FISMA Starter Kit Help

All new information systems require that the following forms be completed to establish an information system's security-impact rating, authentication requirements, privacy implications, and mission criticality:

- FIPS-199 System Security Impact Categorization (FIPS-199)
- E-Authentication Risk Assessment (E-Auth)
- Privacy Impact Assessment (PIA)
- Business Impact Analysis (BIA)

We refer to these forms collectively as the "security starter kit" because they need to be completed before any other security compliance work begins. The information needed for these forms also helps define a system's security and privacy requirements. The starter kit is a precursor to the formal FISMA authorization that is required prior to a system going live.

The information below will help you complete the starter kit.

Form Titles	Purpose	Responsibilities
FIPS-199	Establishes a system's security-impact rating based on confidentiality, integrity, and availability requirements.	You must work with the Information System Security Officer (ISSO) to complete this form to ensure the correct information categories and ratings are applied to your system. Send any questions to NCIIRM@mail.nih.gov.
E-Auth	The E-Authentication Risk Assessment (E-Auth) establishes the appropriate identity proofing and authentication requirements for remote users.	The system owner or project manager completes the eAuth. The completed E-Auth form must be signed by the system owner.
PIA (right click and save to open)	Helps determine whether any information covered by the Privacy Act is collected, processed, or stored in your system.	The NIH privacy review process and all PIAs are governed by the NIH Office of the Senior Official for Privacy (OSOP). Contact the NCI Privacy Coordinator to start the PIA, and the NCI ISSO for assistance with security-related questions in the PIA.
BIA	The BIA captures the mission essential functions supported by a system, identifies dependencies, and defines recovery time objective, recovery point objective, and maximum tolerable downtime.	The system owner or project manager completes the BIA. The completed BIA must be signed by the system owner and ISSO.

Send any questions to NCIIRM@mail.nih.gov