



December 2019

ASSESSING DATA RELIABILITY

Contents

Letter		1
	Preface	1
	Section 1: Understanding Data Reliability	3
	Section 2: Deciding Whether a Data Reliability Assessment Is Necessary	11
	Section 3: Determining the Extent of the Assessment	15
	Section 4: Steps for Collecting Information When Assessing Data Reliability	17
	Section 5: Making the Data Reliability Determination	24
	Section 6: Including Appropriate Language in the Report	31
	Section 7: Additional Considerations	34
Appendix I	Example Documentation Requests and Interview Questions	38
Appendix II	Assessing the Reliability of Data from Statistical Agencies	44
Appendix III	Examples of Data Tests	46
Appendix IV	Example Language for Reporting on Data Reliability	49
Appendix V	GAO Contact and Staff Acknowledgements	68
Figures		
	Figure 1: Overview of the Data Reliability Assessment Process	10
	Figure 2: Determining the Need for a Data Reliability Assessment	11
	Figure 3: Steps for Collecting Information When Assessing Data Reliability	17
	Figure 4: Making the Data Reliability Determination	25

Abbreviations

GAGAS generally accepted government auditing standards

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.



Preface

Data from outside sources are often central to audits. While these data are simply one type of evidence that auditors rely on, appropriately assessing their reliability may require more technical effort than other types of evidence. The purpose of this guide is to describe the principles behind and steps involved in assessing the reliability of data used for audits. This guide is consistent with the Yellow Book — the 2018 *Government Auditing Standards* — which defines generally accepted government auditing standards (GAGAS), and supersedes GAO’s 2009 guidance, *Assessing the Reliability of Computer-Processed Data*.¹ This guidance covers computer-processed data, referred to in this document simply as “data”, which result from computer processing or entering data into a computer system.² Data can vary in form and may be housed in electronic files or tables in published reports. A more detailed discussion of the types of data covered by this guidance is found in section 1.

Various tests of sufficiency and appropriateness are used for all types of evidence, whether or not they are part of a dataset, to assess whether evidence standards are met. Because assessing sufficiency and appropriateness of data may require a more technical review than other types of evidence, it may appear that such data are subject to a higher standard of testing than other evidence. This is not the case.

This guide provides a flexible, risk-based framework for data reliability assessments that can be geared to the specific circumstances of each engagement. The framework gives structure to planning and reporting by encouraging auditors to:

- make use of existing information about the data,
- conduct only the amount of audit work necessary to determine whether the data are reliable enough for audit purposes,

¹GAO, *Government Auditing Standards: July 2018 Revision*, [GAO-18-568G](#) (Washington, D.C.: July 2018), and GAO, *Assessing the Reliability of Computer-Processed Data*, [GAO-09-680G](#) (Washington, D.C.: July 2009).

²Prior versions of this guidance use the term “computer-processed data” to characterize the type of information covered by these guidelines. The 2018 Government Auditing Standards makes reference to computer-processed and computer-generated information. The current version of this guidance uses the term “data” without a modifier and is intended to encompass all of these terms. The term “data” in this guidance covers the same kinds of information as prior versions.

-
- maximize professional judgment, and
 - involve the appropriate people, including management and stakeholders, in key decisions.

The primary focus of a data reliability assessment is to determine whether the data can be used for the audit's intended purposes. This guide is designed to help auditors make an appropriate, defensible assessment in the most efficient manner.³



Nancy Kingsbury
Managing Director, Applied Research and Methods

³This guidance uses the term “auditor” and “audit team” to maintain consistency with GAGAS terminology. According to GAGAS, auditors include: “individuals who may have the title auditor, information technology auditor, analyst, practitioner, evaluator, inspector, or other similar titles”. Similarly, use of the term “audit” here is inclusive of terms such as engagement and evaluation. See [GAO-18-568G](#), section 1.27f.

Section 1: Understanding Data Reliability

Attributing the data to its source does not alleviate the need for auditors to assess the reliability of the data.

While all evidence is subject to GAGAS, this guide provides a framework for assessing the sufficiency and appropriateness of one type of evidence: computer-processed data (here: “data”). According to GAGAS, auditors should assess the sufficiency and appropriateness of computer-processed information, regardless of whether this information is provided to auditors or they extract it independently.⁴ Attributing the data to its source does not alleviate the need for auditors to assess the reliability of the data. This guide will help the auditor design a data reliability assessment that is appropriate to the audit’s purpose and then evaluate the results of the assessment.

Types of Data Covered by this Guide

This guide pertains to data obtained from an outside organization (e.g., from an audited agency, an organization the agency has contracted with, a state or local government agency, or a private or foreign entity) regardless of the system in which the data resides. While under the broadest definitions almost all information could be considered “data”, this guidance primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files (i.e., datasets).

Data vary widely in form, from data in electronic files to tables in published reports, and include:

- data extracts from databases, data warehouses, or data repositories;
- data maintained in Microsoft Excel or Access, or similar commercial products;
- data extracts from enterprise software applications supported by information technology departments or contractors;
- public use data or other replicated detail or summary-level databases accessible through an application other than the original source system;
- data collected using web-based forms and surveys.

Often data for an audit are initially received in the form of an aggregate number or estimate but are still derived from computer processing. For example, these may be data or numbers summarized in a report, copied

⁴See [GAO-18-568G](#), sections 8.90 - 8.98.

from a document, provided verbally or in writing, or provided through a survey or other data collection instrument.⁵ When these numbers originate from a data system, auditors should follow this guidance in deciding whether and how to assess the reliability of the underlying data.

While this guidance primarily applies to structured data – data in organized records in which each field has a pre-defined data type like numeric, date, alphabetic, etc., some of these principles may apply to examining unstructured data, which is often primarily textual information that has not been organized into a structured format for analysis. For example, when organizing and analyzing unstructured data, such as a collection of narrative reports, image files, or data scraped from federal agency websites that is not in a prepared data file, auditors still need to ensure they have extracted complete and accurate information from the original source.

Defining Data Reliability in an Audit Environment

In an audit environment, reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate.

- **Applicability for audit purpose** refers to whether the data, as collected, are valid measures of the underlying concepts being addressed in the audit’s research objectives.
- **Completeness** refers to the extent to which relevant data records and fields are present and sufficiently populated.
- **Accuracy** refers to the extent that recorded data reflect the actual underlying information.⁶

⁵The processes involved in assessing the reliability of data collected through a survey will often differ from reliability assessments of data from other sources. See discussion in section 7.

⁶While this guide focuses on the reliability of data in terms of completeness, accuracy, and applicability for audit purpose, other data quality considerations may affect these aspects of the data. In particular, *consistency* refers to whether data are sufficiently clear and well defined to yield comparable results in similar analyses. For example, if data are entered at multiple sites, inconsistent interpretation of data entry rules can lead to data that, taken as a whole, are unreliable.

Relevance of Internal Controls and Information System Controls

A key element of data reliability assessments is the consideration of internal controls including information system controls. An organization's internal controls over data can include the establishment of control activities through policies and procedures intended to achieve objectives and respond to risks. Information system controls support the underlying structures and processes of the system where data are maintained. They consist of those internal controls that depend on information systems processing and include general controls, application controls, and user controls. Examples of information system controls are limits on access to the system and edit checks on data entered into the system.⁷ The steps taken to collect information during a data reliability assessment can help auditors better understand these controls and assess whether they have been designed, implemented, and are operating in a manner that supports the reliability of data. Depending on the audit objectives, auditors may learn more about information system controls by gathering information from knowledgeable officials, reviewing documentation about the system and processes, and testing the data for indicators that such controls are present. See section 4 for more information about performing these steps.

⁷For more information about system controls, and how specific controls contribute to internal control and the reliability of computer processed data, see: GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); GAO, *Federal Information System Controls Audit Manual*, [GAO-09-232G](#) (Washington, D.C.: February 2009); and GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*, vol. 1, [GAO-18-601G](#) (Washington, D.C.: June 2018).

Types of Information System Controls

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure the proper operation of information systems. They include security management, configuration management, and logical and physical access controls, among others.

Application controls, or business process controls, are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. They include controls over input, processing, output, master file, interface, and the data management system.

User controls are controls that are performed by people interacting with information systems. A user control is considered an information system control if a dependency on information system processing exists. The effectiveness of a user control typically depends on information system processing or the reliability of information produced by information systems. (For example, the effectiveness of a user control to review and follow-up on exceptions typically depends on the reliability of the exception report produced by the information system.)

Source: Adapted from GAO, *Government Auditing Standards: July 2018 Revision*, GAO-18-568G (Washington, D.C.: July 2018), section 8.63; GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009); and GAO and Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*, vol. 1, GAO-18-601G (Washington, D.C.: June 2018). | GAO-20-283G.

Assessment of Data Reliability Depends on Audit Purpose

Assessments of reliability are made in the broader context of the audit's purpose and the risk associated with using insufficiently reliable data. Auditors determine whether data are fit for use given the audit's objectives and any expected findings and conclusions. A data reliability determination does not involve attesting to the overall reliability of the data or database. The audit team is only determining the reliability of the specific data needed to support the findings, conclusions, or recommendations in the context of the audit objectives.

A decision that data are reliable for audit purposes does not necessarily mean that the data are error-free. Errors are considered acceptable when an audit team has assessed the associated risk and concluded that the errors are not substantial enough to cause a reasonable person, aware of the errors, to doubt a finding, conclusion, or recommendation supported by the data. As part of this decision, the audit team may consider changing the use or characterization of the data within the report in response to the results of the data reliability assessment.

The Role of Professional Judgment in Data Reliability Assessments

The use of professional judgment is an essential element of determining the reliability of data for use in an audit. According to GAGAS, professional judgment includes exercising reasonable care and professional skepticism.⁸ Among other things, attributes of professional skepticism include a questioning mind and critical assessment of evidence. Auditors use this critical mindset to assess data that may initially seem appropriate. Exercising professional judgment in determining the sufficiency and appropriateness of evidence is integral to the engagement process.

Professional judgment is the application of the collective knowledge, skills, and abilities of all personnel involved with an engagement. These personnel may include those with expertise in data analysis, economics, methodology, information technology, statistics, and other related specialties. The audit team's professional judgment is important in each stage of a data reliability assessment including deciding whether a data reliability assessment is necessary, determining the extent of the assessment, and making the final determination of reliability. At times, members of the audit team, including technical specialists, may have differing judgments on how to evaluate available information about the data and whether the data can be used for the audit. To ensure transparency in how the audit team's judgment is applied, it is important to document how the information obtained about the data informed the audit team's judgment during the assessment process. When differences in judgment among audit staff affect the final decision about whether and how to use the data, appropriate management will need to make the final decision about the reliability of the data for the audit's purpose.

⁸See [GAO-18-568G](#), sections 3.109 - 3.117.

Professional Judgment in the Yellow Book (selected content)

3.109 Auditors must use professional judgment in planning and conducting the engagement and in reporting the results.

3.110 Professional judgment includes exercising reasonable care and professional skepticism. Reasonable care includes acting diligently in accordance with applicable professional standards and ethical principles. Attributes of professional skepticism include a questioning mind, awareness of conditions that may indicate possible misstatement owing to error or fraud, and a critical assessment of evidence. Professional skepticism includes being alert to, for example, evidence that contradicts other evidence obtained or information that brings into question the reliability of documents or responses to inquiries to be used as evidence. Further, it includes a mindset in which auditors assume that management is neither dishonest nor of unquestioned honesty. Auditors may accept records and documents as genuine unless they have reason to believe the contrary. Auditors may consider documenting procedures undertaken to support their application of professional skepticism in highly judgmental or subjective areas under audit.

3.112 Professional judgment represents the application of the collective knowledge, skills, and abilities of all the personnel involved with an engagement, as well as the professional judgment of individual auditors. In addition, professional judgment may involve consultation with other stakeholders, specialists, and management in the audit organization.

3.115 Using professional judgment is important to auditors in determining the necessary level of understanding of the engagement subject matter and related circumstances. This includes considering whether the audit team's collective experience, training, knowledge, skills, abilities, and overall understanding are sufficient to assess the risks that the subject matter of the engagement may contain a significant inaccuracy or could be misinterpreted.

3.116 An auditor's consideration of the risk level of each engagement, including the risk of arriving at improper conclusions, is also important. Within the context of audit risk, exercising professional judgment in determining the sufficiency and appropriateness of evidence to be used to support the findings and conclusions based on the engagement objectives and any recommendations reported is integral to the engagement process.

3.117 While this requirement places responsibility on each auditor and audit organization to exercise professional judgment in planning and conducting an engagement, it does not imply unlimited responsibility nor does it imply infallibility on the part of either the individual auditor or the audit organization. Absolute assurance is not attainable because of factors such as the nature of evidence and characteristics of fraud. Professional judgment does not mean eliminating all possible limitations or weaknesses associated with a specific engagement, but rather identifying, assessing, mitigating, and concluding on them.

