GovRAMP

VERSION 2.0

Data Classification Tool

June 2026

A Companion Guide to the GR-199 Worksheet

Table of Contents

Document Revision History

Date	Description	Version	Author
December 2020	Original Publication	1.0	GovRAMP Steering Committee
October 2021	Security status updates	1.1	GovRAMP Staff
April 2022	Updates	1.2	GovRAMP Standards and Technical Committee and Board
May 2026	Updated to GovRAMP Branding, align to NIST SP800-60, and incorporate the GovRAMP GR-199 form	2.0	GovRAMP Standards and Technical Committee
June 2026	Adopted	2.0	GovRAMP Board of Directors

Introduction and Purpose

This document is a companion guide to the GR-199 worksheet and is intended to be used by service providers to determine the impact level (High, Moderate, or Low) of their product offerings.

It may also be used by state and local governments and procurement officials as a tool for determining the appropriate GovRAMP security requirements in solicitations with the intent of procuring a service provider using or offering IaaS, SaaS, and/or PaaS solutions that process, store, and/or transmit government data including PII, PHI, and/or PCI.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure vendors are providing solutions that meet the minimum security requirements to process, store, and transmit certain types of government data.

It is necessary for government agencies to accurately determine their required security baseline prior to publishing a solicitation so that the agency can select a vendor that meets the government's needs and provides the appropriate security controls to protect the government data. The GR-199 worksheet is based on the NIST SP 800-53 Revision 5 requirements and NIST SP 800-60 Vol 2 data types. It is designed to help governments easily identify the appropriate GovRAMP security impact category to include in a solicitation.

Instructions

The process of determining the Impact Level of a system can be broken down into four (4) steps:

1. **Identify Information Types**: Determine the types of information that need to be categorized utilizing the GovRAMP 199 Impact Analysis Worksheet.
2. **Select Provisional Impact Levels**: Assign provisional impact levels to the information types based on their potential impact.
3. **Adjust Provisional Impact Levels**: Adjust or finalize the impact levels for the information types.
4. **Assign Overall Impact Level**: Determine the system's security category and overall impact level based on the provisional impact levels.

Step 1: Identify Information Types

The first step is to identify the information types your organization handles. This means taking a comprehensive inventory of the data that flows through the system—whether it is collected, processed, stored, or transmitted.

This step is critical because it lays the foundation for all subsequent security decisions. If information types are overlooked or misclassified, the resulting security categorization will be incomplete or may be inaccurate. To do this effectively, organizations should involve stakeholders like system owners, data stewards, and program managers, since they have the best understanding of how information is used and its potential impact. A thorough identification process ensures that sensitive data—such as medical records or financial transactions—are properly recognized and can later be mapped to the right security objectives.

GovRAMP leverages the data types found in NIST SP 800-60 Volume II Table C and Table D as well as those found in Appendix A of this guide. These tables categorize information into groups such as mission-based information (e.g., law enforcement, healthcare, education) and management and support information (e.g., financial management, human resources, IT operations). By aligning with these standardized categories, we ensure consistency across agencies and avoid subjective or ad hoc classifications.

Using the GovRAMP GR-199 worksheet, simply select the appropriate Data Types from the drop-down selector. Each Data Type is labeled with the corresponding NIST SP 800-60 Volume II section number for easy reference.

Step 2: Select Provisional Impact Levels

When a Data Type is selected in the GovRAMP GR-199 worksheet, the tool automatically assigns the appropriate provisional impact levels for confidentiality, integrity, and availability based on the ratings found in the NIST SP 800-60 Volume II or Appendix A.

Step 3: Review Provisional Impact Levels

Organizations may need to adjust the provisional security impact levels for the security objectives of each information type. To accomplish this, organizations should:

1. Review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing requirements;
2. Adjust the security objective impact levels as necessary. NIST SP800-60 Volume II provides “special factors” guidance that could be considered for each adjustment; and

3. Document all adjustments to the impact levels and provide rationale or justification for the adjustments.

> For confidentiality, consider how unauthorized disclosure could harm the organization, its mission, or individuals.
>
> For integrity, consider how inaccurate or altered data would disrupt operations or decision-making.
>
> For availability, consider how loss of access would hinder essential functions or services.

These adjustments should be made in the corresponding *Adjusted Confidentiality Impact Level*, *Adjusted Integrity Impact Level*, or *Adjusted Availability Impact Level* field. Individual adjustments should be limited to a one-level increase or decrease.

Step 4: Assign Overall Impact Level

Once the impact levels have been adjusted, if necessary, the GovRAMP GR-199 worksheet will calculate the highest rating for Confidentiality, Integrity, and Availability. The overall system impact level is determined by the highest value assigned to Confidentiality, Integrity, or Availability.

Save a copy of the completed GovRAMP GR-199 worksheet for your records. Service providers may be required to submit their GovRAMP GR-199 worksheet to their Third-Party Assessment Organization (3PAO) or the GovRAMP Program Management Office.

Appendix A – GovRAMP Data Types

GovRAMP has identified the following Data Types as a supplement to the NIST SP800-60 Volume II.

1. **Public Data**: For non-sensitive government data, metadata, and/or data that may be released to the public that requires no additional levels of protection use the "General Government | General Information" data type.
2. **Personally Identifiable Information (PII)**: For Personally Identifiable Information (PII) as defined by the U.S. Department of Labor (DOL) use the "General Government | Personal Identity and Authentication" data type.
3. **Protected Health Information (PHI)**: For Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) use the appropriate Data Type found in the "Health" section of Table D-2 in the NIST SP-800-60.
4. **Payment Card Industry (PCI)**: Payment Card Industry (PCI) data is defined by the PCI Security Standards Council (PCI SSC). NIST SP 800-122 sites both financial data and card data as forms of Personally Identifiable Information, therefore use the "General Government | Personal Identity and Authentication" data type.
5. **Criminal Justice Information (CJI)**: For Criminal Justice Information (CJI) as defined by the FBI Criminal Justice Information Services division use the appropriate Data Type found in the "Law Enforcement" section of Table D-2 in the NIST SP-800-60.
    a. Note: Governments may add additional controls to GovRAMP Moderate to comply with state-specific CJIS requirements.
6. **Federal Tax Information (FTI)**: Any return or return information received from the IRS or other authorized sources that is protected under Internal Revenue Code §6103 for confidentiality.
    a. Per *Section 2.B.1 General* of IRS Publication 1075 (Rev. 11-2021), the overall: "The IRS has categorized federal tax information as moderate risk."
7. **Family Educational Rights and Privacy Act (FERPA)**: Per the act, FERPA data is any records, files, documents, and other materials that (i) contain information directly related to a student and (ii) are maintained by an educational agency or institution or by a person acting on behalf of such an agency or institution. NIST SP 800-122 sites educational data as a forms Personally Identifiable Information, therefore use the "General Government | Personal Identity and Authentication" data type.