE ON REQUIREMENTS AND ASSESSMENTS OF STATES (GAO-20-123)

directly conduct any assessments of state systems, but reviews the results of assessments as part of the process to grant state systems authorization to connect to the Federal Data Services Hub. CMS also provides guidance to states on their requirements for completing a security and privacy control assessment as well as targeted technical security and privacy assistance. CMS provides states flexibility to coordinate their assessments around other ongoing assessments and allows states to use findings from other assessments with overlapping controls and IT boundaries, as feasible. CMS plans to update guidance to provide further detail on how states may maximize coordination to reduce their overall burden.

GAO made twelve recommendations, two of which were directed at CMS. GAO's recommendations to CMS and CMS' responses are below.

Recommendation 3

The Administrator of CMS should, in collaboration with OMB, solicit input from FBI, IRS and SSA, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible and document CMS's rationale for maintaining any requirements variances.

HHS Response

HHS concurs with GAO's recommendation. As stated above, CMS already collaborates with federal agencies through the development of MARS-E guidance. In developing the MARS-E guidance, and during subsequent updates, CMS solicited feedback and approval from Federal partners, including the IRS, SSA, and FBI/CJIS. Based on feedback from Federal partners of controls deemed essential in protecting data for which these agencies were responsible, CMS made updates to the requirements. As CMS updates existing security policies for PPACA Administering Entities, we will continue to solicit feedback from our Federal partners. In addition, CMS regularly communicates with state agency stakeholders, and will continue to do so to solicit feedback as we update security policies. CMS has documented the overall rationale for its decisions on selected controls, and has begun to document more granular rationale. Upon direction from the Office of Management and Budget (OMB), CMS will collaborate with other federal agencies on cybersecurity requirements pertaining to state agencies, as feasible.

Recommendation 4

The Administrator of CMS should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable.

HHS Response

HHS concurs with GAO's recommendation. However, as the GAO noted, CMS does not conduct assessments of states' compliance with security policy. These assessments are conducted by an "independent assessor," sometimes referred to as a "third-party" assessor hired by the states. Therefore, states would be responsible for maximizing coordination with other federal agencies in the planning and coordination of the assessment. CMS provides states flexibility to coordinate their assessment around other ongoing assessments and allows states to use findings from other assessments with overlapping controls and IT boundaries, as feasible. CMS will update guidance

**Appendix IV: Comments from the Department
of Health and Human Services**

**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED — CYBERSECURITY: SELECTED FEDERAL AGENCIES
NEED TO COORDINATE ON REQUIREMENTS AND ASSESSMENTS OF STATES
(GAO-20-123)**

to provide further detail on how states may maximize coordination to reduce their overall burden.

Appendix V: Comments from the Federal Bureau of Investigation

U. S. Department of Justice
Federal Bureau of Investigation



Washington, D. C. 20535-0001

Date: April 27, 2020

TO: Vijay D'Souza
Director, Information Technology
Government Accountability Office
441 G Street, NW
Washington, DC 20548

FROM: Michael D. DeLeon
Assistant Director
Criminal Justice Information Services (CJIS) Division

RE: CJIS DIVISION RESPONSE TO GOVERNMENT ACCOUNTABILITY OFFICE
(GAO) DRAFT *CYBERSECURITY: SELECTED FEDERAL AGENCIES NEED TO
COORDINATE ON REQUIREMENTS AND ASSESSMENTS OF STATES*

Dear Ms, Harris:

The FBI CJIS Division has reviewed the March 2020 GAO Draft *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*. In addition to the technical comments submitted on 3/26/2020, the FBI CJIS Division provides responses to the three recommendations within the draft directed to the FBI.

