FIPS-199 (Categorization)

Completing the Federal Information Processing Standard (FIPS)-199: Standards for Security Categorization of Federal Information and Information Systems

The FIPS-199 should be filled out with assistance from the NCI Information Systems Security Officer (ISSO) to ensure that the best information category or categories are selected and the final ratings are well supported. For help, contact the NCI ISSO

.

A FIPS-199 must be completed for all federal information systems and applications in order to establish a system's security-impact rating based on the sensitivity of the information collected, stored, or processed by the system. The system's final rating is critical to identifying its required minimum security controls and helps determine all subsequent security testing that may be done on the system, following the National Institute of Standards and Technology (NIST) risk management framework (RMF).

NIST SP 800-60 Volume 2, Special Publication *Guide for Mapping Types of Information and Information Systems to Security Categories* provides an extensive list of information types commonly used by government organizations.

Step 1/Page 1: Complete the System Information Summary

On page 1 of the FIPS, fill in the:

1. System Name (if you are unsure of the official system name, please contact the NCI ISSO for verification at NCIIRM@nih.gov)
2. Fill in NCI under the IC box
3. Choose the correct System Type.
   - The majority of systems will be Tier 2/3/4. Only select Major or GSS system type if you have verified with the NCI ISSO that yours is one of these two types.
4. Fill in the date the FIPS was completed
5. Choose the appropriate overall system security rating by choosing the highest watermark of all final adjusted confidentiality, integrity, and availability ratings given on the subsequent pages of the FIPS-199 form (e.g., Choose Moderate if your highest individual rating is Moderate, even if all other ratings are Low)
6. Fill in the current SDLC status form the dropdown box options
7. Enter the highest watermark rating for each of the categories by using the dropdown lists. You will enter the highest adjusted Confidentiality, Integrity, and Availability (C-I-A) ratings noted on page 3. For example, if you have more than one information type, then choose the highest value for each category (C-I-A) and enter it on Page 1 in the appropriate dropdown box.

Step 2/Page 2: Fill in the System Description and POCs

1. On page 2, Provide the official system description. The description should include enough detail to explain the general purpose of the system and should note whether the system is publicly accessible, if it includes any sensitive or restricted access information, and the approximate number of users if known.
2. List the designated POCs. The only name that should change from system to system is the System Owner name. The system owner name should be the federal business owner/sponsor. The other names are Jeff Shilling (CIO), Bruce Woodcock (ISSO), and Suzanne Milliard (Privacy Coordinator).
3. Once the form has been completely filled in, all three of the provided signature blocks must be completed by their designated representatives. The form supports electronic signatures in MS Word or you can print and apply traditional "wet" signatures if you choose. If you are unable to apply more than one digital signature, then please print the form and have each person apply a wet signature by pen.

Step 3/Page 3: Provide applicable Information Categories and Adjusted Impact Ratings

1. Refer to NIST 800-60 Volume 2 for a catalog of common federal information categories. If you are unsure what categories to use, please contact the NCI ISSO for help be emailing NCIIRM@nih.gov, or by calling 240-276-5159.
2. Choose the appropriate category(ies) from 800-60 V2 that capture the primary function and mission of your system by entering them in one of the Category boxes on page 2
3. Enter the provisional impact ratings (provisional ratings are given in 800-60 V2 for each selected information type, but you may need to adjust ratings based on additional considerations. If you do need to adjust the ratings, enter an adjusted rating in the Adjusted Impact Levels area for each information category used.
   - If you adjust any of the provisional impact ratings, then you MUST provide a rationale for the adjustment(s) in the Rationale box. The rationale box only needs to be completed if you have adjusted one or more provisional ratings. For example, if are provisional impact rating for confidentiality is Low, but you wish to adjust the rating to Moderate, then you need to address why you have raised the confidentiality rating in the rationale box.
4. If you need to use more than one information category, repeat steps 2 and 3 until you have entered all of the appropriate information categories

NOTE: Most systems can be described by using just 1 or 2 information categories from NIST 800-60 Volume 2. In rare cases, a system owner might need to use more than that, but be careful not to choose categories that are a "stretch" or that are not part of the mission/function of the system. Usually, a careful review of the description in 800-60 Volume 2 will help avoid un-necessary inclusion of additional categories.

FIPS-199 resources

- Blank template - FIPS-199
- NIST 800-60 Volume II Appendices