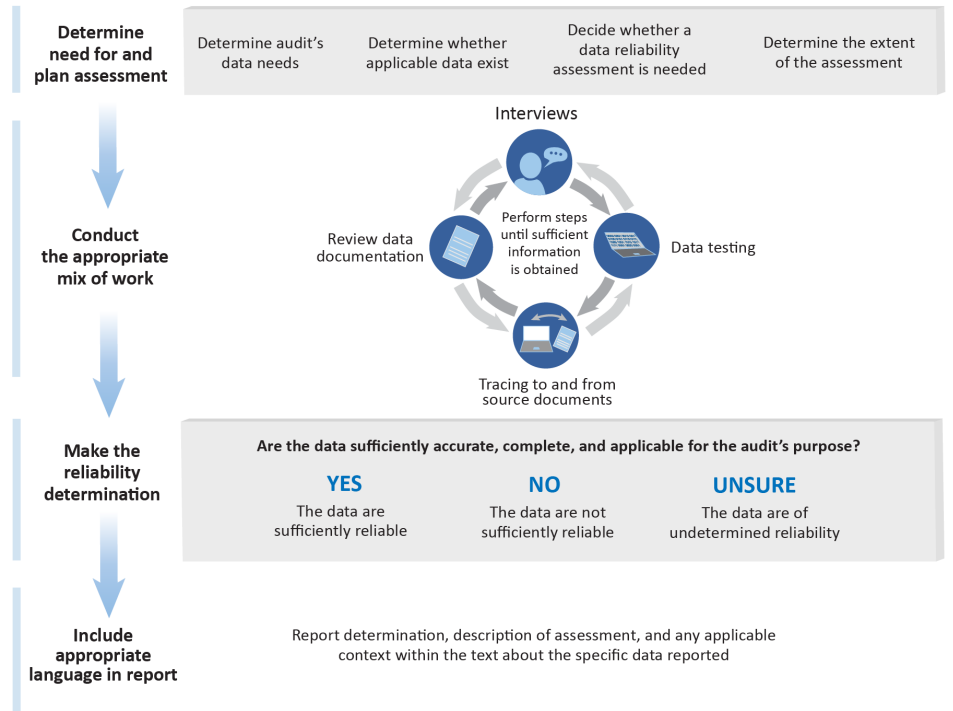
Source: GAO, *Government Auditing Standards: July 2018 Revision*, [GAO-18-568G](#) (Washington, D.C.: July 2018). | GAO-20-283G.

An Overview of the Assessment Process

The data reliability assessment process takes into account the expected importance of the data, the strength of corroborating evidence, and the risk of using the data, along with what is learned during the assessment. While the specific steps differ from one audit to another, an assessment should include sufficient work to allow the audit team to have a good understanding of how the data are collected, the systems they are extracted from, and the relevant information system controls for key data elements. Technical specialists can help the audit team consider these factors and plan the work.

Figure 1 illustrates the overall process for data reliability assessment, which is described in detail in sections 2 through 6. This process includes several key stages in the assessment, as well as actions to take and decisions to expect when completing the assessment. The data reliability process allows the audit team to select the appropriate mix of assessment steps to fit the particular needs of the audit. Not all the elements in figure 1 are necessary for all assessments.

Figure 1: Overview of the Data Reliability Assessment Process

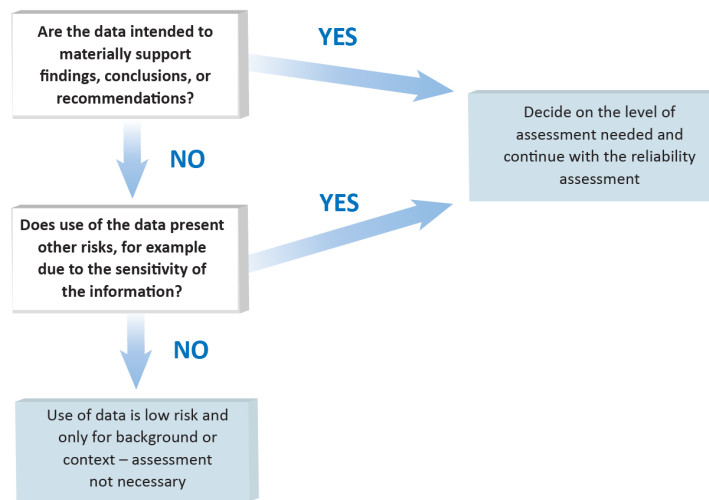


Source: GAO. | GAO-20-283G

Section 2: Deciding Whether a Data Reliability Assessment Is Necessary

To decide whether a data reliability assessment is necessary, consider the planned use of the data. The decision process is illustrated in figure 2 and described in more detail below.

Figure 2: Determining the Need for a Data Reliability Assessment



Source: GAO. | GAO-20-283G

Note: Financial and financial-related audits performed in accordance with the *Financial Audit Manual* and *Federal Information System Controls Audit Manual* are not required to follow this guidance.

Conditions Requiring a Data Reliability Assessment

Auditors should assess reliability if the data to be analyzed are intended to materially support findings, conclusions, or recommendations.

If data in the report provide context but also present additional risk...an assessment should be conducted that is appropriate to the risk of using the data.

Auditors should assess reliability if the data to be analyzed are intended to materially support findings, conclusions, or recommendations. Data reliability assessments are needed even when the report includes only a description of a condition; a finding does not need to be evaluative in order for data to be material. In addition, data material to a finding can include record-level data, summary or aggregate data, and estimates or projections based on data.

Whether data are material to a finding is a decision made for each engagement and based on the professional judgment of the audit team, including technical specialists. One way to think about materiality is to consider whether the evidence supporting the finding would still be sufficient and appropriate if the data being assessed were no longer used as evidence in the finding.⁹

In some circumstances, data that seem like background information may also materially affect the findings. If data in the report provide context but also present additional risk due to the sensitivity of the information because, for example, they serve as an impetus for the audit or are likely to be subjected to a high degree of scrutiny, an assessment should be conducted that is appropriate to the risk of using the data.

For example, if an estimate of the amount of dietary supplements Americans take is presented as a basis for conducting an audit of a regulatory agency, auditors should conduct a data reliability assessment to be reasonably confident of the estimate's accuracy.

If the audit team determines that a data reliability assessment is necessary, they may want to consider whether data from the system might be used for multiple audits and if a more in-depth, information system controls assessment is warranted. In an information system controls assessment, auditors generally perform a risk-based evaluation of controls. The nature, timing, and extent of procedures performed to assess information system controls vary, depending on the audit's objectives, the nature and extent of information system control risk, and other factors, such as the nature and complexity of the entity's information systems.¹⁰ If the auditors conclude that information systems controls are

⁹Materiality here is equivalent to the concept of significance in the context of performance audits; see [GAO-18-568G](#), section 8.15.

¹⁰For guidance on information system controls assessments, see [GAO-09-232G](#).

effective, this may reduce the need for direct testing of the data. An information system control assessment generally necessitates a greater investment of auditing resources and requires additional technical support but may be more efficient when data will be used in multiple audits. Technical specialists can help the team design an appropriate information system controls assessment that is aligned with the audit objectives and can connect the team with needed resources.

Conditions Not Requiring a Data Reliability Assessment

Auditors generally do not need to assess the reliability of data when the data do not materially affect findings, conclusions, or recommendations, and when the risk of using the data without the assessment is deemed acceptable. In many circumstances, information presented as background, context, or example does not require an assessment. However, as mentioned above, risk is a major determinant when deciding on the necessity of the assessment. One example of where an assessment is not needed is data that are only used to set the stage for reporting an audit's results or provide information that puts the results in proper context (e.g., the size of the program or activity under review). While such data may not need to be assessed, auditors should still ensure that the data are from the best available source and include attribution to that source.

For example, an audit finding might include the number of uninsured Americans, and auditors might want to put this number in the context of the overall U.S. population. While the estimate of the number of Americans who are uninsured would require a data reliability assessment, the estimate of the U.S. population may not require an assessment as long as the estimate came from a reliable source (for instance, the U.S. Census) and the information is only used to provide context.

In addition, if an audit relies on information that is used for widely accepted purposes and is obtained from sources generally recognized as appropriate, it may not be practical or necessary to conduct an assessment. Such information may include, for example, price indices that government agencies issue for adjusting for inflation. Deciding to use such information without further assessment calls for professional judgment by individuals with appropriate knowledge of the nature of the information and how it is being used in the audit (for example, technical specialists).

Finally, if an auditor is performing a financial audit or an information system controls assessment in accordance with the *Financial Audit Manual* and *Federal Information System Controls Audit Manual*, following this guidance is not required because concepts related to data reliability are incorporated into these methodologies.¹¹ However, this guide may be useful as a reference for auditors performing financial audits, as well as other types of engagements, such as attestation engagements involving an examination of internal controls.

¹¹See [GAO-09-232G](#) and [GAO-18-601G](#).

Section 3: Determining the Extent of the Assessment

The purpose of a data reliability assessment is to determine whether the data can be used to address the audit objectives. The professional judgment of the audit team, including technical specialists, is an important part of determining the extent of, and steps included in, a data reliability assessment. Factors to consider when determining the extent of the assessment are the:

- expected importance of the data to the final report,
- strength or weakness of any corroborating evidence, and
- anticipated risk of using the data.

Professional judgment is key when incorporating these factors into decisions about the extent of the assessment. In addition, changing audit circumstances may warrant reconsideration of decisions regarding the extent of the data reliability assessment. For example, in the course of an ongoing audit, new data or information may become available; the objectives of the audit may evolve or require modification; or additional resource, time, or other constraints may arise. If there are changes in the importance of or risk associated with using the data, or if other factors affect the intended use of the data, the audit team may decide to adjust the data reliability assessment accordingly.

Importance of the Data in the Final Report

In making an assessment, consider the data in the context of the final report. If the data are the sole source of information leading to findings and recommendations, a more extensive assessment will likely be necessary than if there are additional sources of evidence.

The assessment should focus on whether the data are reliable given the way that they will be reported. The precision of the data that will be reported can also be a factor in how extensive of an assessment is needed. When an objective calls for the use of precise numbers, a more thorough review may be warranted than when more approximate data is sufficient.

For example, when assessing the ability of charities to respond to a disaster, auditors can consider whether it is enough to know that resources will shelter a range of 400,000 to 500,000 people or whether more exact figures are needed.

Corroborating Evidence

Consider whether independent corroborating evidence exists and will support the findings, conclusions, or recommendations. The presence of corroborating evidence may reduce the extent of the data reliability assessment needed. Such evidence, when available, may be in the form of alternative databases, expert views, or other sources of evidence. The usefulness and strength (or persuasiveness) of corroborating evidence differs for each review.

For help in determining the strength or weakness of corroborating evidence, consider whether the corroborating evidence is:

- consistent with Yellow Book standards of evidence—sufficiency and appropriateness;
- able to provide crucial support;
- drawn from multiple sources;
- drawn from multiple types of evidence, such as testimonial, documentary, and physical; and
- independent of other sources.

Risk of Using the Data

Risk, in the context of data reliability, is the likelihood that using data of questionable reliability could have substantial negative consequences for the auditing agency or on the decisions of policymakers and others.

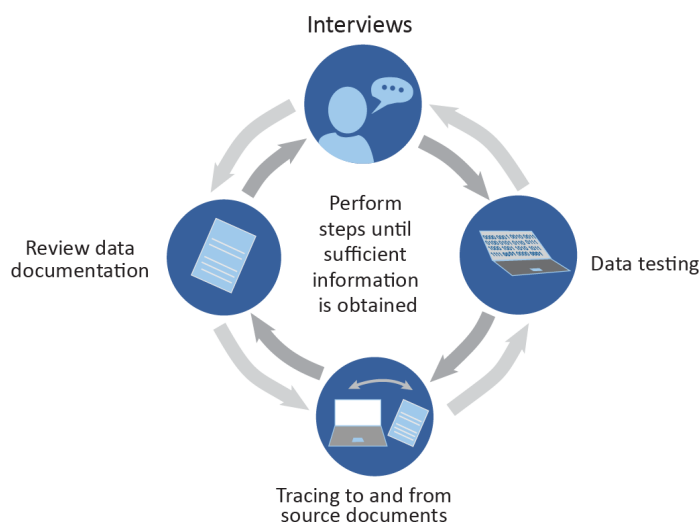
Risk, in the context of data reliability, is the likelihood that using data of questionable reliability could have substantial negative consequences for the auditing agency or on the decisions of policymakers and others. When using the data presents a greater risk, a more thorough assessment of data reliability may be needed. When considering the risk presented by the use of a set of data, auditors can think about whether the data:

- may be used to inform legislation, policy, or a program that could have substantial effect;
- may be used to inform important decisions by individuals or organizations with an interest in the subject;
- will be the basis for numbers that are likely to be widely quoted;
- are relevant to a sensitive or controversial subject; or
- have been evaluated for their quality by experts or external stakeholders.

Section 4: Steps for Collecting Information When Assessing Data Reliability

Data reliability assessment as a process includes a range of possible steps for collecting information about the data, as shown in figure 3. An assessment of data reliability can entail reviewing existing information about the data, including conducting interviews with knowledgeable officials and reviewing documentation; performing tests on the data; and other steps, such as tracing to and from source documents. The audit team exercises their professional judgment when deciding which information collection steps to incorporate into an assessment depending on audit circumstances.

