

May 4, 2026 Outline

Reading: *text*, §20, 22–22.2

Due: Homework #3 due May 11; Project progress report, due May 11

1. Policy and requirements
 - (a) Security specifications
 - (b) Problems with precision
 - (c) Example: System X and Bell-LaPadula
 - (d) Justifying requirements
2. Design documents
 - (a) Security functions summary specification
 - (b) External functional specification
 - (c) Internal design description
3. Justifying design meets requirements
 - (a) Reviews
4. Techniques to support implementation assurance
 - (a) Implementation considerations
 - (b) Implementation management
 - (c) Testing
5. Operation and Maintenance Assurance
6. Evaluation criteria
 - (a) Trusted Computer Security Evaluation Criteria (TCSEC, Rainbow Series)