



1	INTRODUCTION.....	2
1.1	PURPOSE	2
1.2	SCOPE	2
1.3	ASSUMPTIONS	2
1.4	RESPONSIBILITIES	2
1.5	DOCUMENT LAYOUT.....	2
2	SYSTEM IMPACT OVERVIEW	3
2.1	LOW IMPACT	3
2.2	MODERATE IMPACT	3
2.3	HIGH IMPACT	3
3	DATA SENSITIVITY CLASSIFICATION.....	3
3.1	CONFIDENTIALITY	3
3.2	INTEGRITY	3
3.3	AVAILABILITY	3
4	METHODOLOGY FOR DETERMINING IMPACT LEVELS	3
4.1	IDENTIFY INFORMATION TYPES.	3
4.2	SELECT PROVISIONAL IMPACT LEVELS	3
4.3	REVIEW PROVISIONAL IMPACT LEVELS	3
4.4	ADJUST/FINALIZE INFORMATION IMPACT LEVELS	3
4.5	ASSIGN SYSTEM SECURITY CATEGORY.....	3



Data Sensitivity Worksheet Guidance

1 INTRODUCTION

FIPS 199 establishes the requirement for Agencies to categorize and rank its information types using confidentiality, integrity, and availability.

1.1 Purpose

The purpose of this document is to establish guidelines for the classification of data and information types with respect to its confidentiality, integrity and availability. By determining the sensitivities of the information, Education will be able to apply those classifications to the overall categorization of the information systems that process or store the information.

1.2 Scope

This document serves to outline the specifics for categorizing information types that a system/application processes as it relates to confidentiality, integrity, and availability and the overall classification a system/application receives using the guidance provided in FIPS 199.

1.3 Assumptions

The Department of Education made the following assumptions when creating this guidance.

1. Data Sensitivity levels are determined using Government-wide recommendations from FIPS 199.
2. High availability is based on the assumption that the two Mission Essential functions for the COOP (Title IV and Project SERV) are important at the U.S. Government level as well.
3. Information that is not covered by the Privacy Act and not considered sensitive is still labeled low.

1.4 Responsibilities

The owner of each system, or an individual designated by the owner, is responsible for identifying the information types stored in, processed by, or generated by that system. In the case of mission information, the responsible individuals, in coordination with management, operational, and security stake holders, should compile a comprehensive set of lines of business and mission areas conducted by the agency, as well as the functions and sub-functions necessary to conduct agency activities.

1.5 Document Layout

Section 1: Introduction

Section 2: System Impact Overview

Section 3: Data Sensitivity Classification

Section 4: Methodology for determining impact levels



2 SYSTEM IMPACT OVERVIEW

The Department of Education evaluated the requirements in FIPS 199 and, as recommended by NIST, applied the requirements to the Education environment. At Education, we do not expect ANY systems to have a HIGH confidentiality or integrity based on the information types present and the definitions provided in FIPS 199. Additionally, Education does not store, process, or manage any information that could result in *physical* harm to an individual. As a result, this categorization was removed from Education's definition of impact.

FIPS 199 categorizes impact into low, moderate or high levels.

2.1 Low Impact

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

2.1.1 FIPS 199 Definition

A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Result in minor damage to organizational assets;
- Result in minor financial loss.

2.1.2 Department of Education application of FIPS 199:

The impact would *not* affect

- Essential functions required for Principal Office business continuity plans or the Department's continuity of operation plan (COOP). The two essential COOP functions are the SERV program and Title IV.
- Includes damaging public confidence to such a severe degree that the Department would not be trusted to complete these functions.
- A financial impact of more than \$3 million over 3 years

2.2 Moderate Impact

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

2.2.1 FIPS 199 Definition

A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to organizational assets;
- Result in significant financial loss; or

2.2.2 Department of Education application of FIPS 199

- Essential functions required for Principal Office business continuity plans to a point that they could not be completed but would not affect the Department's COOP.



- Damaging public confidence to such a severe degree that the Department would not be trusted to completed these functions.
- Result in a financial impact between \$3 million over 3 years and \$1 billion

2.3 High Impact

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

2.3.1 FIPS 199 Definition

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- Result in major damage to organizational assets;
- Result in major financial loss

2.3.2 Department of Education application of FIPS 199

- An essential function required for Principal Office business continuity plans or the Department's COOP could not be completed.
- This includes causing a lawsuit or damaging public confidence to such a severe degree that the Department would not be trusted to complete these functions.
- Result in a financial impact over \$1 billion dollars

3 DATA SENSITIVITY CLASSIFICATION

Based on the definitions in NIST’s standards and guidance, the Department of Education developed an implementation methodology to identify its information types and categorize the data’s sensitivity.