Figure 3: Steps for Collecting Information When Assessing Data Reliability



Source: GAO. | GAO-20-283G

Deciding on the Appropriate Information Collection Steps

Deciding which information collection steps to take in an assessment is an iterative process. Most often the assessment will start by interviewing knowledgeable officials, reviewing data documentation, and conducting basic testing. The outcome of these steps can lead the audit team to conclude that sufficient information has been gathered to make a determination or to take additional steps to gather more information. Auditors may need to reconsider decisions about necessary steps if audit circumstances change, such as the identification of new data or a change in audit objectives. The mix of steps taken depends on circumstances specific to the audit, such as the importance of the data to the findings and information gathered during the assessment. The specific steps

should also be tailored to the data elements that will be used in the audit. The audit team may need to assess only a few elements of a database or assess many variables in various modules of a data collection system.

As discussed in section 1, the data reliability assessment process may also inform auditors about the information system controls present in the data system and whether they are likely to have resulted in reliable data. It may be helpful to consider the types of information system controls that are or are not present as information is gathered about the data and system. For example, one purpose of reviewing documentation about the system and data is to look for the presence of appropriate controls over data entry. When system documentation is limited, the need for additional interviews or electronic testing (to determine whether data contain appropriate values) may increase. Further, potential errors found during testing may lead to additional questions for the data owner about system controls.

An effective and efficient data reliability assessment considers aspects of the data that pose the greatest potential risk to the audit and the extent to which issues with accuracy and completeness are likely to occur.

An effective and efficient data reliability assessment considers aspects of the data that pose the greatest potential risk to the audit and the extent to which issues with accuracy and completeness are likely to occur.

For example, it may be appropriate to consider whether:

- data are generated using an automated process rather than entered manually,
- data fields are well-defined in data documentation and training materials,
- data entry is controlled by features such as drop down lists rather than open-ended text fields, or
- data are subject to verification.

Initiation of the data reliability assessment is optimally done early in the audit and includes the audit team members, as well as appropriate technical staff. The time and effort needed to take any or all these steps will depend on the audit and the amount of risk involved.

Using Information from Prior Data Reliability Assessments

To inform the assessment, auditors can use information from previous reliability assessments of the same data. This information may include prior interviews, previously collected documentation and reports, and the results of past electronic testing, among others. Because audit objectives differ in purpose, auditors will not necessarily draw the same conclusion

about the reliability of the data as the prior assessments. Nevertheless, if an earlier assessment is timely and relevant to the engagement, the information can be used as part of the assessment.

A prior data reliability assessment might be helpful but will not necessarily be sufficient for the new engagement. Consider the data fields, purposes, and time periods that were assessed, as well as other issues that could affect previous assessments' relevance to the current engagement. Generally, some additional steps beyond reviewing the prior data reliability assessment will be needed to ensure the data are sufficiently reliable for the specific purposes of the new engagement.

Steps for Collecting Information on the Reliability of Data

Auditors use their professional judgment to select among several possible steps when collecting information to assess the reliability of data. The information auditors collect can help determine the applicability of any data to the audit objectives as well as the accuracy and completeness of the collection, maintenance, and processing of the data. This information can come from interviews with knowledgeable individuals, reviews of reports or system documentation, data testing, or tracing to and from source documents. Sources for information and knowledge that may already exist include the agency under review and other data users. Keep in mind that information from agency officials, regardless of format, may be biased and therefore auditors should maintain appropriate skepticism about the information provided. Where possible, consult with technical specialists for help in collecting and reviewing this information. Appendix I provides example interview questions and document requests that auditors can consider using when collecting information on data reliability, and appendix II describes additional considerations for collecting information when assessing data from federal statistical agencies.

Interviews with Knowledgeable Officials

In most cases, auditors will ask knowledgeable officials questions about their data system and how it is used. These officials may include agency program officials, data managers, or technical specialists, or others outside the agency who are knowledgeable about the data. Auditors use what they know about the program under review and the data system to focus interview questions on the specific issues that most directly affect the usability of the data for the audit.

Ideally, interviews start taking place early. Interviewing agency officials to assess whether the data are applicable for audit purposes can help inform decisions about how to use the data. For example, auditors can inquire about whether the data include the population and time period of

interest, as well as variables appropriate to the audit objectives. Auditors can also use interviews to identify potential reliability issues with the data in the early stages of the assessment. Interview questions can focus on the completeness and accuracy of the data and the system controls surrounding the data or its system. Interviews later in the audit may focus particularly on gaining a better understanding of the data and addressing specific questions raised by the review.

Review of Data Documentation and Reports

A key source of information that agency officials or data owners may provide is documentation about the data or data system. Relevant documentation may include user manuals, data dictionaries, system documentation, table layouts, data entry and processing policies, and data quality assurance program materials. Auditors can review documentation to identify whether information system controls are appropriate for the audit purpose. Review of documentation can help auditors determine, for example, whether data entry controls seem sufficient to minimize errors or whether documented quality control steps such as validation procedures seem adequate given the type of data and how they will be used in the audit. However, other steps, such as data testing or tracing to or from source documents, may be needed to confirm whether the data are consistent with documentation.

In addition, there may be evaluations of the data or systems that provide useful information about the quality of the data. Such reviews (e.g., financial audit reports) may be performed by agency officials, contractors, or others, such as academics. Other agency information can include reports under the Federal Managers' Financial Integrity Act and the Clinger-Cohen Act, GPRAMA Modernization Act (GPRAMA) plans and reports, and Chief Information Officer and Inspector General reports.¹² Some of this information can be found on agency websites. Information can also be obtained from other data users, as well as relevant literature. Understanding whether the data have been used by others, and for what purposes, may provide helpful information about the usability of the data

¹²See, Federal Managers' Financial Integrity Act of 1982, Pub. L. No. 97-255, 96 Stat. 814 (Sept. 8, 1982), 31 U.S.C. § 3512; Clinger-Cohen Act of 1996, Pub. L. No. 104-106, divs. D, E, 110 Stat. 186, 642-703, 679 (Feb. 10, 1996) 40 U.S.C. § 11101 *et seq.*; GPRAMA Modernization Act of 2010 (GPRAMA), Pub.L. No. 111-352, 124 Stat. 3886 (Jan. 4, 2011). GPRAMA updated the Government Performance and Results Act of 1993 (GPRAMA), Pub.L. No. 103-62, 107 Stat. 285 (Aug. 3, 1993); and Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 *et seq.* largely superseded by Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) 44 U.S.C. § 3551 *et seq.*

for audit purposes. To help identify documentation, auditors can use a variety of databases and other research tools as well as other organizations' websites.

GAO may also have relevant information in its reports or website. For example, GAO has conducted financial statement audits and reported on the effectiveness of controls for financial information systems at several federal agencies.

Data Testing

Testing data for accuracy and completeness is another important step in assessing the reliability of the data. Consider what data tests are needed given the information available through documentation and interviews. Data testing can provide new information about the effectiveness of information system controls. For example, testing can verify whether the data comply with stated requirements in system documentation. Data testing can be done by applying logical tests to record-level electronic data or to summary data. For record-level data, computer programs can be used to test key data elements in an entire data file. Keep in mind that testing will focus primarily on the data elements used in the audit. However, it may be useful to look at the relationships with values in other data fields for a better understanding of the data.

When using summary data, for example data presented in a publication or document, it may be useful to obtain the record-level data file that was used to generate the summary numbers. If it is not feasible for the audit team to obtain record-level data, the team should decide whether enough is known about the summary numbers to provide confidence in their reliability. Regardless of whether auditors have a record-level data file or summary data, some examination or tests of the data can be performed.

The data tests conducted will vary for each assessment and can include:

- checking total number of records provided against agency totals;
- testing for missing data, either entire missing records or missing values in key data elements;
- looking for duplicate records;
- looking for invalid or duplicate identifiers;
- testing for values outside a designated range;
- looking for dates outside valid time periods or in an illogical progression;

-
- looking for unexpected aspects of the data—for example, extremely high values associated with a certain geographic location;
 - testing relationships between data elements, such as whether data elements correctly follow a skip pattern from a questionnaire; and
 - verifying that computer processing is accurate and complete, such as testing a formula used in generating specific data elements, or testing to ensure that edit checks or validations are working correctly.

Appendix III provides additional examples of data tests.

Some testing may require a range of programming skills, from creating cross tabulations on related data elements to duplicating an automated process with more advanced programming techniques. Appropriate technical specialists can help in conducting this testing.

Tracing to and from Source Documents

In some situations, information gathered through interviews, documentation reviews, and data testing may not sufficiently resolve questions about data reliability. One method that may provide a more thorough understanding of the reliability of the data is tracing the data being used to or from source documents to compare data records and values.

When record-level data are available, tracing a sample of data records to or from source documents can help auditors determine whether the data accurately and completely reflect these documents. If auditors are particularly concerned that some records might not have been entered into the data system and that, as a result, the data are incomplete, tracing from source documents to the database can help identify any gaps. If auditors are concerned that ineligible cases have been included in the database, or that information was entered incorrectly, they can trace from the database back to source documents. Matching the data entered to or from source documents can allow auditors to quantify the magnitude of error.

Tracing a sample of data, rather than all records, reduces time and costs. Ideally, the sample should be random and large enough to estimate the error rate within reasonable levels of precision. Tracing an appropriate random sample can allow auditors to estimate the error rate and the magnitude of errors for the entire data file. It is this error rate that helps determine the data's reliability. Statisticians can help select the sampling method most suited to the audit.

In some instances, tracing to or from source documents may not be a realistic option. Source documents, separate from data entered into a system, may have been destroyed or may not exist if data were entered directly into a system. If source documents exist only in hard copy and are distributed across wide geographic areas, it may not be feasible to trace to a sample of source records. However, auditors may be able to request scanned electronic copies in this circumstance. It is also important to consider the integrity of the source documents and whether there was a possibility of alteration. In the absence of source documents, auditors may need to rely more heavily on other data testing and examination of information system controls.

Section 5: Making the Data Reliability Determination

The audit team, including any technical specialists, should utilize their professional judgment - informed by their knowledge and expertise - when making a data reliability determination.

Data reliability determinations are made in the context of the audit objectives and how the data will be used. Throughout the course of the engagement, changes in the objectives, the audit's use of the data, or the information gathered can affect the auditor's understanding of the appropriateness of using the data, as well as whether additional information is needed in order to determine data reliability. However, the final determination should only be made when the audit team has obtained enough information to determine that the data are or are not sufficiently reliable for audit purposes, or when the audit team is unable to gather information needed to make a determination. The audit team, including any technical specialists, should utilize their professional judgment - informed by their knowledge and expertise - when making a data reliability determination.

There are three possible determinations about data that can be made: (1) data are sufficiently reliable for the audit's purpose, (2) data are not sufficiently reliable for the audit's purpose, or (3) data are of undetermined reliability. A data reliability determination does not involve attesting to the overall reliability of the data or database. The audit team is only determining the reliability of the specific data needed to support the findings, conclusions, or recommendations in the context of the audit objectives. For this reason, there may be situations in which the audit team finds that some parts of the data are sufficiently reliable for the audit purpose while others are not.

Factors to Consider in the Determination

To determine whether the data are sufficiently reliable for the engagement, auditors consider all factors related to the audit as well as assessment work performed. As discussed in section 3, these factors include:

- the expected importance of the data in the final report,
- the presence of corroborating evidence,
- the risk of using the data, and
- the results of assessment work performed.

The strength of corroborating evidence and the degree of risk will affect data reliability decisions. For example, if the corroborating evidence is strong and the risk is low, the data are more likely to be considered sufficiently reliable for the audit's purposes. If the corroborating evidence is weak and the risk is high, the data are more likely to be considered not

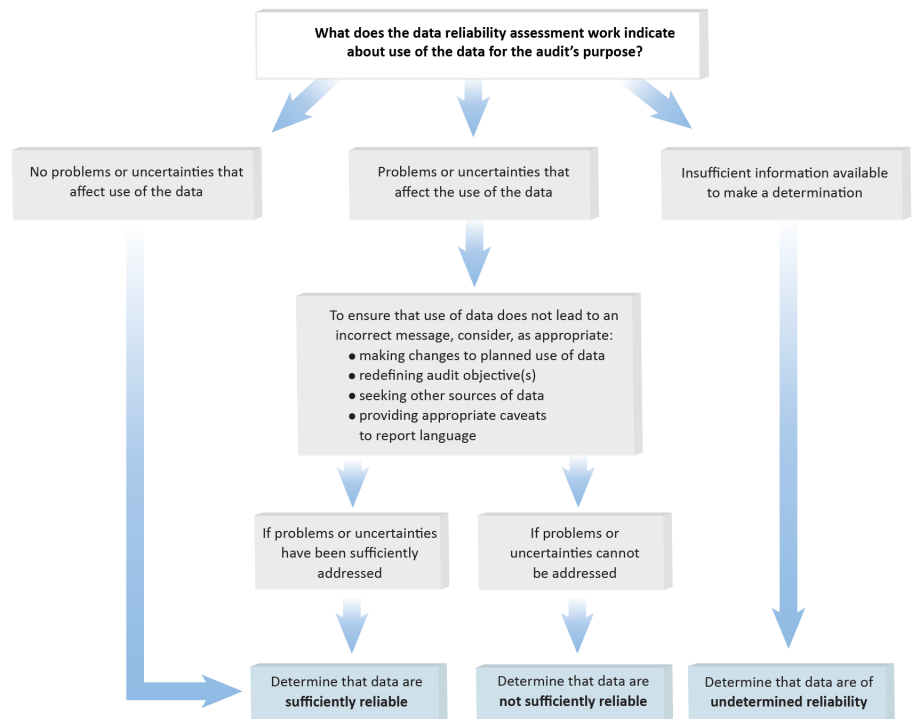
sufficiently reliable or of undetermined reliability. If data testing does not raise questions and the results are consistent with existing documentation, then the data are more likely to be sufficiently reliable for the audit's purposes.

