RISK DEFINITIONS

This handout lists the risk areas identified in OMB Circular A-11, as presented in the NIST Integrating IT Security into Capital Planning and Investment Process Workshop.

1. **Schedule:** Risk associated with schedule slippages, either from lack of internal controls or those associated with late delivery by vendors, resulting in missed milestones.

2. **Initial costs:** Risk associated with "cost creep" or miscalculation of initial costs that result in an inaccurate baseline against which to estimate and compare future costs.

3. **Life-cycle costs:** Risk associated with misestimating life-cycle costs and exceeding forecasts, reliance on a small number of vendors without sufficient cost controls.

4. **Technical obsolescence:** Risk associated with technology that becomes obsolete before the completion of the life cycle and cannot provide the planned and desired functionality.

5. **Feasibility:** Risk that the proposed alternative fails to result in the desired technological outcomes; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.

6. **Reliability of systems:** Risk associated with vulnerability/integrity of systems.

7. **Dependencies and interoperability between this investment and others:** Risk associated with interoperability between other investments; risk that interoperable systems will not achieve desired outcomes; risk of increased vulnerabilities between systems.

8. **Surety (asset protection) considerations:** Risk associated with the loss/misuse of data or information; risk of technical problems/failures with applications; risk associated with the security/vulnerability of systems.

9. **Risk of creating a monopoly for future procurements:** Risk associated with choosing an investment that depends on other technologies or applications that require future procurements to be from a particular vendor or supplier.

10. **Capability of agency to manage the investment:** Risk of financial management of investment, poor operational and technical controls, or reliance on vendors without appropriate cost, technical and operational controls; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.

11. **Overall risk of project failure:** Risk that the project/investment will not result in the desired outcomes.

12. **Project resources/financial:** Risk associated with "cost creep," miscalculation of life-cycle costs, reliance on a small number of vendors without cost controls, or (poor) acquisition planning.

13. **Technical/technology:** Risk associated with immaturity of commercially available technology and reliance on a small number of vendors; risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality.

14. **Business/operational:** Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or initiative will not be achieved; risk that the investment will not achieve operational goals; risk that the program effectiveness targeted by the project will not be achieved.

15. **Organizational and change management:** Risk associated with organizational-, agency-, or government-wide cultural resistance to change and standardization; risk associated with bypassing or lack of use or improper use or adherence to new systems and processes because of organizational structure and culture; inadequate training planning.

16. **Data/information:** Risk associated with the loss or misuse of data or information, risk of compromise of citizen or corporate privacy information; risk of increased burdens on citizens and businesses because of data collection requirements if the associated business processes or the project (being described in the Exhibit 300) requires access to data from other sources (federal, state, and/or local agencies).

17. **Security:** Risk associated with the security/vulnerability of systems, web sites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the evolution of credible threats; risk associated with the misuse (criminal/fraudulent) of information; must include level of risk (high, medium, basic) and what aspect of security determines the level of risk (e.g., need for confidentiality of information associated with the project/system, availability of the information or system, or reliability of the information or system).

18. **Strategic:** Risk associated with strategic/government-wide goals (i.e., President's Management Agenda and e-Gov initiative goals); risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them.

19. **Privacy:** Risk associated with the vulnerability of information collected on individuals or risk of vulnerability of proprietary information on businesses.