3.1 Confidentiality

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542] A loss of *confidentiality* is the unauthorized disclosure of information.

Level	Description
N/A	Information that has no expectation of privacy.
Low	At a minimum, all Privacy Act information (other than social security numbers) or other sensitive information (other than preaward contract information). Refer to Appendix XX. <i>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i>
Moderate	Privacy Act information that contains a Social Security Number. Also, information types that were labeled moderate in NIST 800-60 Volume 2, Second Public Draft, that were specific to the Privacy Act are also covered in this category including



	<p>income info (other than government employee income information), personal identity and authentication, entitlement event information, and representative payee information)</p> <p><i>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>
High	<p>Any information that could result in death or major financial loss. [At this time, the Department does not process, store, etc. any data of this type.]</p> <p><i>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>

Common Confidentiality Factors

Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with the answers to the following questions:

- How can a malicious adversary use the information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- How can a malicious adversary use the information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders, or agency regulations?

Each use of the information type and each known variant of the information belonging to the type should be considered in determining the confidentiality impact level.

3.2 Integrity

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542] A loss of *integrity* is the unauthorized modification or destruction of information.

Level	Description
Low	<p>Information processed through a system or application that is part of an overall project but is not the final version that is disseminated or processed. The issuance of improper information could be detected elsewhere and would not cause a disruption in the business process.</p> <p><i>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>
Moderate	<p>Any information processed that a financial action is based on and disseminated to other organizations or to the public that will not be detected elsewhere in the business process.</p> <p><i>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>
High	<p>Information that if compromised could cause a major financial impact or cause COOP or BCP essential functions to cease.</p> <p><i>The unauthorized modification or destruction of information could be expected to have</i></p>



a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)

Common Integrity Factors:

Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with unauthorized modification or destruction of 1] each known variant of the information belonging to the type and 2] each use of the information by the system under review. Unauthorized modification or destruction of information can take many forms. The changes can be subtle and hard to detect, or they can occur on a massive scale. One can construct an extraordinarily wide range of scenarios for modification of information and its likely consequences.

Each information type should be evaluated with respect to the low/moderate/high impact associated with the answers to the questions below.

How can unauthorized modification or destruction of information:

- Reduce public confidence in an agency,
- Fraudulently achieve financial gain,
- Influence personnel decisions,
- Interfere with or to manipulate law enforcement or legal processes,
- Influence legislation, and
- Achieve unauthorized access to government information or facilities.

In most cases, the most serious impacts of integrity compromise occur when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public. Undetected loss of integrity can be catastrophic for many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitate unauthorized access to sensitive or private information or deny access to information or information system services). Unconstrained malicious write access to information and information systems can do enormous harm to an agency’s missions and can be employed to use an agency system as a proxy for attacks on other systems. In many cases, the consequences of unauthorized modification or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

3.3 Availability

“Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542] A loss of *availability* is the disruption of access to or use of information or an information system.

Level	Description
Low	Information that is considered Supportive to the operations of the Department. This information is processed/stored in Education assets that are determined to be our Mission Supportive Education assets based on our CIP survey. <i>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.(FIPS199, Table 1, pg 6)</i>
Moderate	Information that is considered Mission Essential to the operations of a Principal



	<p>Office. The business process owner will determine if the information is essential for the Principal Office Business Continuity Plan and COOP. This information is processed/stored in Education assets that are determined to be our Mission Important Education assets based on our CIP survey.</p> <p><i>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>
High	<p>Information that is considered Mission Critical to the operations of the U.S. Government. This information is processed/stored in Education assets that are determined to be our Mission Critical Education assets based on our CIP survey. This information would be determined by their support of Education’s COOP Essential Functions.</p> <p><i>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (FIPS199, Table 1, pg 6)</i></p>

Common Availability Factors:

Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with loss of availability of 1] each known variant of the information belonging to the type and 2] each use for the information by the system under review. For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information data bases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time-consuming and expensive. The disruption to agency operations would be serious to severe. In most cases, the adverse effects of limited-duration availability compromise on agency mission functions and public confidence in the agency will be limited. In contrast, for time-critical information types, availability is less likely to be restored before serious harm is done to agency assets, operations, or personnel (or to public welfare). As a result of this property, the rationale for most availability impact recommendations will indicate whether or not the information is time-critical.

Each information type should be evaluated with respect to the low/moderate/high impact associated with the answers to the questions below.

- Is the system considered a mission essential asset?
- Is the system part of the organization’s business continuity plan?
- Does the system have a continuity of operations plan?