Before making a determination about the reliability of the data for the audit's purposes, auditors should consider the results of all steps taken in conducting the assessment. They should also appropriately document and review the results, because these results provide the evidence that the data are sufficiently reliable (or not) for the purposes of the audit. The audit team may decide that further steps are needed to come to a conclusion about the reliability of the data for audit purposes.

Outcomes to Consider in the Assessment

Data reliability assessments result in one of three possible determinations of reliability for the audit's purpose: sufficiently reliable, not sufficiently reliable, or undetermined reliability. An overview of the determination process is illustrated in figure 4 and described in more detail below.

Figure 4: Making the Data Reliability Determination



Source: GAO. | GAO-20-283G

Sufficiently Reliable Data

The audit team can consider the data sufficiently reliable when the results of work performed for the data reliability assessment (including from interviews, documentation reviews, data testing, and/or tracing to or from source documents) provide assurance that (1) the level of errors or incomplete data is acceptable given the audit objectives, and (2) using the data is not expected to lead to an incorrect or unintended message.

Data may be acceptable if, for example, the audit team identifies some concerns with the data, but the issues found are not material relative to the audit objectives and intended use of the data.

When the assessment does identify data issues with the potential to lead to an incorrect message, there are additional options which may allow for at least limited use of the data. These include:

- changing the planned use of the data;
- reporting results in a way that adjusts for limitations by including qualifiers or other language that reduces the precision of reported data (e.g., text like “about 100,000 students” or “at least \$430,000 in spending”; or presenting data graphically to provide a sense of scale without reporting exact numbers);
- providing caveats to report language to describe the limitations to the data and their potential effect on the message (e.g., descriptions in text or footnote about limitations);
- making corrections to the data after consulting with the owners or source of the data; and
- making changes to the audit objective to reflect an appropriate use of the data.

Not Sufficiently Reliable Data

The audit team can determine the data to be not sufficiently reliable for the audit objectives when the results of assessment work indicate that either (1) the level of errors or incomplete data in some of or all of the key data elements is not acceptable given the audit objectives, or (2) using the data would likely lead to an incorrect or unintended message.

When the data are deemed not sufficiently reliable, auditors can seek evidence from other sources, including alternative data - the reliability of which will also need to be assessed - or other information, such as from surveys, case studies, or expert interviews.

If the audit team is unable to identify alternative information that is sufficiently reliable, they should inform the requester that data necessary to respond to the request are unavailable and consider further steps, such as:

- redefining the audit objective to eliminate the need to use the data,
- changing the audit objective to include evaluation of the quality of the data, or
- ending the audit.

The audit team, not the requester, is responsible for deciding what data to use. Although the requester may want information based on insufficiently reliable data, auditors are responsible for ensuring that data are reliable and used appropriately. The audit team should consult with the auditing organization's management before agreeing to use data that are not sufficiently reliable. If the audit team, in consultation with appropriate management, decides that there is a compelling reason to use the data despite problems that have been identified, auditors should make the limitations of the data clear to avoid incorrect or unintentional conclusions.

When a data reliability assessment identifies significant and systematic issues with data that are owned by an audited agency, it may be appropriate to consider recommending changes to the data or data system.¹³ Consider further investigating data reliability issues when there is a strong likelihood that the identified data issues could, for example:

- materially change publicly disseminated agency information;
- materially change organizational decisions where the organization uses these data;
- materially misrepresent an agency's program or an organization's operational inputs, clients, or outcomes;
- call into question whether the entity was in compliance with federal laws or regulations; or
- undermine internal controls over high-risk operations or financial resources.

¹³In some cases, data owner policies and procedures or *Standards for Internal Control in the Federal Government* can be used as criteria for a finding on the reliability of agency data; see [GAO-14-704G](#).

In these cases, it may also be appropriate to report examples of the data, in order to illustrate the unreliability of the data.

When the types of data reliability issues described above are present, auditors may consider making a recommendation that addresses the data problems or issuing a management letter to the audited organization. A management letter can address management or operational issues that are beyond the substance of the audit.

However, if the data reliability issues result from the auditor's attempt to use the data for purposes other than those for which the organization collects them and the data issues do not result in a situation such as those outlined above, then a recommendation to the audited agency will likely not be warranted. One exception to this is a situation in which the auditor can make a strong case that the data should be sufficiently reliable for the use the auditor intended. For example, a strong case might be that these data are essential to documenting a condition critical to effective decisions or operations when an agency is not currently using these data for that purpose.

Data of Undetermined Reliability

When the audit team's review of the information collected, and any data testing, raises questions about the data's reliability that cannot be resolved, or when too little information is available to judge the reliability of the data, the audit team may conclude that the data are of undetermined reliability.

Data may be of undetermined reliability if specific factors are present, including:

- limited or no access to the data source,
- presence of a wide range of data that cannot be examined with current resources,
- data limitations that prevent an adequate assessment,
- the deletion of original computer files, or
- a lack of access to needed documents.

For example, there may be limited or no access to information about the data source. This is particularly likely when the data are produced by international agencies, other countries, or private organizations, or when there are privacy or security concerns with the data. It can occur when

there is no audit authority to ask for more information or when insufficient information exists in the form of source documents or documentation about the data. In such cases, auditors should nevertheless attempt to gather as much information as possible, for example, by contacting data owners or users, identifying research that has used the data, or by looking for corroborating evidence. However, when such steps have been taken and information continues to be unavailable, it may be appropriate for the audit team to decide that the data are of undetermined reliability.

Alternatively, data may have been gathered from a large number of organizations (e.g., using a survey of 50 states), making it difficult to examine the reliability of each submission. Organizations, such as state governments, often collect and report information differently. In this situation, before deciding that data are of undetermined reliability, the audit team can assess the overall reliability of the information by, for example, asking high level questions of all the states to identify potential issues or substantive differences in data collection that would affect the ability of the auditor to aggregate data in a reliable manner. See section 7 for more information about collecting data through surveys.

Data limitations may also be a reason to decide that data are of undetermined reliability. For example, the reliability of financial data that are self-reported by other countries, affected by differences in exchange rates, and based on varying definitions may be in question. In this case, a lack of further access to information from the countries may necessitate a determination of undetermined reliability.

Inadequate planning earlier in the engagement is not a sufficient reason to use data of undetermined reliability, particularly if the data are being used as key evidence. To minimize last-minute challenges, auditors should address data reliability issues in the planning phase of engagements, set realistic commitment dates, and be prepared to ask for more time to assess data that arrives later than expected.

When the audit team decides that the data are of undetermined reliability and the data are needed to address the audit objective, they should inform the audit's requester that they are unable to identify data that are sufficiently reliable. Although the requester may want information based on data of undetermined reliability, auditors are responsible for ensuring that reliable data are used. The audit team should consult with the auditing organization's management before agreeing to use data of undetermined reliability. If the audit team, in consultation with appropriate management, decides that there is a compelling reason to use the data,

auditors should make the limitations of the data clear, so that incorrect or unintentional conclusions will not be drawn.

Section 6: Including Appropriate Language in the Report

A description of the data reliability assessment and determination is an important part of describing the appropriateness of evidence used in the audit. To comply with GAGAS, auditors should include a description of the assessment and determination in the methodology section and any applicable context within the text about the specific data reported.

Stating the specific purpose associated with the determination can help the reader to better understand how the audit team determined the data can or cannot be used.

GAGAS emphasizes the importance of using appropriate data. The audit team conforms to GAGAS with respect to data reliability by describing (1) the steps taken to assess the data, (2) any relevant data concerns, and (3) their judgment about the reliability of the data for the audit's purpose. In the methodology section of the report, the audit team should describe its assessment of data reliability and the basis for its determination. The language in this description will depend on whether the data are sufficiently reliable, not sufficiently reliable, or of undetermined reliability given the audit's purpose. Stating the specific purpose associated with the determination can help the reader to better understand how the audit team determined the data can or cannot be used.

It may also be appropriate to discuss the reliability of the data in other sections of the report. This is important when presentation of the data without related reliability information could lead to misinterpretation of the results or findings. Additional context may be placed in the body of the report, in a footnote, or in a note to a table or figure containing the data. For example, a table note could include a discussion of the extent of missing data and the possible effects on results. Text in the body might include a general discussion of errors in the data and their potential impact on the accuracy and precision of statistics. In addition, reported results may be worded in a less precise way to adjust for limitations in the data. Any context provided should be commensurate with how the data are used in the report. When data present more risk, either because of how they are used or the type of limitations identified, it may be appropriate to make any contextual information more prominent in the report.

(See appendix IV for examples of reporting language.)

Sufficiently Reliable Data

When describing the assessment of data appearing in the report, audit teams should present the basis for determining that the data are sufficiently reliable, given the research questions and intended use of the data, including:

-
- an explanation of the steps in the assessment;
 - a description of any corrections made to the data; and
 - a description of any data limitations, which could include an explanation of why using the data does not lead to an incorrect or unintentional message, how limitations could affect interpretation of the message, and why any data limitations are minor in the context of the engagement.

Not Sufficiently Reliable Data

When there is a reason to refer in the report to data that were determined to be not sufficiently reliable, audit teams should present the basis for determining that the data are not sufficiently reliable, given the research questions and intended use of the data. This presentation includes:

- an explanation of the steps in the assessment;
- a description of the problems with the data;
- an explanation of why the data problems have the potential to lead to an incorrect or unintentional message; and
- a statement that the report contains a conclusion or recommendation that is supported by evidence other than these data, where applicable.

Finally, if the data are not sufficiently reliable, auditors may consider whether to include this as a finding in the report and recommend that the audited organization take corrective action (see section 5 for factors to consider and possible follow-up actions).

Data of Undetermined Reliability

When the audit team has decided, in consultation with appropriate management, to use data of undetermined reliability in the report, the audit team should present the basis for determining that the data are of undetermined reliability given the research questions and intended use of the data. This presentation should include an explanation of the steps in the assessment and the reasons for the determination, for example, the deletion of original computer files, data limitations that prevent an adequate assessment, or the lack of access to the data source or to needed documents.

Further, if the audit team in consultation with the auditing organization's management has decided to use data of undetermined reliability, the team needs to explain the rationale for using the data despite this determination. This may include that the data are supported by credible corroborating evidence, are widely used by outside experts or

policymakers, or are used as a general indicator and not to support specific findings. In addition, auditors should clearly describe the limitations of the data so that incorrect or unintentional conclusions will not be drawn from them. For example, auditors can indicate how using these data could lead to an incorrect or unintentional message. Finally, if the report contains a conclusion or recommendation that is supported by evidence other than the data of undetermined reliability, it may be useful for the report to include a statement explaining this.

Section 7: Additional Considerations

This section contains additional topics that are helpful for auditors to be familiar with when conducting a data reliability assessment.

Documenting the Assessment

All work performed as part of a data reliability assessment should be documented in a manner consistent with the audit organization's usual standards for evidence. Required documentation includes a plan for steps the audit team will take in the assessment, as well as analysis of and the results from all testing, documentation review, and interviews related to the data reliability assessment. In addition, decisions made during the assessment, including the final determination of whether the data are sufficiently reliable for the audit's purposes, should be summarized in the documentation. The documentation should be clear about what steps the audit team took and what conclusions they reached. Use of a standardized template for recording all documentation related to the data reliability assessment can help improve consistency of assessments within the audit organization.

Planning the Assessment

Early examination of data reliability helps the team to determine whether the data are appropriate for addressing the audit objectives.

Data reliability assessments are best initiated as early as possible in an audit. Early examination of data reliability helps the team determine whether the data are appropriate for addressing the audit objectives. The audit plan should discuss how data reliability will be assessed, any limitations that may exist because of shortcomings in the data, and any additional steps that still need to be taken. Before finalizing the audit plan, the audit team usually takes initial steps to test the data and review existing information about the data and the system that produces them. To minimize last-minute challenges, auditors should address data reliability issues in the planning phase of engagements, set realistic commitment dates, and be prepared to ask for more time to assess data if it arrives later than expected.

