FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL
Policies and Procedures Manual

PART	**I**	**Operations Policies and Procedures**
SECTION	**OIG-110**	**General Management Policies and Procedures**
CHAPTER	**110.10**	**OIG Guidance on the Use of Personal Digital Assistants at FDIC**

1. Purpose. This policy provides guidance on the implementation of FDIC Circular 1380.4, *FDIC's Policy on the Use of Personal Digital Assistants (PDAs)*, within the Office of Inspector General (OIG).

2. Scope. This policy applies to all FDIC OIG employees and FDIC OIG contractors who use PDAs on the FDIC network.

3. Policy. The OIG will comply with the policies and provisions for PDA use, as specified in Circular 1380.4. The provisions specified in this chapter supplement that circular and provide detailed requirements addressing the authorization and approval of PDAs within the OIG, as well as guidance regarding sensitive information as it relates to the use of PDAs. It is the policy of the OIG that:

a. Corporate-owned PDAs must be properly authorized and approved.

b. Employee-owned or contractor-owned PDAs that are used to exchange information utilizing the FDIC network must be properly authorized and approved.

c. Corporate-owned PDAs, employee-owned PDAs, and contractor-owned PDAs may not be used to transmit or store FDIC information that is of a sensitive or non-public nature.

4. Background. PDAs are palm-sized computing devices that provide access to locally stored information, email, and the Internet. The FDIC Division of Information Resources Management (DIRM) places responsibility on each FDIC office for ensuring that PDA use within their offices is adequately authorized and that employees exercise secure information practices when using PDAs. Generally, wireless connections lack sufficient security and should not be used as a mode to transmit or store sensitive data.

5. Responsibilities. The Assistant Inspector General for Management and Congressional Relations is the OIG's Authorizing Official (AO) for PDAs and is responsible for approving all PDA use within the OIG and for ensuring that the OIG's PDA policy is in accord with and adequately supplements FDIC Circular 1380.4.

a. The AO is assisted by the OIG Information Security Manager (ISM). All completed Request for PDA Forms (FDIC Standard Form 1380/08, Page 1) and associated PDA Service Agreements (FDIC Standard Form 1380/08, Page 2) should be submitted to the ISM for review to ensure that the forms are complete and the requestor is aware of the related FDIC and OIG policies and procedures. The ISM will maintain the original signed PDA Request Forms and PDA Service Agreements on file and, if necessary, forward copies of the forms to the DIRM National Technical Call Center (DIRM NTCC) for processing.

b. Those individuals within the OIG that meet all requirements to be assigned an FDIC-owned PDA must follow the policies and procedures as outlined in both FDIC Circular1380.4 and this OIG PDA policy. A Request for PDA Form (FDIC Standard Form 1380/08, Page 1) and PDA Service Agreement (FDIC Standard Form 1380/08, Page 2) must be completed, signed, and submitted to the OIG ISM.

c. OIG employees or OIG contractors may use their own PDA to establish a link between their personally owned PDA and the FDIC network provided they follow the policies and procedures as outlined in both FDIC Circular 1380.4 and this OIG PDA policy. A Request for PDA Form (FDIC Standard Form 1380/08, Page 1) and a PDA Service Agreement (FDIC Standard Form 1380/08, Page 2) must be completed and submitted for supervisory review. The supervisor or oversight manager should indicate their approval by initialing Section IV of the Request for PDA Form (FDIC Standard Form 1380/08, Page 1). The completed Request for PDA Form (FDIC Standard Form 1380/08, Page 1) and PDA Service Agreement (FDIC Standard Form 1380/08, Page 2) should then be submitted to the OIG ISM.

6. Protection of Sensitive Information. Corporate-owned PDAs, employee-owned PDAs, and contractor-owned PDAs may not be used to transmit or store FDIC information that is of a sensitive or non-public nature. Because of the broad range of activities conducted by the OIG and the diverse situations it encounters in carrying out its mission, it is not practical to provide a comprehensive description of information considered sensitive or non-public throughout the OIG. OIG personnel are expected to exercise their own discretion and sound judgment in determining the types of information that should not be transferred to their PDAs. Additional guidance on the types of information considered sensitive in email is contained in Section 8 of FDIC Circular 1310.5, *Encryption and Digital Signatures for Electronic Mail.*

7. Contact. Questions regarding this policy should be directed to the OIG ISM.