4 METHODOLOGY FOR DETERMINING IMPACT LEVELS

System owners, or designee, should use the following methodology to categorize each system's information system and potential impact level. These steps provide guidance to determine the impact level recommendations of the confidentiality, integrity and availability of the data processed, stored, etc. by the Department's systems. When determining impact, the evaluator should remember that FIPS 199 applies the level definitions of *potential impact* on organizations or individuals **should there be a breach of security** within the context of each organization and the overall national interest.

1. Identify information types.
2. Select provisional impact levels
3. Review provisional impact levels
4. Adjust/finalize information impact levels
5. Assign system security category

4.1 Identify information types.

Information types that are input into, stored in, processed by, and/or output from the system must be identified. Identify subsystems and interconnectivity and state the information types that are used. (Please reference Appendix XX for a listing of the information types specific to the Department of Education. Check all that apply for your system. If needed, add information types not included in the list – see methodology below. Also note that definitions of terms are provided at the end of the document. Note - Government wide impact level recommendations are defined by NIST 800-60, which determines Low, Moderate and High ratings for data sensitivity based on a government-wide scale. This methodology was tailored to the Department of Education Enterprise Architecture, resulting in impact level recommendations specific to the type of data processed by the Department and the impact if the data was compromised. Refer to Section XX for an explanation of what factors are applied to determine data sensitivity at the Department.

The following methodology must be used to identify the information types processed, stored, etc. by each system:

For each automated business function, identify the single line of business that best describes the purpose of the system in functional terms;

- The Department has identified the following seven lines of business in its Enterprise Architecture:
 - Grants
 - Loans
 - Evaluation
 - Research and Statistics
 - Information Dissemination
 - Compliance
 - Administration

Once the automated business process has been aligned with a single Department Line of Business, next identify the associated business function from the Department's Enterprise Architecture. There are currently 16 business functions associated with the seven lines of business. Following the process outlined in NIST Special



Publication 800-60, the Department is equating these business functions with the Department's basic information types

Once the automated business process has been aligned with a single Department information type (i.e., business function under the Enterprise Architecture), identify the information processed by the system that is required by statute, executive order, or agency regulation to receive special handling (e.g., with respect to unauthorized disclosure or dissemination, like Privacy Act data). Compare the information in the system to the description of the information in the associated basic information type. The system's information may be used to adjust data sensitivity impact levels, up or down, from the base line data sensitivity impact levels for the associated basic information type. Appendix ZZ provides a listing of information that is considered confidential and the impact level recommendation defined by the Department.

An information type should be identified for each line of business listed. Appendix YY (refer to NIST 800-60 Appendix or insert into document) lists legislative and executive sources that establish sensitivity or criticality protection requirements for specific information types. Although this guideline identifies a number of information types, only a few of the types identified are likely to be processed by any single system. Also, each system may process information that does not fall neatly into one of the listed information types. Once a set of information types identified in this guideline has been selected, it is prudent to review the information processed by each system under review to see if additional types need to be identified for impact assessment purposes.

Where an information type processed by a system is not categorized by this guideline, an initial impact determination will need to be made based on the criteria determined by the Department following FIPS 199 criteria (refer to Section XX).

A Principal Office may identify information types not listed in this guideline or may choose not to select a default impact level from Section EE. If this is the case, the Principal Office should employ the Department's guidance based on FIPS 199 criteria to determine provisional impact levels.

In general, impact assessment is independent of mechanisms employed to mitigate the consequences of a compromise. Pg. 11 NIST 800-60 V I

4.2 Select provisional impact levels

Provisionally assign impact levels to each identified information type. Refer to Appendix XX for the Department's recommended impact levels for information types.

4.3 Review provisional impact levels

Review the appropriateness of the default impact levels recommended for the information types in the context of the organization Department wide, environment, mission, use, and connectivity associated with the system under review. [Re-evaluate based on Department of ED specific examples]

4.4 Adjust/finalize information impact levels

Based on the results of the review of provisional impact levels, adjustments should be made to the recommended default impact levels as appropriate. [Revise impact level and provide explanation]

4.5 Assign system security category.

Establish the level of confidentiality impact, integrity impact, and availability impact associated with the system under review. The adjusted impact levels for information types are reviewed with respect to the aggregate of all



information processed in or by each system. In some cases, the consequences of loss of confidentiality, integrity, or availability of the information aggregate can be more serious than that for any single information type. In addition, a system’s access control information and the system software that protects and invokes it can both affect the integrity and availability attributes of a system and even access to other systems to which the system under review is connected.