Working within Short Timeframes

In some instances, an audit may need to be completed in a very short period of time for reasons outside of the control of the audit team. When this is the case, data reliability assessment tasks will likely need to be condensed. However, the risks of using unreliable data should be minimized, and there may still be time to, at a minimum, review existing information and test data that are critical for answering a research question. Thoughtful consideration of the potential sources of error, and how they might affect audit findings, is particularly important when working under short time frames because it allows the audit team to focus

their assessment effort on aspects of the data that present the greatest risk.

Examples of information collection steps that can typically be performed quickly include questioning knowledgeable agency staff about the reliability of the data and reviewing existing GAO or Inspector General reports to quickly gather information about data reliability issues. In addition, critical data elements can generally be tested electronically for obvious errors of completeness and accuracy in a short time. From that review and testing, auditors can make a more informed determination about whether the data are sufficiently reliable for the specific purpose of the audit, what caveats may be necessary, and whether further investigation is needed.

Level of Detail of the Data

While the reliability of data supporting audit findings should be assessed regardless of the level (i.e., record or summary) at which it is analyzed and reported, there are some differences in how these two types of data are assessed. Record-level data are those that provide detailed information at the “case” or “record” level, while summary-level data have been categorized or summarized at a higher level of detail. Record-level data enable more opportunities to analyze data and assess reliability because they provide the auditor with more information with which to evaluate accuracy and completeness.

Use of summary-level data still requires a data reliability assessment, but testing and understanding of the data may be more limited, because the process of aggregating the records reduces the amount of information that can be examined. It will be important to understand any process used for summarizing or extracting the data. Depending on the importance of the data to the report’s message and whether there are complexities that may impact the accurate extraction of the data, whether record or summary-level, the audit team may need to request the computer code or queries used to obtain the data. Reviewing the code used to extract records allows auditors to see whether the correct criteria were used when providing records or summarizing data, and therefore that the data provided are consistent with the information needed for the audit. In most circumstances, while it may require more time and resources, obtaining record-level rather than summary-level data provides the audit team with more options in assessing the reliability of, and reporting, the data,

For example, auditors might be reviewing the timeliness of agency decisions for a certain program. Obtaining detailed data for all decisions

as opposed to only reviewing aggregate or summary data might allow the audit team to:

- report timeliness data at the national, regional, and field office levels;
- check to see if important information is missing or whether duplicate records are in the file;
- use beginning and ending dates to determine whether the agency was calculating timeliness accurately;
- take advantage of greater reporting flexibility to present data in a variety of ways; and
- have more opportunities to find data problems which could lead to a recommendation.

Combining Data from Different Datasets

Sometimes an audit plan or objectives call for combining or linking data from more than one dataset by, for example, using a unique identifier. This raises additional considerations related to data analysis and reliability. In order to combine data, auditors need to consider issues such as differing timeframes or geographic locations covered by the datasets, the meanings of variables and values and whether there are differences between datasets, the population covered, the unit of measurement (e.g., person or household), the frequency of data entry or data availability, and the level and nature of missing data. The extent to which the datasets can be appropriately linked affects decisions about reliability for the audit purpose. Linking datasets also requires consideration of the quality and accuracy of the match, including examination of the extent that records do not match or the possibility that records have been erroneously linked. Further, each dataset may individually have an acceptable level of error, but when combined, these errors may rise to a level deemed unacceptable for audit purposes.

Assessing the Reliability of Data Auditors Collect through Surveys

Sometimes, as part of a survey, auditors request aggregate or summary data in addition to or in place of questions asking for respondent perspectives. Because the data requested comes from many different sources, or respondents, it may not be feasible to conduct the level of data reliability assessment work usually conducted for an audit. However, auditors need to determine that the data are appropriate for their use and can seek ways to validate the data provided in survey responses.

For example, auditors can consider:

-
- including survey questions about topics such as the source of the data, whether the data are precise numbers or estimates, the owner's confidence in the accuracy of the data, or the definitions of included data fields;
 - requesting documentation on the data from some or all survey respondents;
 - asking more in depth questions of selected survey respondents before (e.g., during pretesting) or after fielding the survey;
 - conducting logic checks on survey responses to identify unexpected or out of range values; and
 - comparing survey responses to other sources of data or benchmarks.

One challenge that can arise from data collected through surveys is meaningful differences in data collection practices among the sources, or respondents. To identify such differences, it may be appropriate to ask questions about how the data are collected and calculated to ensure the audit team has full information about the data being used. Because the survey data will often be reported in aggregate (or at least presented together), differences in data collection practices among the surveyed respondents can create enough inconsistency that aggregating responses across respondents may not result in reliable information.

Appendix I: Example Documentation Requests and Interview Questions

This appendix provides example documentation requests and interview questions. Many of these examples will not be applicable to all datasets or audit needs. Auditors, in collaboration with technical specialists, as appropriate, should use their professional judgment to select or modify items depending on the relevance of the data to the audit objectives, and the specific data elements to be analyzed. Examples can also be modified to be applicable to spreadsheets or data extracts, as well as data systems. Data reliability assessment is often an iterative process, requiring some revisiting of issues as they arise in documentation reviews, interviews, electronic testing, and data analysis.

In developing interview questions or a documentation request, auditors can incorporate the questions or documents from below that are relevant for the assessment. The following language, specifying the purpose of the request and data to be used, may be used or adapted to start an interview or information request:

We are conducting a review of _____. In this review, we plan to use data from your agency's _____ database (or _____ program). To ensure that we are presenting the data correctly and that any conclusions we draw based on the data are warranted, we need to understand how the data were collected, maintained, analyzed, and presented. Therefore, we would like to ask you questions about the data and the information system that produces the data. The data fields we are interested in using are _____ for the purpose of _____.

Examples of Data Documentation to Request

Data documentation can provide detailed information about the characteristics of a dataset and its quality control features. Obtaining and reviewing data documentation, prior to interviewing individuals responsible for and familiar with the data, can help inform discussions. In addition to documentation requested from the data owner, some documentation may be available on the Internet or from prior engagements. Such documentation may include:

- information on a system's purpose and structure, such as user manuals, system flow charts, or design specifications;
- written policies and procedures for data entry, maintenance, and validation;
- information on data elements (or fields), their definitions, descriptions, codes, and values (e.g., a data dictionary);

- information about the data file, such as record counts, range of values, and frequencies of responses;
- training materials for data system users (including, as applicable, documentation showing that training was provided to users);
- financial statement audit reports (for data from financial systems);
- published reports that have used the data and can provide a comparison to audit results;
- the survey instrument or other data collection form used to collect the data (if applicable);
- and reviews of data quality, including:
 - Inspector General or internal audit reports;
 - internal reviews and studies;
 - contractor or consultant studies;
 - reports of congressional hearings or copies of congressional testimony related to the data; and
 - summaries of ongoing or planned audits, reviews, or studies of the system or data.

When using data from statistical databases or other data collected using sample-based surveys, additional information may be needed on topics such as:

- population definition;
- sample design;
- description of data editing procedures, including any imputation;
- impact of imputation;
- unit and item nonresponse rates;
- non-sampling error;
- comparability with related data; and
- limitations obtained from users.

For established systems, this information may be publicly available from the source.

Example Questions for Data Owners

Auditors can ask data owners, in an interview or written request, some of the following questions if they are relevant given the audit objectives and the nature of the data being used. The questions can also be rewritten or modified to meet audit objectives. In asking these questions, the auditor is looking for information on the characteristics, quality controls, and limitations of the data rather than simply looking for confirmation that the data are reliable. While the questions are written to be answered by data owners, auditors may be able to obtain needed information through review of data documentation.

Auditors must use their professional judgment to make the assessment, and should consider aspects of data collection that might lead to unintentional bias, such as employee incentives or performance measures that could affect data entry or maintenance practices. For many of the questions below, the auditor can consider whether to ask for documentation that verifies the data owner's response.

Example Questions about the Data System and Its Users

Note: data system "users" in this section can refer to staff that enter, review, and conduct other quality control procedures on the data and staff that analyze the data.

When was the data system created, and what is its purpose?

How does the data owner use the data?

Who are the data system's primary users? How do users access the system?

Who has access to enter or update the data? Are there different "levels" of access to the data?

What, if any, training is provided to system users? Is training made available to all users?

Have there been any changes to the data system (e.g., major system upgrades, changes to new vendors) that would affect the consistency of data during the time period requested?

Example Questions about Data Collection

How and where are data collected (e.g., manual data entry, form completed by agency representative, entry by entities outside the data owner)? Who is responsible for data entry?

How current are the data? How frequently are data entered?

What instructions does the data owner provide for data entry, particularly for data fields that are open-ended or otherwise subject to variation in user input?

What is known about the consistency of data entry across staff, offices, or other units?

If data are produced by aggregating across units (e.g., states, organizations), are there differences in how the units collect or calculate the data that might result in inconsistencies within the data once aggregated?

Are data entries subject to change in the future, either because of quality reviews or other procedures?

What unit of analysis does each record in the data represent (e.g., an individual, event, household)?

What is the structure of the data system? Are data maintained in a “flat file” or is the data system relational/hierarchical? If the data are relational, what unique identifier(s) are used to link the tables?

Are any data (either records or fields) in this dataset fed in from other data systems?

If any of these data are fed in from another data system, what quality control features are in place to ensure that data are read in accurately and completely?

Are any new variables created by recoding existing variables or calculated based on values for existing variables (e.g., calculation of number of days between recorded dates or creation of variable based on age ranges)? Does data system documentation explain how new variables are created or calculated?

What modifications, if any, are made to data values in order to protect confidentiality or for other purposes?

Do any variables use categorizations developed by another organization (e.g., categories of industry type or race)?

Have there been changes to any procedures - including how a data element is defined, entered, or maintained - over the period of time for which data are requested (e.g., changes to populations or geographic areas, variable definitions, variable values or categories, data entry instructions, available drop down values)?

If there have been changes to procedures within the time period for which data are requested, what steps have been taken to ensure the accuracy and consistency of the data?

Example Questions about
Quality Control Features

What procedures ensure that the data system consistently captures all data occurrences (records, observations) and all data elements?

What procedures are in place to prevent duplicate records from being created in the data?

Does the system have any edit checks or controls to help ensure that the data are entered accurately?

Are there electronic safeguards, such as error messages for out-of-range entries or inconsistent entries?

Does someone review all, or a sample of, data entries to ensure that key fields are accurate and non-duplicative? If reviews take place, how frequently do they occur?

What process, if any, is used to track and oversee changes made to the data?

Does the data system maintain a history of the changes made to the data or is historical information overwritten when new data are entered?

(If data are contained in a spreadsheet) What procedures are in place to ensure that data are not inadvertently changed or deleted? Are any formulas in the spreadsheet reviewed for accuracy?

What are the procedures for follow-up if errors are found, and who is responsible for correcting them?

Example Questions about Prior
Reviews of Data Quality

To the extent you have previously identified errors in relevant data fields, what were the reasons for the errors and have these issues been addressed?

Do systematic reviews or exception reports examine accuracy and present error rates? How frequently?

If studies or evaluations of the system have been conducted, what were the results and how did you address any issues?

If applicable, do external users of the data or individuals who are the subject of data records have the opportunity to review and provide feedback on the accuracy of data?

Example Questions on Data
Owner's Assessment of Data
Quality

What is your opinion of the quality of the data, specifically its completeness and accuracy?

Are there any data limitations such as data elements that are often incomplete or incorrect? How would those limitations affect the intended use of the data?

Are there concerns about timeliness or usability of the data?

Are there any purposes for which the data should not be used?

Have any corrective actions been taken to improve the quality of the data?

Appendix II: Assessing the Reliability of Data from Statistical Agencies

Data collected and published by federal government statistical agencies constitute a large portion of the available information about the U.S. economy, population, natural resources, environment, and public and private institutions. Standards and guidelines governing federal statistical agencies are intended to ensure that their surveys and studies are designed and administered to produce reliable data as efficiently as possible and that their methods are documented and results presented in a manner that makes the data as accessible and useful as possible.¹

Although data that federal statistical agencies collect are generally reliable for their purposes, auditors must still assess and document whether these data are sufficiently reliable for the audit purpose. For example:

Census data may measure how many natural-born children are living with parents in the United States, but these data are not reliable for determining the total number of natural-born children in the United States, because some children may not be living with their parents.

An audit team may want to use Current Population Survey data to determine the proportion of law enforcement officers who are Asian. Because this information is at the intersection of two separate subpopulations—race and occupation—the number of people may be too small to be reliable because of the sampling design used to collect these data.

Consider these kinds of data reliability issues when planning to use federal statistical agency data.

In most cases, federal statistical agencies have information on their statistical collection procedures and methods readily available on the Internet. Often, this published information serves as much of the documentation the audit team will need to review in conducting a data reliability assessment.

Auditors can look for the following types of documentation though not all will be applicable to a given database:

- Survey development descriptions

¹In addition to statistical surveys, the federal agencies may collect a large amount of administrative data, which are not subject to these survey standards.

