

## FIPS 199 Standards for Security Categorization of Federal Information and Information Systems Assessment (FIPS 199 Assessment)

### Purpose:

The Federal Information Processing Standards (FIPS) 199 Assessment was designed by the federal government to develop standards for categorizing information and information systems in order to protect both the Government and contractors from the risks associated with compromise of the confidentiality, integrity or availability of information. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security and law enforcement communities; and allows for consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures and practices.

The security categories are based on potential impact on an organization should certain events occur which jeopardize the information and information systems needed by an organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerabilities and threat information in assessing the risks to an organization. Further information on the purpose of the FIPS 199 Assessment can be found under Additional Resources.

### Instructions:

In accordance with the Information and Physical Access Security section of the contract, the contractor shall submit a FIPS 199 Assessment within thirty (30) days after contract award. The FIPS 199 Assessment shall be consistent with the cited NIST standards contained within [NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories](#) and [NIST FIPS PUB 199](#). More information on the NIST standards can be found under Additional Resources.

**Please note:** The purpose, instructions and additional resource sections should not be included in the actual FIPS-199 form submitted to the Contracting Officer. These are references to aid the contract in completing its IT security contract deliverables. Please separate these sections and only submit the FIPS-199 form.

The FIPS 199 Assessment should be signed by the Designated Approving Authority (DAA) on the contract. The DAA is the individual on the contract who formally assumes responsibility for operating the information technology systems under the contract's purview at an acceptable level of risk. The DAA is often the contractor's Director of Information Technology, Chief Information Officer or similar role.

The contractor should use the resources provided within this document in addition to the fully executable contract provided by the Contracting Officer to complete the FIPS 199 Assessment. The appropriate resource needed for completing each section within the FIPS 199 Assessment is noted in *italics* under each section header. Some additional information to guide the contractor in completing the FIPS 199 Assessment is provided below:

### **System Information Type**

System information type is the category of information (e.g. privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) contained within the system. Many information systems are not employed directly to provide services to citizens and clients, but are primarily intended to provide administrative or business services that support mission accomplishments. These types of systems are considered management and support system information types.

Information systems however that are employed directly to provide services to citizens and clients are considered mission-based system information types.

It is worth noting that some systems will fulfill both the Management and Support and the Mission-Based Systems Information Types. Check all applicable information types under this section.

### **Overall System Security Category**

Please note most contracts with one of the following conditions will have an overall system security category of Moderate:

- Whenever any contractor (and/or any subcontractor) employee will develop, have the ability to access, or host, and/or maintain federal information and/or federal information system(s);
  - Federal Information is defined as information developed by the United States federal government (and its contractors) for use in computer systems by government agencies and government contractors.
  - Information that is generated under a contract which is to be turned over to the federal government as a deliverable and is not used in the operations of the federal government is not considered federal information.
  - If however, the information is collected on behalf of the federal government in such a way that a reasonable person could assume that the information is being collected by the federal government than this information could be considered federal information.
    - As an example of this scenario, if information is collected from a website that features the HHS and/or NHLBI logo it could be reasonably assumed, and therefore considered, to be federal information.
- Whenever any contractor (and/or any subcontractor) employee will access, or use, Personally Identifiable Information (PII), and other sensitive information, including instance of remote access to or physical removal of such information beyond agency premises or control;
- Whenever any contractor (and/or any subcontractor) employee will have regular or prolonged physical access to a “federally-controlled facility,” as defined in FAR Subpart 2.1; or
- When acquiring cloud services

### **Suggested Means of Lowering the Level of Overall System Security Categorization**

In order to reduce the risk to an organization and in an effort to reduce the cost associated with the resulting information security requirements; contractors are encouraged to explore means of lowering the level of overall

system security category associated with their systems through risk avoidance related the to specific risk criteria above.

For sensitive information, contractors could explore means of de-identifying, masking, and/or anonymizing the information within their systems. If accessing, handling, storing or transmitting genomic or phenotypic information contractors should consider handling partial rather than whole genomic or phenotypic sequences. Refer to [NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#), for more information on these potential controls.

Other means of lowering the level of overall system security categorization through risk avoidance include assessing if the contractor needs to have regular or prolonged physical access to a federally-controlled facility or federal information system(s) to complete the required work. Many contractors find that they can easily accomplish the necessary work remotely without regular or prolonged physical access to these types of facilities and information system(s). It should be noted that all the controls and alternatives within this section should be discussed with the Contracting Officer Representative and/or Contracting Officer prior to implementation.

