Background and Purpose

With the proliferation of new technology and global interconnectivity, public key cryptographic technology has become a vital security tool for ensuring the integrity, privacy, authenticity, and non-repudiation of electronic information exchanges. Primarily, public key algorithms are used for: (1) cryptographic key exchange; (2) data encryption; and (3) digital signature generation and verification. As more Federal agencies begin to employ new advances in technology in a broad range of public service and business functions, enabling informational exchanges with vast numbers of diverse trading partners, there are greater needs for public key cryptographic technology. To effectively implement this security approach on a broad scale, the use of cryptographic technology must be combined with the development of infrastructure service support. For this purpose, the Federal Public Key Infrastructure (FPKI) Steering Committee was commissioned to facilitate a lead advisory role to guide Federal agencies, executive agents, and the Government Information Technology Services (GITS) Board on matters germane to the public key infrastructure; interoperability; business functions, technical, legal, and policy. In this capacity, the FPKI Steering Committee has chartered three working groups under its direction that will lend specific expertise as required on business, technical, legal and policy matters. The role of the Business Working Group is established under this Charter.

Mission and Responsibility

The Business Working Group (BWG) will function as one of three working arms of the FPKI Steering Committee. The other two working groups are Technical, and Legal and Policy. The BWG will operate at the discretion of , and will respond to, specific requests for action by the FPKI Steering Committee on matters pertaining to FPKI business requirements, including, but not limited to: research on technology; business trends in government and industry; current business applications in government; identifying security products used; architectures; interoperability; provide a forum for information exchanges and outreach, inter-agency coordination, provide recommendations for pilots, and research projects for developing business cases. The BWG will interact and work in cooperation with the technical, and legal and policy working groups. It is understood that interactions between the BWG and the other two working groups will include informational exchanges on cross-cutting issues, requests for comments, and general research activities. Any BWG activities that result in the need for major project action from the other two working groups will be coordinated through the FPKI Steering Committee Chair, and as determined by the Chair, presented to the FPKI Steering Committee for approval. Final recommendations of the BWG to the FPKI Steering Committee will be determined by consensus of the voting members present during the time of vote. Other positions presented will be identified.

Membership

Membership and voting privileges in the BWG will be open to all Federal agencies who are participating in the public key cryptography pilots. Representatives from other Federal agencies including the Office of Management and Budget and the General Accounting Office may participate, but without voting privilege. Representatives from non-Federal agencies, such as State and local entities, universities or private industry

involved in PKI may be invited to meetings as determined, but will not have voting privileges.

Role and Action Plan
All BWG members will be expected to attend monthly meetings, and actively participate in discussions and actions required. The BWG will develop a general work plan, which may be revised from time to time. The work plan will serve as a functional operating instrument that will direct the activities of the BWG, and outline the expected results to be achieved under the auspices of this Charter.

Approval
/s/ 11/22/96 _____