- Data collection details
- Sample design
- Data dictionaries or other documentation about variables in the dataset
- Descriptions of processing and editing of data
- Details about the production of estimates and projections
- Data analysis discussions
- Reviews of procedures
- Reporting of response rates
- Discussion of limitations
- Discussion about the dissemination of the data

When there is a lack of needed information in available documentation, other steps, such as interviews and electronic testing of the data, may provide the needed additional information to determine the reliability of the data.

Appendix III: Examples of Data Tests

This appendix includes a variety of possible data tests, some of which may not be applicable to every audit. Many of these tests can be performed using statistical software programs, spreadsheet functions, or manually and are best conducted when informed by the topic area knowledge of the audit team. Results of these data tests could be indications of problems in the data, but consultation with the data owner or agency may reveal reasonable explanations. For example, there may be a change in data element definition over time, which may not be a data deficiency, but could affect time trends or comparisons. Further, depending on the audit purpose, some degree of error may be acceptable. For example, auditors will need to consider the amount of missing data or values out of range and determine whether it substantially undermines the message.

Tests of whether expected data were received

- For any data extract provided, request programming or query code in order to compare to request criteria and ensure appropriate interpretation of request
- Compare total number of records provided to agency totals
- Compare expected record lengths to the actual record lengths
- Compare data elements provided to those listed in data dictionary
- Check whether there are field names that need to be explained or defined
- Check for truncation of data fields or presence of hidden characters
- Check for uneven columns or rows that may indicate a problem with data import
- Check that certain variable formats are correct and consistent (e.g., dates, unique identifiers, abbreviations)

Tests that may indicate data reliability issues

- Check for duplicate records
- Check for invalid or duplicate identifiers
- Check for missing data, either entire missing records or missing values in key data elements
- Check for values outside a designated range (e.g., calculation of maximums and minimums, including negative numbers)
- Check for values that are meaningful or correspond to expected values
- Check for dates outside valid time periods
- Check for dates in an illogical progression

- If data are continuous, check for data gaps (e.g., dates or months that appear to be missing)
- Verify that any computer processing or calculations are accurate and complete, for example:
 - verify a formula used to generate specific data elements
 - test to ensure that edit checks or validations are working correctly
- Examine relationships between data elements, for example:
 - cross tabulations (e.g., does an analysis of type of crops grown by state correspond with expectations?)
 - whether data elements appropriately follow a skip pattern from a questionnaire
- Examine trends in the data over time, for example:
 - whether there are unexpected spikes or dips that could indicate duplicate or missing records
 - whether there are expected or unexpected seasonal changes
- When linking data from different tables:
 - check whether the unique field(s) used to link the tables have the same format and length
 - check whether a record in one table has only one unique match in another (a one-to-one match), whether a record in one table matches to multiple records in another (a one-to-many match), or whether multiple records match to multiple records (a many-to-many match)
 - check for records in a table that do not match to any records in other tables

Remember that it can be easy to miss potential concerns identified in data reliability test output. The following may help draw attention to such concerns in the output:

- Use automated highlighting to indicate potential concerns (e.g., values outside a designated range, missing values, or percentages over a certain threshold)
- Format reliability test output to enhance readability (e.g., carefully label titles, use comments to emphasize important table content or explanation of what results suggest a problem)
- Output examples of data or testing results to illustrate potential concerns
- Separate reliability test output from other output

Source: GAO. | GAO-20-283G

Appendix IV: Example Language for Reporting on Data Reliability

This appendix provides example language for reporting on data reliability assessments. A description of the data reliability assessment and determination is an important part of describing the appropriateness of evidence used in the audit. To comply with generally accepted government auditing standards (GAGAS) auditors include a description of the assessment and determination in the methodology section and any applicable context within the text about the specific data reported.

General Reporting Language Examples

Example 1:

We assessed the reliability of _____ data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Example 2:

We assessed the reliability of _____ data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. In addition, we traced a statistically random sample of data to source documents (see appendix X for details). We determined that the data were sufficiently reliable for the purposes of responding to our objectives.

Example 3:

To assess the reliability of _____'s data, we (1) performed electronic testing for obvious errors in accuracy and completeness; (2) reviewed related documentation, including contractor audit reports on data verification; and (3) worked closely with agency officials to identify any data problems. When we found discrepancies (such as missing data, duplicate records, or data entry errors), we brought them to _____'s attention and worked with _____ to correct the discrepancies before conducting our analyses. We determined that the data were sufficiently reliable for the purpose of describing _____ (e.g., general trends in the population, the minimum amount of money spent on...).

Example 4:

To assess the reliability of the data elements needed to answer the audit objectives, we (1) performed electronic testing, (2) reviewed related documentation, and (3) interviewed agency officials knowledgeable about the data. The results of our electronic testing showed that data elements key to our review contained high percentages of missing data. (See appendix X for further details.) Therefore, we determined that the data were not sufficiently reliable for the purposes of this report. To answer the research question, we....

Examples Adapted from GAO Reports

Sufficiently Reliable for Audit Purpose with No or Few Caveats

GAO, SOCIAL SECURITY DISABILITY: Additional Measures and Evaluation Needed to Enhance Accuracy and Consistency of Hearings, [GAO-18-37](#) (Washington, D.C.: December 2017).

Examined statistical program code used by agency to pull data

From Objectives, Scope, and Methodology: [Social Security Administration] constructed custom files for GAO from several SSA datasets in response to our data requests. We assessed the reliability of the data used in our analyses through electronic testing, analyzing related database documentation, examining the SAS code used by SSA to construct the custom files, and working with agency officials to reconcile discrepancies between the data and documentation that we received. We determined that the 831, Structured Data Repository, and CPMS data on ALJ decisions and claimant characteristics and the FPPS data on ALJ appointments were sufficiently reliable for the purposes of describing the extent of variation in the outcomes of ALJ decisions. We also determined that SSA's data on pending caseloads and ALJ and decision writer staffing, by year and hearing office, were sufficiently reliable for the purpose of describing hearing office characteristics.

Worked with agency to reconcile discrepancies

Specific purpose for use of data stated

GAO, HIGHER EDUCATION: Education Should Address Oversight and Communication Gaps in Its Monitoring of the Financial Condition of Schools, [GAO-17-555](#) (Washington, D.C.: August 2017).

From Objectives, Scope, and Methodology: We also analyzed Education data on schools that were required to provide a letter of credit to the department due to financial concerns for school years 2010-11 through 2013-14, the most recent year of data available. We assessed the

Traced sample of records to source documents

reliability of these data by reviewing Education’s data systems and documentation, tracing 40 randomly drawn records back to the source documents, and interviewing Education officials, and we determined that the data were sufficiently reliable for our reporting purposes.

Compared against news reports to assess completeness

To assess the effectiveness of Education’s oversight, we analyzed 10 years of Education’s data on school closures from school year 2006-07 to 2015-16, with more detailed analysis of closures since school year 2010-2011. We assessed the reliability of these data by reviewing Education’s data system and checking the data for completeness against news reports of school closures, and we determined that the data were sufficiently reliable for our reporting purposes.

GAO, *FOSTER CARE: States with Approval to Extend Care Provide Independent Living Options for Youth up to Age 21*, [GAO-19-411](#) (Washington, D.C.: May 2019).

Assessed the reliability of data obtained through a survey

From Objectives, Scope, and Methodology: To address each research question, we designed and administered an electronic survey of state child welfare agencies in the 26 states approved by HHS to offer federally funded extended care as of February 2018. The survey was conducted between August and October 2018 and we obtained a 100 percent response rate. The survey included open-ended and closed-ended questions about states’ policies and practices regarding supervised independent living arrangements, states’ data on youth in extended care and in supervised independent living, state spending and funding sources for these living arrangements in state fiscal year 2017, as well as questions about data reliability. We also analyzed states’ responses on the number of youth in extended care and the number of youth in care that were eligible for title IV-E reimbursement in state fiscal year 2017 to determine their title IV-E eligibility rate for the fiscal year.

To ensure the quality and reliability of the survey, we pretested the questionnaire with three extended-care states that vary in geographic location and numbers of youth in care, among other factors. We conducted the pretests to check (1) the clarity and flow of the questions, (2) the appropriateness of the terminology used, (3) if the information could be easily obtained and whether there were concerns about the reliability of data that would be collected, and (4) if the survey was comprehensive and unbiased. We revised the questionnaire based on the pretests. We reviewed responses to assess if they were consistent and contained all relevant information, and followed up as necessary to determine that states’ responses were complete, reasonable, and

Sufficiently Reliable for Some Purposes, with Caveats or Data-related Findings

Data determined to be sufficiently reliable for one purpose but not another

sufficiently reliable for the purposes of this report; we excluded data where we had concerns about their reliability.

GAO, TOBACCO TRADE: Duty-Free Cigarettes Sold in Unlimited Quantities on the U.S.-Mexico Border Pose Customs Challenges, GAO-18-21 (Washington, D.C.: October 2017).

From Objectives, Scope, and Methodology: To describe how duty-free cigarettes are sold and exported and how duty-free stores report data, we analyzed Automated Export System (AES) data from Census for 2010 through 2015 on recorded transactions at the 88 duty-free stores CBP identified as being adjacent to the U.S.-Mexico border, also referred to as the southwest border, spanning Texas, New Mexico, Arizona, and California. We determined that data were sufficiently reliable to review filing practices with respect to duty-free cigarette transactions. We determined that value and quantity data for those transactions were not reliable for the purposes of this report due to unexplained variations in the calculated prices; we based our assessment on a review of related documentation and on interviews with Census officials about the agency's procedures to ensure the quality of the data and interviews with CBP officials to discuss relevant aspects of how transaction data might be entered in AES. See appendix I for more details on our scope and methodology and appendix II for our assessment of AES data reliability.

From findings: The export information includes 28 mandatory data elements such as the value, quantity, name of exporter, name of the person receiving the shipment, and method of transportation. AES data from Census showed a total of 18,504 such transactions from 2010 through 2015 from duty-free stores on the southwest border, with almost 70 percent exported from Texas.¹

Findings included footnote about reliability of data

Footnote 1: We tested these data and found that the unprocessed, transaction-level AES data on duty-free cigarettes for 2010 through 2015 are not reliable for use in describing the value and quantity of duty-free cigarettes sold over time in the U.S. states bordering Mexico. For more information on the steps we took to assess the reliability of these data, please see app. II.

From findings: According to CBP, in many cases duty-free stores on the southwest border are filing some noncompliant information that they are required to report on cigarette exports valued at more than \$2,500. Our analysis of export data from Census also showed that many transactions include some noncompliant information.²

Findings distinguish between data that were sufficiently reliable and data that were not

Footnote 2: We determined that data were sufficiently reliable to review filing practices with respect to duty-free cigarette transactions. We determined other AES data, including value and quantity of export, to not be reliable for reporting purposes. See app. II for more information.

Included appendix to describe data reliability assessment

From appendix II: Our testing found that the unprocessed transaction-level AES data on duty-free cigarettes for 2010 through 2015 are not reliable for use in describing the value and quantity of duty-free cigarettes, and associated trends, exported from the southwest border....

Provided details of data testing

To examine the data on value and quantity, we evaluated the reasonableness of the ratio of these variables, the unit price (value divided by quantity), and the consistency and stability of reported prices. We found that many of these transactions' reported unit prices are far below reasonable price levels....

We also found high levels of reported price variation in the data, with reported median unit sales prices frequently doubling or halving from year to year, even within the same port location.

GAO, VETERANS AFFAIRS CONTRACTING: Improvements in Policies and Processes Could Yield Cost Savings and Efficiency, GAO-16-810 (Washington, D.C.: September 2016).

From Objectives, Scope, and Methodology: To assess the extent to which Department of Veterans Affairs (VA) data systems accurately reflect VA procurement spending for fiscal years 2013 through 2015, we obtained data on VA contract spending from fiscal years 2013 through 2015 from VA's Electronic Contract Management System (eCMS). We used eCMS as our main source of information because it is intended to be the official repository for VA procurement information and contains fields, such as the responsible contracting office and obligation amount, relevant to our review. While we found errors and missing data in eCMS, we determined that the data were sufficiently reliable for the purposes of our reporting objectives. We made this determination by conducting our own testing of the data for consistency, including matching it against Federal Procurement Data System-Next Generation (FPDS-NG) data for the same period, which we found sufficiently reliable for our purposes. This comparison matched individual contract numbers across the two databases, and, although it found a large gap in total obligations, it indicated that the gap was due almost exclusively to obligations under the pharmaceutical prime vendor program. We also compared entries in certain data fields to information in contract files for the 37 contracts and

Compared values against other electronic data

Traced sample of records to source documents

19 task orders we selected for review and found that data on extent of competition was generally accurate. Finally, we discussed the accuracy and completeness of the data with contracting office managers, system administrators, and other VA officials who work with eCMS, and gathered information on internal controls used to ensure the reliability of the data.