Following completion of the security categorization process, the confidentiality, integrity, and availability impact level determinations that result from this process can then be used to select the set of security controls necessary for each system. The minimum security controls recommended for each system security category can be found in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Classify each information type by impact level then determine highest level for each – confidentiality, integrity and availability, also evaluate if any levels should be raised even higher based on aggregation of data, criticality, etc.

Appendix: Information Covered by the Privacy Act & Freedom of Information Act (FOIA) Exemptions

Confidential information transmitted, stored, or processed on the GSS or MA, may include, but is not limited to, financial, proprietary and personal information.

TYPES OF CONFIDENTIAL INFORMATION	
Financial Information	
<ul style="list-style-type: none"> • Sales statistics • Profit and loss data • Overhead and operating costs • Reports on financial condition • Capital expenditures 	<p>Exemption (b)(4) of the FOIA protects proprietary “commercial or financial information obtained from a person [that is] privileged or confidential.” The term "person" refers to a wide range of entities, including corporations, banks, state governments, agencies of foreign governments, and Native American tribes or nations. Records are ‘commercial’ so long as the submitter of those records has a commercial interest in them. This exemption protects the interests of the submitters of information.</p>
Proprietary Information	
<ul style="list-style-type: none"> • Trade Secrets • Business plans or technical designs • Research and development data • Internal personnel rules & practices of the agency 	<p>Exemption (b)(2) of the FOIA protects from disclosure records that are related solely to the internal personnel rules and practices of the agency. Exemption (b)(4) of the FOIA also protects "trade secrets." A trade secret is a commercially valuable plan, formula process or device that is used for making or processing trade commodities and that is the end result of substantial effort or innovation.</p>
Legal and Decisional Information	



<ul style="list-style-type: none"> • Attorney-client documents • Attorney Work Product • Deliberative Process Documents 	<p>Exemption (b)(5) of the FOIA protects from disclosure inter or intra-agency documents that would be privileged in a civil lawsuit. This includes information disclosed by a client in confidence to OGC for legal advice, and OGC’s advice based on such information. It also includes materials produced by an attorney or at his direction in contemplation of litigation. And it includes documents that reflect the pre-decisional thinking, advice, opinions, or recommendations of employees on pending legal or policy decisions.</p>
<p>Personal Information</p>	
<ul style="list-style-type: none"> • Social security numbers (or other number originated by a government that specifically identifies an individual) • Credit history • Loan history • Personal addresses • Personal financial information • Name • Date of Birth • Photographic Identifiers (e.g., photograph image, x-rays, and video) • Driver’s License • Biometric Identifiers (e.g., fingerprint and voiceprint) • Mother’s Maiden Name • Vehicle Identifiers (e.g., license plates) • Mailing Address • Phone Numbers (e.g., phone, fax, and cell) • Medical Records Numbers • Medical Notes • Financial Account Information and/or Numbers (e.g., checking account number and PINs) • Certificates (e.g., birth, death, and marriage) • Legal Documents or Notes (e.g., divorce decree, criminal records, or other) 	<p>Exemption (b)(6) of the FOIA protects from disclosure information about individuals contained in “personnel, medical or similar files” when release of the information “would constitute a clearly unwarranted invasion of personal privacy.” An individual's name and address may not be sold or rented by an agency unless specifically authorized by law. On the other hand, no agency shall withhold names and addresses that are otherwise permitted to be made public. Any contractor or employee of a contractor is considered to be an employee of the agency.</p>



<ul style="list-style-type: none"> • Device Identifiers (e.g., pacemaker, hearing aid, or other) • Web URLs • Email Address • Education Records • Military Status and/or Records • Employment Status and/or Records • Foreign Activities and/or Interests 	
Law Enforcement Information	
<ul style="list-style-type: none"> • ED law enforcement investigations • Confidential Sources • Law enforcement techniques 	<p>Exemption (b)(7) of the FOIA protects from disclosure records or information compiled for law enforcement purposes to the extent such records could reasonably be expected to interfere with enforcement proceedings, constitute an unwarranted invasion of personal privacy, disclose the identity of a confidential source, endanger the life or safety of any individual, or risk circumvention of the law by disclosing law enforcement techniques. Law enforcement refers to both civil and criminal laws. As such, it includes OIG, OCR, and similar investigations.</p>
TYPES OF NON-CONFIDENTIAL INFORMATION	
<ul style="list-style-type: none"> • Grantee name (business contact information) • Employee names, titles, grades, salaries, position descriptions, duty stations, office phone numbers or e-mail addresses • Contractor names, e-mail addresses or business contact information 	<p>Exemption (b)(6) of the FOIA states that information submitted with no expectation of privacy should be considered non-confidential information.</p>