Appraisal Subcommittee

Federal Financial Institutions Examination Council

TO: State Appraiser Regulatory Officials

FROM: Jim Park, Executive Director

DATE: July 1, 2013

RE: Safeguarding Access to the National Registry

Revised Policy Statement 3, *National Registry*, effective June 1, 2013, requires States that access the National Registry directly through the ASC extranet application to adopt and implement a written policy to protect access as well as ASC issued user names and passwords. This policy must include, among other things, written designation of Authorized Registry Officials (ARO) with the authority to request National Registry access for staff members. A policy compliant with Revised Policy Statement 3 must be in writing and, at a minimum, address the following requirements:

1. Designation of authorized users for each permission level. Each user must be assigned an access permission level. There are three secure permission levels for the National Registry: (1) User, which gives access only to viewing the non-public side of the Registry; (2) Extranet User, which allows viewing of the non-public side of the Registry as well as the ability to make changes directly to the National Registry data for that State; and (3) File Transfer User, which allows users to securely upload data files to the ASC extranet application for processing by ASC staff.
2. Making requests to the ASC for additional users as well as informing the ASC of the termination of access privileges for any user or a change in access level.
3. Safeguarding passwords and other user identification, including a prohibition on sharing logon information.
4. Appropriate restrictions on hardware and use of virus protection software including requirements that all users log off of the Registry at the end of each work-day and that lockouts occur during reasonable periods of absence.
5. Maintenance of records adequate to demonstrate compliance with all elements of the State's policy.

Attached is a sample of a State National Registry policy which would be acceptable to the ASC.

States are responsible for ensuring the integrity of their access to the National Registry. Failure to ensure that integrity, consistent with the requirements of Policy Statement 3, may result in a denial of access to the National Registry.

1401 H Street, NW • Suite 760 • Washington, DC 20005 • (202) 289-2735 • Fax (202) 289-4101

Sample National Registry Access Policy

The Appraisal Subcommittee (ASC) of the FFIEC has issued Policy Statement 3, *National Registry,* which requires that States using the ASC's extranet application for submission of data to the National Registry (Registry) have a written policy governing access to the Registry. This requirement also applies to States with access to the Registry's full data base. The [insert name of STATE REAL ESTATE APPRAISAL REGULATORY ENTITY] adopts this policy as required by the ASC.

The [Board/Commission/Agency] will appoint a senior official of the [Regulatory Entity] as [insert State name] Authorized Registry Official (ARO) and notify the ASC in writing of this appointment. The notification will include the ARO's full name, contact address and telephone number, and position with [Regulatory Entity]. The notification will also contain any restrictions on the ARO's authority to designate additional users and levels of access for those additional designees. Unless otherwise noted in the ARO designation provided to the ASC, the ARO may designate access under any of three secure permission levels for the Registry: (1) User, which gives access only to viewing the non-public side of the Registry; (2) Extranet User, which allows viewing of the non-public side of the Registry as well as the ability to make changes directly to the National Registry data for that State; and (3) File Transfer User, which allows users to securely upload data files to the ASC extranet application for processing by ASC staff. Each such designation shall be in writing sent to the ASC, and shall identify the individual, level of access to be granted and contact information for that designee. The ASC will, on receipt of such designation, issue a User Name and password unique to that designee.

The ARO will ensure that the list of designated users for the Registry is accurate and that the ASC is notified promptly of any changes to the designated users such as termination of access privileges, changes to access levels, etc. Requests for additional users will be made by the ARO in writing and will identify the individual, level of access requested and contact information for the additional user. All records related to access to the Registry will be maintained for X years.

The ARO will develop an education program required of all users of the Registry prior to initial use. This program will, at a minimum, include the following:

1. User name and password security. Users will not share passwords or user names with anyone, including other associates, management personnel or technical personnel. Passwords are not to be written, displayed or stored where another person may access or see them.
2. Access security. Users may not log on to the Registry with any other user's identification or otherwise have unauthorized access to the Registry. All users must log off of the Registry at the end of each workday, and prior to any extended absence during the workday. As an alternative to logging off of the Registry during the workday users may lock all equipment used to access the Registry in such manner that a password is required to unlock the equipment. This option must be verified by technical personnel and records of this verification maintained.
3. Software security. All equipment used to access the Registry must have adequate anti-virus software installed. Technical personnel will verify installation of anti-virus software and will

ensure that such software is kept current. Written records of verifications and updates will be maintained.

Users of the Registry are responsible for all access made with their User Name and password. Unauthorized access to Registry data may result in violations of State and Federal laws and expose the State to civil penalties. Unauthorized access or failure to comply with the requirements of this Policy may constitute grounds for disciplinary action and/or termination. The ARO must immediately notify the ASC and the [Board/Commission/Agency] of any known or suspected breach of security involving the Registry or its data and provide a description of the known or suspected breach.