Header in findings: Available Data Are Incomplete but Indicate That VA Obligated Nearly \$46 Billion from Fiscal Years 2013 to 2015

Findings and recommendation about data

From findings: Our analysis of the available eCMS data found that VA obligated about \$46 billion on goods and services via contracts in fiscal years 2013 through 2015; however, the data are incomplete. VHA accounted for 62 percent of these obligations during fiscal years 2013 through 2015. While eCMS—VA’s central repository for all contract actions and supporting documentation—provides useful data on VA contracting, we found that data on high-tech medical equipment and prime vendor orders were not complete, leading eCMS to reflect much lower total obligations than FPDS-NG. While we determined that the available data were sufficiently reliable for describing certain characteristics of VA contract obligations over this period, we found that shortcomings limit its usefulness.

Data determined to be sufficiently reliable for one purpose but not others

Recommendation: In order to ensure that VA’s procurement data is complete and accurate, the Office of Acquisitions and Logistics should develop policies and procedures to ensure that obligations made through prime vendor orders—such as medical-surgical orders—are consistently captured in eCMS.

GAO, COAST GUARD SHORE INFRASTRUCTURE: Applying Leading Practices Could Help Better Manage Project Backlogs of At Least \$2.6 Billion, [GAO-19-82](#) (Washington, D.C.: February 2019).

From Objectives, Scope, and Methodology: To assess the reliability of the Coast Guard’s data discussed in this report, we interviewed knowledgeable agency officials, reviewed documentation, and electronically tested the data for obvious errors and anomalies. Specifically, we interviewed Coast Guard officials and discussed the mechanisms they use to assess the quality of their data and the extent to which Coast Guard employs quality control mechanisms, such as automated edit checks. Additionally, in August 2018, the Coast Guard informed us that its data on its shore infrastructure may not be complete if field inspectors did not identify problems at the facilities they inspected. Coast Guard officials also told us in July 2018 that not all projects on the

Limitations noted, including incomplete data

Coast Guard's PC&I backlog have cost estimates. As a result, the amount of funding needed to address the Coast Guard's backlog of shore infrastructure projects could be understated because the Coast Guard has not identified all deficiencies that exist at its facilities nor estimated the cost to fix all of the deficiencies it knows about. Despite these limitations, we determined that the Coast Guard's data are sufficiently reliable for the purposes of reporting on the Coast Guard's overall portfolio of shore infrastructure assets and the minimum amount of money the Coast Guard identified as needed to complete deferred repair and PC&I projects.

Specific purpose for use of data stated

Finding stated in terms of "at least" due to incomplete data

From findings: Coast Guard data show that it will cost at least \$2.6 billion to address its two project backlogs—(1) recapitalization and new construction, and (2) deferred maintenance.

However, the number of projects in the Coast Guard's backlogs and the associated cost for addressing them is incomplete. In July 2018, Coast Guard officials told us that the majority of the projects on the PC&I backlog do not yet have associated cost estimates, and thus have not been factored into the backlog cost estimates they have previously reported to Congress.

GAO, *FEDERAL STUDENT LOANS: Education Needs to Verify Borrowers' Information for Income-Driven Repayment*, [GAO-19-347](#) (Washington, D.C.: June 2019).

Compared to agency published data

Traced sample of records to other electronic data

From Objectives, Scope, and Methodology: To assess the reliability of the EDWA data, we reviewed documents related to the database and officials; performed electronic testing to determine the validity of specific data elements that we used to perform our work; compared the data we received to published Education data on the number of IDR borrowers and amount of their outstanding loans; and compared borrowers' personal information to the Social Security Administration's Enumeration Verification System to identify borrowers whose information may not have been accurate. As part of our reliability assessment of the EDWA data, we selected a nongeneralizable sample of 16 borrowers and their IDR plan and loan information from the EDWA data to compare against four selected loan servicers' records. Specifically, we stratified borrowers into two groups based on common and potentially outlying incomes and family sizes in the EDWA data. We then randomly selected two borrowers from each stratum for each of the four selected loan servicers (a total of four borrowers per loan servicer). We reviewed all IDR plan data in our scope for each selected borrower, including the plan type, family size, income,

Followed up with agency about discrepancies

and total monthly payment. We did not review original documents, such as the IDR applications or documentation of income. We discussed the results of our review with knowledgeable Education and loan servicer officials to gain additional understanding of each selected borrower's IDR plan information as well as any differences between EDWA and loan servicer data.

Changed scope of analysis based on data issues

We originally obtained EDWA data on approximately 6.5 million IDR plans approved between January 1, 2016 and September 30, 2017 that were held by almost 4.8 million Direct Loan borrowers. Based on data reliability issues we identified during our review, we had to limit the scope of our analysis to a subset of EDWA data that we determined were sufficiently reliable for our purposes. Education officials disclosed issues that impacted the IDR plan data reported to Education by one of its loan servicers. Specifically, Education and the loan servicer had identified instances where the loan servicer's internal data were changed for valid reasons but the changes were not reported to Education correctly. As a result, we excluded data reported by this servicer from all analyses in our report. We also identified issues with monthly payment amounts for some borrowers in the EDWA data. Accordingly, we limited our borrower-reported income analysis to borrowers who reported zero income and had a scheduled monthly payment of zero dollars.¹ Ultimately, we analyzed about 878,500 IDR plans held by about 656,600 borrowers for our income analysis and approximately 5 million IDR plans held by 3.5 million borrowers for our family size analysis. Consequently, our overall income and family size analyses results may be understated and are not generalizable to all IDR plans and borrowers.

Stated effect of reduced dataset on findings

Footnote 1: There were nearly 1.3 million IDR plans held by over 1.1 million borrowers who had reported zero income in the Education data we originally received. From this we determined that about 878,500 IDR plans were sufficiently reliable for our analysis.

Not Sufficiently Reliable for
Audit Purpose

GAO, *ELDER JUSTICE: Goals and Outcome Measures Would Provide DOJ with Clear Direction and a Means to Assess Its Efforts*, [GAO-19-365](#) (Washington, D.C.: June 2019).

From Objectives, Scope, and Methodology: We also interviewed the unit chief from the FBI's Internet Crime Complaint Center to discuss available data about elder abuse in the United States. Although complaint center data include self-reported incidents from individuals who were at least 60 years of age, individuals submitting reports to the system are not required to include their age or the age of the victim of the crime they are reporting. As such, we determined that the data related to individuals age 60 and above were not reliable for the purposes of this report.

Not reliable due to incomplete key data

GAO, *FOSTER CARE: States with Approval to Extend Care Provide Independent Living Options for Youth up to Age 21*, [GAO-19-411](#) (Washington, D.C.: May 2019).

From Objectives, Scope, and Methodology: To develop our methodologies, we reviewed related literature and interviewed child welfare experts. During this process, we explored analyzing federal data on youth in foster care from two federal databases: (1) the Adoption and Foster Care Analysis and Reporting System (AFCARS), and (2) the National Youth in Transition Database (NYTD). We determined these databases to be insufficiently reliable for our reporting purposes due to concerns about the completeness of the data pertaining to extended care services and participants.¹

Not reliable due to incomplete and inconsistent data on population of interest

Footnote 1: Stakeholders, including ACF officials, raised concerns about the consistency and completeness of AFCARS data for all extended-care youth, and said that NYTD may not include consistent data on the independent living services provided to youth in foster care since these services may be underreported.

GAO, *NATIVE AMERICAN YOUTH: Involvement in Justice Systems and Information on Grants to Help Address Juvenile Delinquency*, [GAO-18-591](#) (Washington, D.C.: September 2018).

From Objectives, Scope, and Methodology: We assessed the reliability of the record-level and some of the summary data by conducting electronic testing of the data and interviewing knowledgeable agency officials about the data systems. We assessed the reliability of the remaining summary data by interviewing knowledgeable agency officials about the summary

Found some data to be sufficiently reliable and some not; stated that unreliable data were not used

data. We determined that the record-level and summary data sources included in this report were sufficiently reliable for the purposes of our reporting objectives. We determined that some record-level and summary data sources, such as certain data related to arrests and sentencing information, contained information already provided by other data sources or contained too few Native American youth observations to provide reliable, reportable information. We did not include these data sources in our report. We also determined that some data variables in certain data sources were not reliable for our purposes. For example, two data sources did not contain reliable information for the race of individuals. We did not include these data sources in our report.

Explained why some presented data did not match published data

From footnotes in findings: We limited our analysis to youths who had been adjudicated and placed in a residential facility and did not include youths who were awaiting a trial or whose adjudication was pending. Since our analysis focused on records that met our criteria (e.g., race, and adjudication status), the data presented in this report do not match data in published DOJ statistical bulletins and web-based resources.

We were unable to incorporate gender into our analysis of federal adjudication data because complete data were not available.

Explained cleaning of data to remove invalid and duplicative records

From footnotes in OSM: The Executive Office for United States Attorneys (EOUSA) could confirm that all records in the administrative data they provided were for persons who were under 18, but could not specify the age category for all records. When we analyzed the data by age categories, we excluded records with unknown or unreliable age categories. However, we included all EOUSA records when we analyzed other variables contained in the EOUSA data (e.g., offense).

To address the duplicates we took steps to exclude duplicate records in our analysis while retaining relevant offense values from the duplicate observation prior to deleting the record.

Undetermined Reliability

GAO, *DRINKING WATER: Approaches for Identifying Lead Service Lines Should Be Shared with All States*, [GAO-18-620](#) (Washington, D.C.: September 2018).

From Objectives, Scope, and Methodology: Our objectives were to examine (1) what is known about the number of existing lead service lines nationally, and among states and water systems, and....

To examine what is known about the number of existing lead service lines nationally, and among states and water systems, we reviewed existing studies and other documents regarding the extent of and experience with such lines. We found three written studies with estimates of lead service lines—one using national data and two that were state-specific. We took a number of steps, including conducting interviews with each study’s authors, to examine the reliability of the data used in the studies. For the one study we reviewed that used national data, the data were of undetermined reliability because the sample of water systems included in the study was not generalizable to all water systems and the authors could not verify the accuracy of the information provided by water systems. Appendix I provides more information on our reasons for designating the data as undetermined reliability. For the two state-specific studies, we determined that the data represented reasonable efforts to estimate the number of lead service lines, although the states also could not verify the accuracy of the information provided by water systems. Therefore, we also found these estimates to be of undetermined reliability.

Example of the details included about one study that produced data of undetermined reliability

From appendix I: For the 2016 American Water Works Association study, we determined that the data were of undetermined reliability because the responses of the water systems surveyed were not generalizable to all water systems and the study authors could not verify the accuracy of the information. Specifically, the sample in the 2016 American Water Works Association study was not based on a statistical sample, and therefore the sampling error was not calculated and information was not available to determine whether responding water systems were similar to nonresponding water systems. For example, the estimate is based on survey responses from 978 of the approximately 23,000 water systems that existed around the time of the surveys, and therefore may not represent all water systems nationwide. In addition, since many water systems do not have complete inventories of their lead service lines, the accuracy of data that water systems submitted in response to the survey is difficult to verify. For example, our interview with the study authors indicates that the information provided by water systems varied in quality, with some systems basing their responses on rough estimates. We based our determination about the data using the criteria of Total Survey Error, which is a framework for assessing the validity and reliability of survey estimates. It includes sampling error (the difference between the population and the sample), nonresponse error, measurement error (the difference between the true response and the response provided by the respondent) and coverage error (the discrepancy between the list of individuals that is used to select a sample and the target population).

Headers and findings note limitations of the data

Header in findings: The Total Number of Lead Service Lines Is Unknown, and National, State, and Local Estimates Vary

Subheader in findings: National, State, and Local Estimates of Lead Service Lines Exist, and Those We Reviewed Had Significant Limitations; but the Methods Used to Arrive at These Estimates Vary

High level data presented in report, along with caveats about the limitations

From findings: The total number of lead service lines is unknown, and while some entities have developed estimates of lead service lines at the national, state, or local water system level, the estimates we reviewed have significant limitations to their reliability. Moreover, the approaches used to arrive at these estimates vary, making it challenging to compare estimates. Nationally, according to EPA's October 2016 Lead and Copper Rule Revisions White Paper, there are an estimated 6.5 million to 10 million homes served by lead service lines. This range of estimates, based in part on data from a study for the 1991 Lead and Copper Rule, has significant limitations. In appendix I we explain why EPA's estimate may not accurately reflect the total number of lead service lines, nationwide.

An April 2016 American Water Works Association study estimated 6.1 million lead service lines nationwide. The authors of this study extrapolated the number based on survey responses from 978 water systems in 2011 and 2013. While this study is the most recent attempt to provide a national estimate, it has significant limitations. First, the sample was not statistically representative of all 68,000 water systems subject to the Lead and Copper Rule. Rather, the water systems that responded to the American Water Works Association's survey are not a statistical sample. Second, according to the study's authors, survey responses were based on water systems' best guesses of the number of lead service lines in their systems. However, since water systems have not been required to maintain inventories of lead service lines, many of them do not know the exact number. For these reasons, we are not confident that the number accurately reflects the total number of lead service lines nationwide.