**Appendix V: Comments from the Federal
Bureau of Investigation**

The FBI Director should, in collaboration with OMB, solicit input from CMS, IRS, SSA, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible. (Recommendation 5)

The FBI CJIS Division concurs with GAO Recommendation 5. The FBI CJIS Division will, in collaboration with OMB and to the greatest extent possible, solicit input from CMS, IRS, SSA, and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance. The FBI CJIS Division requests that the GAO and/or the OMB provide the points of contact at CMS, IRS, and SSA who participated in this GAO study. This offers optimal efficiency for the FBI CJIS Division to initiate the recommendation. The FBI CJIS Division is embarking on a modernization of the CJIS Security Policy consisting of data categorization and updating current security controls. Once identified, members from IRS, SSA, CMS, and other state agencies will be given the opportunity to participate in this modernization.

The FBI Director should fully develop policies for coordinating with state agencies on the use of prior findings from relevant cybersecurity assessments conducted by other organizations. (Recommendation 6)

The FBI CJIS Division concurs with GAO Recommendation 6. Implementation of this recommendation has been completed by the FBI CJIS Division. As noted in the report, the FBI CJIS Division had procedures for coordinating with states, however, they were not formally documented. Following this GAO study, the FBI CJIS Division documented its policies for coordinating with state agencies on the use of prior findings from relevant cybersecurity assessments conducted by other organizations. A copy can be provided upon request. The FBI CJIS Division recommends Recommendation 6 be closed.

The FBI Director should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. (Recommendation 7)

The FBI CJIS Division concurs with GAO Recommendation 7. The FBI CJIS Division will revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable. The FBI CJIS Division requests that the GAO and/or the OMB provide the audit points of contact at CMS, IRS, and SSA who participated in this GAO study. This offers optimal efficiency for the FBI CJIS Division to initiate the recommendation.

Appendix VI: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

April 8, 2020

Mr. Vijay D'Souza
Director, Information and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. D'Souza,

Thank you for the opportunity to review the draft report, "CYBERSECURITY: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States" (GAO-20-123). We agree with the recommendations.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

A handwritten signature in blue ink that reads "Stephanie Hall".

Stephanie Hall
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix VII: Comments from the Internal Revenue Service



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

April 28, 2020

Mr. Vijay D'Souza
Director, Information Technology
and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. D'Souza:

I have reviewed the draft report entitled CYBERSECURITY: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States (GAO-20-123) and appreciate the opportunity to provide comments. As acknowledged in the report, each federal oversight agency addresses different legal requirements for protection of information shared with states. The Internal Revenue Service (IRS) has the unique authority of enforcing disclosure and use restrictions under Internal Revenue Code (IRC) § 6103 when tax records are disclosed, which authority our Counsel advises cannot be redelegated.

Federal, state and local agencies that receive tax data under the various provisions of IRC § 6103 are statutorily required to establish safeguards to protect the confidentiality of the data. They must meet IRC § 6103(p)(4) requirements, IRS Regulations and standards published in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. Oversight by the IRS Office of Safeguards applies to the state agency officers, employees and contractors (where statutorily allowed) who are authorized to receive and legally bound to protect the data. We have an excellent relationship with our agency partners and collaborate with them regularly to ensure they understand and address compliance with IRS policies and procedures.

Often these agencies have service level agreements with the state's consolidated data center and IRS is not a party to such agreements. The state data center manages the agency's information systems security; however, they are not legally authorized to receive tax data independently. Each state agency is responsible for the coordination of IRS reviews within the agency and at the data center where the state's chief information officer and chief information security officer often have a role in the security assessments but do not have an official relationship with IRS.

2

To reduce burden and increase effectiveness, IRS conducts most system testing for security configuration and control implementation using automated scanning tools. The platforms that are shared between multiple state agencies are only tested once and the results are reported to the head of each agency. IRS plans reviews through advance coordination with agency contacts to ensure relevant systems are properly identified and prepared for onsite assessments, which expedites the review and eliminates scanning barriers. Publication 1075 utilizes the most current versions of NIST 800-53 and NIST 800-63 moderate as the baseline for configuration requirements. Benchmarks for our assessments are provided by the Center for Internet Security, Treasury Directives and the Internal Revenue Manual. To ensure a robust security program, the IRS selects the most appropriate controls and configuration standards for agencies to protect the confidentiality of tax data.

