



***Federal Housing Finance Board
Office of Supervision***

Date: February 13, 2002
To: Federal Home Loan Bank Chairs, Presidents and Directors of Internal Audit
From: Gwen R. Grogan, Acting Deputy Director
Office of Supervision
Subject: Disaster Recovery Planning

Background:

Guidance: The Office of Supervision encourages each FHLBank to consider the following when evaluating its disaster recovery planning:

Disaster Recovery Plan (DRP)

- ❑ The DRP process should consider every type and magnitude of disaster, including the total destruction of the headquarters building.
- ❑ The DRP should address losing one or more (or combinations) of the following critical components of the business: people, physical space, information systems, communications, and records.
- ❑ In addressing the above five critical components, the DRP should focus on three key areas: internal communications, external communications, and the FHLBank's systems that transact money and securities.
- ❑ The DRP should address transportation, temporary equipment and space considerations.
- ❑ Each FHLBank should focus on incorporating drills and exercises into the DRP and executing them on a regular basis.
- ❑ The DRP should provide for a broad-based recovery team that would meet daily to review what has been done and determine what remains to be done.

Disaster Recovery Site (DRS)

- ❑ The DRS should be able to effectively replicate the operation of the primary data center, with effectively real-time data back up a strong consideration.
- ❑ Each FHLBank should consider the benefits (in terms of reliability, effectiveness, and cost) of setting up its own dedicated site, rather than using a vendor.



- ❑ The DRS should be tested regularly, including operational drills that include traveling to and operating from the DRS.
- ❑ Basic supplies, including check paper and master forms, should be available at the DRS.
- ❑ Distance from the primary FHLBank site and employee accessibility should be considerations in locating the DRS.

Communications

- ❑ In the event of a disaster, effective communications, both internally and externally, are key.
- ❑ In the event a FHLBank building has to be evacuated, the DRP should identify an external assembly area for staff away from the building.
- ❑ A communication tree should be in place identifying key employees to act as communication facilitators.
- ❑ The communication tree should include an employee list, updated regularly, with all available means of communication, including home telephone, cell phones, and email.
- ❑ The Office of Finance should be a key emergency contact, as it has established lines of communication with the other FHLBanks and the Federal Reserve.
- ❑ Each FHLBank's website is an important tool for communicating with employees and the public including customers.

Business Continuation

- ❑ Several key employees need to have the prior day's advance and collateral positions and projected cash flows accessible to them at all times.
- ❑ Each FHLBank should consider a hierarchy of business activities while operating in disaster recovery or business continuation mode, emphasizing meeting liquidity needs and possibly restricting complex or high resource requirement transactions.
- ❑ Each FHLBank should maintain a strong working relationship with the Federal Reserve to facilitate interactions with the Federal Reserve should the FHLBank be unable to operate in its normal manner.
- ❑ Key employees should be advised of the location the Federal Reserve's operations center in the event the Federal Reserve requires on-site authentication for transactions.
- ❑ Each FHLBank should consider designating another FHLBank to act as agent for the FHLBank, thereby granting all the legal authorities to conduct business on a temporary basis for the FHLBank.
- ❑ In assessing a FHLBank's travel policy, the board of directors and management should consider limiting the concentration of key staff traveling together or attending a conference or meeting, thereby placing FHLBank operations at risk in the event of a disaster.



Records

- ❑ Important documents and records should be kept on a common computer network drive, rather than exclusively maintained on individual hard drives, diskettes, or CDs.
- ❑ Critical documents should be identified and copies maintained at different locations. Critical documents include: insurance policies, building leases and documents needed to transact daily business, such as member signature cards.
- ❑ Consideration should be given to implementing an imaging program to lessen the impact of any loss of critical documents.