GAO, MOTOR CARRIERS: Better Information Needed to Assess Effectiveness and Efficiency of Safety Interventions, GAO-17-49 (Washington, D.C.: October 2016).

From Objectives, Scope, and Methodology: To determine the extent to which FMCSA has implemented CSA interventions and how it has applied them, we analyzed FMCSA intervention data from fiscal year 2010 through fiscal year 2015. We intended to analyze whether there

were any notable increases, decreases, or other trends in FMCSA's application of interventions—across states, regions, and motor carrier types. However, data limitations prevented an adequate and comprehensive assessment of the reliability of FMCSA's intervention data. For example, officials told us FMCSA changed the way it counted interventions over time, and as a result, we could not validate the results of our analysis against agency totals—a step to testing data reliability. As a result, we concluded that FMCSA's intervention data were of undetermined reliability, a factor that precluded our analysis of trends in FMCSA's application of interventions across states, regions, and motor carrier types. As a substitute, we requested that FMCSA provide estimates for how frequently it applied each intervention type from fiscal year 2010 through fiscal year 2015 to identify general trends. After reviewing FMCSA documentation related to the estimates and interviewing responsible FMCSA officials, we concluded that FMCSA's estimates were sufficiently reliable for this purpose.

Because data were of undetermined reliability, they were not used for the analysis and alternative data were identified

Audit Objective Focused on Data Reliability

GAO, *WHISTLEBLOWER PROGRAM: IRS Needs to Improve Data Controls for Some Award Determinations*, GAO-18-698 (Washington, D.C.: September 2018).

From Objectives, Scope, and Methodology: This report...(3) describes the purposes for which IRS collects and uses data from the FBAR Database and assesses the controls for ensuring data reliability....

To address our third objective, we evaluated IRS's FBAR Database to identify any control deficiencies, using as criteria principles on design activities for information systems and use of quality information from Standards for Internal Control in the Federal Government; the Federal Information Security Modernization Act of 2014, and National Institute of Standards and Technology Special Publication 800-53. We electronically tested the FBAR Database for missing data, outliers, and obvious errors, and reviewed IRS documentation on the database. We also interviewed IRS officials responsible for maintaining and using the database to determine how IRS uses the data, existing controls, any known limitations of the database, and any planned changes or improvements for the database. While we determined that the data we used from the FBAR Database were sufficiently reliable for the purposes of identifying individuals also named in whistleblower claims as well as FBAR enforcement outcomes, we identified risks to the reliability of the data, as discussed later in the report.

Data determined to be sufficiently reliable for a specific purpose but data issues discussed in findings

From findings: We assessed the reliability of the FBAR Database for the purposes of using limited data from this database for our own analysis. We determined that the data fields we used were sufficiently reliable for our purposes. Specifically, we matched taxpayer identification numbers in the FBAR Database to those in E-TRAK and reported on enforcement outcomes, including a limited number of penalty payments, as discussed previously. These data were the only available data within IRS on FBAR penalties and enforcement actions. Even though we found the data that we used to be sufficiently reliable for our purpose of identifying penalty information and selecting a sample of claims to review further, we identified some data control deficiencies related to data input and validation. We found certain elements of the database to have limited reliability.

Describes limitations to internal controls around data, including lack of quality review of manually entered data

While FBAR team employees transcribe data manually into the database from emails or faxed or mailed paper forms, there are no procedures for data testing or validation. For example, there is no secondary check by another individual to ensure data were entered correctly and completely. The FBAR Database procedures also lack sufficient validity checks to ensure that the data entered are accurate.

Examples of lack of internal controls provided, including results of some data testing

IRS officials also told us that they are aware there are some data missing in the database, such as incomplete records for some taxpayers, but they could not quantify how often this occurs. They also told us that such missing data can contribute to inaccurate reports of FBAR total assessments. For example, if a date field is left blank, certain reports that pull data based on these date fields will not pull the records with this missing field, thereby underreporting FBAR outcomes. We found 44 records with input errors in this date field. The officials stated that they make every effort to input complete data into the database, but sometimes complete information is unavailable from the exam team. Because the FBAR data lack some reliability controls, IRS may rely on insufficient or incomplete data for reporting and decision making, including amounts of whistleblower awards.

Recommendation: The Commissioner of Internal Revenue should ensure that the Deputy Commissioner for Services and Enforcement develops and documents improved controls for the validity, completeness, and accuracy of data on FBAR exams and enforcement actions.

GAO, DEFENSE INFRASTRUCTURE: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance

Utility Resilience Planning, GAO-15-749 (Washington, D.C.: July 2015).

Audit objective addressed data reliability

From Objectives, Scope, and Methodology: This report addresses ... (2) the extent to which DOD's collection and reporting of information on utility disruptions is comprehensive and accurate; and....

Compared data to independent information to evaluate comprehensiveness

To identify the comprehensiveness of DOD's reporting, we compared the military services' data submissions to OSD with the independent research we conducted in support of our efforts to determine whether threats and hazards have caused utility disruptions on DOD installations—and, if so, what impacts have they had. When comparing the data from our sample with the military service data submitted to DOD, we included only the disruptions that occurred on the sample's installations from fiscal years 2012 through 2014. We also reviewed documents on, and met with military service headquarters and OSD officials about, data reporting instructions and the processes to collect, validate, and report the data. To assess the accuracy of DOD's reporting, we reviewed utilities disruption data submitted by the military services to OSD, discussed the data validation processes used by officials at both the military services' headquarters and OSD, and reviewed OSD data validation documentation. We compared DOD's processes for the collection, validation, reporting, and use of these data to several leading practices for the use and management of data and process improvement.

Finding related to data reliability

Header in findings: DOD's Collection and Reporting of Utilities Disruption Data Are Not Comprehensive and Some Data Are Not Accurate

From findings: DOD instructions in a template used to collect utility disruption data from installations stipulate that installations should report on external, commercial utility disruptions lasting at least 8 hours. According to officials from the military service headquarters and OSD, they do not review installations' utilities disruption data to determine whether there are instances that meet the reporting criteria but are not included. Officials from three of the military service headquarters and OSD stated that, in fiscal years 2012 through 2014, there were installations that did not report on all disruptions that meet these criteria.¹ By comparing the utility disruptions we identified through our independent research to those submitted by the military services to OSD,² we confirmed cases of underreporting by installations from all four services, although our comparative analysis does not quantify the extent of underreporting.

Footnote 1: Neither DOD nor GAO is able to determine the total number of underreported disruptions. Because there is no source of information on all disruptions that meet DOD's criteria, there is no baseline to which we can compare the installations' submissions for fiscal years 2012 through 2014. For this reason, we conducted research into utility disruptions; our research was independent of the disruptions reported by the installations. To identify underreporting of disruptions, we compared the results of our research to the installations' submissions. For more information on our research methodology, see app. I.

Footnote 2: This research consisted of identifying news articles and information from DOD websites and press releases on DOD utility disruptions that occurred beginning in 2005 and then having military services officials verify this information and identify which instances lasted 8 hours or more.

Report also included recommendations to DOD to provide more consistent guidance on what disruptions should be reported and to improve the effectiveness of data validation steps.

GAO, *FEDERAL TELEWORK: Improved Guidance and Communication on Recording Telework Hours Needed at Veterans Benefits Administration*, [GAO-17-621R](#) (Washington, D.C.: August 2017).

From Objectives, Scope, and Methodology: You asked us to review VBA's telework policies and practices, and their impact on disability claims processing. This report examines how VBA oversees its telework program and how it tracks employees' telework hours. We were unable to assess the impact of telework on disability claims processing at VA because we found significant issues with the completeness and reliability of VBA's data on employees' telework hours.

To determine the extent of VBA oversight of its telework program, we reviewed VA policies, such as VA's agency-wide telework policy, and VA and VBA guidance on the oversight and monitoring of telework programs against selected internal control standards, requirements in the Telework Enhancement Act of 2010, and Office of Personnel Management (OPM) guidance on telework....

We asked about oversight procedures for telework at the agency and VBA level, as well as how telework data are tracked. In addition, we collected telework data recorded in VA's time and attendance system

Compared data from two sources

(VATAS) for two pay periods—one in January 2017 and one in April 2017. We also obtained VBA regional office data on the types of telework agreements VSRs and RVSRs had in place as of February 2017. We assessed the reliability of the data by comparing the data in both sources and interviewing agency officials knowledgeable about the data. Based on this assessment, we found that while there were no identified issues with the integrity of the VATAS system generally, the telework status of hours worked by VSRs and RVSRs was not systematically reported in VATAS during the two time periods we examined. As a result, we determined that data in the VATAS system is not sufficiently reliable for an analysis to determine any impact of telework on employees' ability to process disability compensation claims. We discuss issues related to the reliability of the data in our report.

Data quality issues affected audit objectives and led to findings and recommendations

From findings: Officials at the Department of Veterans Affairs (VA) told GAO that recording telework hours for each pay period became a requirement in March 2017 at VA, but the agency does not yet have key controls in place to ensure that employees' telework hours are recorded accurately in the time and attendance system. Specifically, VA has not updated its agency-wide written telework policy and other guidance to reflect the change. Moreover, although VA began communicating the change to timekeepers and telework coordinators—officials who help manage the telework program in each office—it has not taken steps to inform all employees and supervisors throughout the agency. Consequently, as of May 2017, some Veterans Benefits Administration (VBA) headquarters officials said they were not aware of the requirement.

Without outlining the new requirement to record telework hours in all relevant guidance and communicating it to all employees, some employees' telework hours may not be accurately recorded. Our analysis of time and attendance data for VSRs and RVSRs for pay periods before and after March 2017 confirmed this concern. Although VA told us that employees are generally expected to work their telework schedules, we found that almost half of the employees with agreements to regularly telework had no telework hours recorded in VA's time and attendance system (VATAS) in April 2017. Thus, VATAS data were unreliable, incomplete, and therefore, insufficient for us to determine the extent to which employees telework across VBA.

Recommendations: Review and update all relevant policies and guidance to reflect the agency's requirement that employees' hours teleworked be recorded in VATAS; communicate that telework hours should be recorded in VATAS to VBA regional office employees; and develop a process to

monitor the quality of data and to ensure that employees' telework hours are recorded accurately and completely in VATAS.

GAO, *K-12 Education: Education Should Take Immediate Action to Address Inaccuracies in Federal Restraint and Seclusion Data*, GAO-19-551R (Washington, D.C.: June 2019).

From Objectives, Scope, and Methodology: We have work under way on districts' reporting practices for restraint and seclusion data in response to a provision in the explanatory statement from the House Committee on Appropriations accompanying the Consolidated Appropriations Act of 2018. As part of our data reliability testing for that work, we analyzed the number of districts that left fields pertaining to restraint and seclusion blank, or that reported all zeros for those fields, to determine the prevalence of blanks or zeros in the CRDC at the national, state, and district levels. Our data reliability testing raised questions about the completeness and accuracy of the CRDC restraint and seclusion data. We are therefore issuing this separate report on the issues we have identified to date regarding potentially incomplete data. Because Education is currently collecting and validating restraint and seclusion data for the 2017-18 school year, it is important it take immediate steps to address underreporting before it publishes these data.

Data reliability issues identified during testing led to separate report about data issues

As part of this work, we reviewed the explanations that Education requires the largest districts to provide if they report zero incidents of restraint and seclusion. We also reviewed documentation on Education's investigations into underreporting of restraint and seclusion. Additionally, we interviewed federal Education officials and the contractor responsible for maintaining the CRDC and providing routine CRDC technical assistance, as directed by OCR.

Header in findings: CRDC Data Do Not Reflect All Incidents of Restraint and Seclusion

From findings: For the most recent CRDC—school year 2015-16—70 percent of the more than 17,000 school districts in the U.S. reported zero incidents of restraint and zero incidents of seclusion. In 39 states and the District of Columbia, more than half of the school districts reported zeros; and in 12 states, 80 percent or more of the districts reported zeros. (See fig. 1.) However, our analyses of 2015-16 CRDC data and review of Education documents indicate that CRDC data do not accurately capture all incidents of restraint and seclusion in schools.

Report also included recommendations to the Department of Education to clarify guidance and instructions to school districts and to follow up with school districts that have reported zero incidents, among others.

Additional report in which an audit objective focused on data reliability and led to recommendations to improve internal controls around data:

GAO, FEDERAL HUMAN RESOURCES DATA: OPM Should Improve the Availability and Reliability of Payroll Data to Support Accountability and Workforce Analytics, [GAO-17-127](#) (Washington, D.C.: October 2016). Data reliability issues identified during testing led to separate report about data issues.

Appendix V: GAO Contact and Staff Acknowledgements

GAO Contact

SaraAnn Moessbauer at (202) 512-4943 or MoessbauerS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michele Fejfar (Assistant Director), Kirsten Lauber (Analyst in Charge), Nora Adkins, Pille Anvelt, Jehan Chase, Melinda Cordero, Elizabeth Dretsch, Danielle Greene, Serena Lo, Monica Savoy, Kathleen Scholl, Walter Vance, and Jack Wang made key 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



Please Print on Recycled Paper.