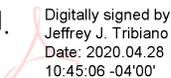
As noted in the report, IRS has several unique cybersecurity requirements and variances from the other agencies reviewed. Our assessments are not focused solely on system configuration and NIST based controls, but also on the user permissions granted and authorized uses of tax data pursuant to IRC § 6103. While the IRS is willing to participate in collaborative working sessions established by OMB to discuss the impact of inconsistent standards on state agencies, our ability to harmonize requirements with other federal oversight agencies may be limited. By law, the IRS must terminate data sharing agreements with agencies that fail to meet IRC § 6103(p)(4) requirements in accordance with Publication 1075 standards and put tax data at risk for loss, breach or misuse.

The IRS has sole statutory oversight authority and enforces requirements for agencies subject to IRC § 6103. No other federal agency has the authority to access tax data in these systems. Therefore, we cannot rely solely on an assessment conducted by another agency and are unable to coordinate joint reviews.

The responses to your specific recommendations are enclosed. If you have questions, please contact me, or a member of your staff may contact Phyllis Grimes, director, Governmental Liaison, Disclosure and Safeguards, at 202-317-4202.

Sincerely,

Jeffrey J.
Tribiano



Digitally signed by
Jeffrey J. Tribiano
Date: 2020.04.28
10:45:06 -04'00'

Jeffrey J. Tribiano
Deputy Commissioner for
Operations Support

Enclosure

Recommendations for Executive Action

Recommendation 8

The IRS Commissioner should, in collaboration with OMB, solicit input from CMS, FBI, SSA and state agency stakeholders on revisions to its security policy to ensure that cybersecurity requirements for state agencies are consistent with other federal agencies and NIST guidance to the greatest extent possible.

Comment

The IRS partially agrees with this recommendation. The IRS will participate in collaborative working sessions established by OMB with interested stakeholders to discuss the impact of inconsistent standards on state agencies and the extent to which the standards might be harmonized.

In addition to following NIST guidance for moderate classification, the IRS must also follow Treasury Directives and internal standards for systems that process tax data. As a result, our ability to harmonize requirements with other federal oversight agencies may be limited. By law, the IRS must terminate data sharing agreements with agencies that fail to meet IRC § 6103(p)(4) requirements in accordance with Publication 1075 standards and put tax data at risk for loss, breach or misuse.

IRS already notifies all Federal and state agencies when changes are proposed to Publication 1075 standards and considers all feedback, including operational impacts, before modifying security policies. Varied standards are routinely addressed by security professionals managing information systems by applying the highest standard in order to properly protect systems and data and meet any assessment.

Recommendation 9

The IRS Commissioner should revise its assessment policies to maximize coordination with other federal agencies to the greatest extent practicable.

Comment

The IRS disagrees with this recommendation. The IRS has sole statutory oversight authority and enforces requirements for agencies subject to IRC § 6103. In each state, there are multiple independent agencies that receive tax data from the IRS under differing authorities with separate systems that require IRS review. No other federal agency has the authority to access tax data in these systems. Our reviews are not focused solely on system configuration and NIST based controls but also on the user permissions granted and authorized uses of tax data pursuant to IRC § 6103. Therefore, we cannot rely solely on an assessment conducted by another agency. While schedule coordination may reduce burden at the state data center, it would significantly increase the burden for the IRS and our state agency partners. IRS already coordinates with multiple independent state agency program owners and agency heads. Each State has between 4 and 10 agencies that IRS works with to accommodate schedules around any competing federal assessments or other conflicts that may arise.

Appendix VIII: GAO Contact and Staff Acknowledgements

GAO Contact

Vijay D'Souza, (202) 512-6240, dsouzav@gao.gov

Staff Acknowledgments

In addition to the individual named above, Josh Leiling (assistant director), Lori Martinez (analyst in charge), Gerard Aflague, Joseph Andrews, David Blanding, Chris Businsky, Rebecca Eyler, Torrey Hardee, Andrea Harvey, Keith Kim, Monica Perez-Nelson, and Carl Ramirez made significant contributions to this report.

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

