

Federal Reserve Bank of San Francisco  
101 Market Street, San Francisco, California 94105

April 17, 2014

To State Member Banks,  
Bank Holding Companies, Financial  
Holding Companies, Savings and Loan  
Holding Companies, and Foreign Banking Offices  
in the Twelfth Federal Reserve District

**FFIEC: OpenSSL “Heartbleed” Vulnerability Alert**

On April 10, 2014, the Federal Financial Institutions Examination Council (FFIEC) members, which include the Board of Governors of the Federal Reserve System, issued [an alert on OpenSSL “Heartbleed” Vulnerability](#). OpenSSL is software used to authenticate services and encrypt sensitive information. A significant vulnerability has been found in OpenSSL that could allow an attacker to decrypt, spoof, or perform attacks on network communications that would otherwise be protected by encryption.

The agencies expect financial institutions to incorporate patches on systems and services, applications, and appliances using OpenSSL and upgrade systems as soon as possible to address the vulnerability. Financial institutions should consider replacing private keys and X.509 encryption certificates after applying the patch for each service that uses OpenSSL and consider requiring users and administrators to change passwords after applying the patch. Financial institutions relying upon third-party service providers should ensure those providers are aware of the vulnerability and are taking appropriate mitigation action.

**Additional Information**

All circulars and documents are available on the Internet through the Federal Reserve Bank of San Francisco’s website, at <http://www.frbsf.org/banking-supervision/publications/district-circular-letters>.

For additional information, please contact:

Federal Reserve Bank of San Francisco  
Banking Supervision and Regulation  
(415) 974-2243  
(415) 974-2923