#### **Category of Information**

Most contracts who complete health care research for NHLBI will have a category of information type of D.14.5 Health Care Research and Practitioner Education Information Type. For a full list of category of information types relevant to the Contract please refer the NIST 800-60 document under Additional Resources.

The System may have more than one applicable category of information type. As such additional sections are provided in the FIPS 199. List all that are applicable.

#### **Provisional Impact Level**

The provisional impact level is NIST's suggested security impact levels for common information types. Refer to the category of information's recommended impact type found in the NIST 800-60 document under Additional Resources. For example, D.14.5 Health Care Research and Practitioner Education Information Type has a provisional impact level of **(confidentiality, Low), (integrity, Moderate), (availability, Low)**.

#### **Adjusted Impact Level**

The adjusted impact level allows the contractor to adjust the provisional impact levels provided by NIST to account for the system's unique needs. For example, if personally identifiable information is stored on the server, the adjusted impact level for D.14.5 may be: **(confidentiality, Moderate), (integrity, Moderate), (availability, Low)**. In this instance, a rationale for the adjustment should be supplied. In the example provided, the rationale could be: *A breach of patient health care data would cause serious adverse effect on organizational operations, assets and individuals, therefore the confidentiality impact is Moderate.*

If no adjustment is necessary to the provisional impact levels, leave these fields blank.

#### **Designated Approving Authority**

The FIPS 199 Assessment should be signed by the Contract Designated Approving Authority (DAA). The DAA is the individual on the Contract who formally assumes responsibility for operating the information technology systems under the Contract's purview at an acceptable level of risk. The DAA is the individual on the Contract who formally assumes responsibility for operating the information technology systems under the Contract's purview at an acceptable level of risk. The DAA is often the Contract's Director of Information Technology, Chief Information Officer or similar role.

#### **Additional Resources:**

[Standards for Security Categorization of Federal Information and Information Systems – FIPS PUB 199](#)

[Volume II: Appendices to NIST Guide for Mapping Types of Information and Information Systems to Security Categories – NIST 800-60-rev1](#)

[Table 1: Security Categorization of Federal Information and Information Systems \(Rev. 06-01-2009\)](#)

[Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\), NIST SP 800-122](#)

## NHLBI FIPS 199 Assessment

Contract Overview						
Project Title						
Contract/Solicitation Number						
Contracting Officer						
Contract Awardee					Award Date	
System Overview						
System Name						
System Description						
System Information Type						
<i>(Reference Volume II: Appendices to NIST Guide to Mapping Types of Information and Information Systems to Security Categories)</i>						
Management and Support <i>(See Appendix C)</i>				Mission-Based <i>(See Appendix D)</i>		
Overall System Security Category						
<i>(Reference Fully Executable Contract Section E. Additional NIH Requirements, 1. Security Categorization of Federal Information Systems (FIPS 199 Assessment), B. Security Categories and Levels)</i>						
Low		Moderate			High	
Overall Impact Levels						
<i>(Reference Federal Standards for Security Categorization of Federal Information and Information Systems, Section 3. Potential Impact on Organizations and Individuals)</i>						
Confidentiality			Integrity		Availability	
Type(s), Provisional Impact Level(s), Adjusted Impact Level(s), Rationale						
<i>(Reference Volume II: Appendices to NIST Guide to Mapping Types of Information and Information Systems to Security Categories)</i>						
Category of Information	Provisional Impact Levels			Adjusted Impact Level		
	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability

Rationale for Designated Potential Impact Levels						
Category of Information	Provisional Impact Levels			Adjusted Impact Level		
	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability
Rationale for Designated Potential Impact Levels						
Category of Information	Provisional Impact Levels			Adjusted Impact Level		
	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability
Rationale for Designated Potential Impact Levels						
<b>Impact Level Determination and Review Performed by:</b>						
Name	Organization			Title		
<b>Designated Approving Authority</b>						
Name			Title			
Address						
Phone			Email			

*By signing below, the DAA acknowledges they have reviewed the FIPS 199 Assessment in its entirety and agree with the system security category and potential impact levels.*

---

DAA Signature

Date