FISMA Security Templates and Forms

The links for security and privacy forms and templates listed below have been divided by functional areas to better assist you in locating specific forms associated with security and/or privacy related activities that are described elsewhere in the NCI IT Security Website.

Prepare (RMF Step "0")

- ATO Schedule

Categorize System and Select Controls (FISMA Starter Kit) (RMF Steps 1 & 2)

- FIPS-199 System Categorization (FIPS-199)
  - NIST SP 800-60 Volume 1 (Mapping Guidelines)
  - NIST SP 800-60 Volume 2 (Information Types w/ provisional security impact level assignments)
- E-Authentication Risk Assessment (E-Auth)
- Privacy Impact Assessment (PIA) (right click and save to open)
- NCI Business Impact Analysis (BIA)

Implement Controls (RMF Step 3)

System Security Plans (SSPs)

- FISMA Moderate SSP (for non-cloud systems categorized as **Moderate** only)
- FISMA Low SSP (for non-cloud systems categorized as **Low** only)
  - NIH Information Security Policy Handbook (Security Policies and Security Control Implementation Requirements) (FOUO - Request from NCI ISSO Office)

System Standard Operating Procedure (SOP) templates

- NCI Identity and Access Management (IdAM)
- NCI Audit Management
- NCI System Physical and Environmental Control
- NIH IT General Rules of Behavior (RoB)

Configuration management

- Configuration Management Plan (CMP)
- NIH Memorandum of Understanding (MOU)
- Interconnection Security Agreement (ISA)
- HHS/NIH Department Standard Warning Banner

Contingency planning and disaster recovery templates

- NIH Contingency Plan (CP)
- NIH Contingency Test Plan and After-Action Report

Incident response planning templates

- NIH Incident Response Plan (IRP)
- NIH Incident Response Plan Test

Assess Controls (RMF Step 4)

- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of action and milestones (POA&M)

Authorize System (RMF Step 5)

- Authority To Operate Letter (ATO)

Monitor System (RMF Step 6)

- Security Impact Analysis (SIA)
- Annual Assessment (AA) Guidance
  - AA Security Control Matrix by Fiscal Year (list of security controls to be assessed during AA)
    - AA Supplemental Testing Guidance (guidance on testing and evidence to be requested during AA)