PRESS RELEASE
Federal Deposit Insurance Corporation ● Each Depositor insured to at least $250,000

April 10, 2014

Media Contact:
Greg Hernandez (202) 898-6993
Email: mediarequests@fdic.gov

FDIC Urges Financial Institutions to Utilize Available Cyber Resources

FOR IMMEDIATE RELEASE

The Federal Deposit Insurance Corporation (FDIC) today urges financial institutions to actively utilize available resources to identify and help mitigate potential cyber-related risks. It is important for financial institutions of all sizes to be aware of the constantly emerging cyber threats and government-sponsored resources available to help identify these threats on a real-time basis.

"Cyber threats have been widely covered in the national media, and we believe that financial institutions and their technology service providers have been managing system updates to mitigate potential vulnerabilities in an effective manner. As discussed in yesterday's meeting of the FDIC Advisory Committee on Community Banking, financial institutions may benefit from greater awareness of the resources available to identify cyber-related risks as quickly as possible," said Doreen Eberley, Director of the FDIC Division of Risk Management Supervision.

Financial institutions should ensure that their Information Security staff are aware of and subscribe to reliable and recognized resources that can help quickly identify cyber risks as they emerge. Government and government-sponsored resources that financial institutions should consider include the following organizations.

United States Computer Emergency Readiness Team (US-CERT)
The Department of Homeland Security's US-CERT facilitates the coordination of cyber information sharing and provides cyber vulnerability and threat information through its national Cyber Awareness System (NCAS). Financial institutions may learn more about US-CERT and subscribe to receive security alerts, tips and other updates through its website at www.us-cert.gov.

FDIC

Congress created the Federal Deposit Insurance Corporation in 1933 to restore public confidence in the nation's banking system. It promotes the safety and soundness of these institutions by identifying, monitoring and addressing risks to which they are exposed. The FDIC receives no federal tax dollars — insured financial institutions fund its operations.

FDIC press releases and other information are available on the Internet at www.fdic.gov, by subscription electronically (go to www.fdic.gov/about/subscriptions/index.html) and may also be obtained through the FDIC's Public Information Center (877-275-3342 or 703-562-2200). PR-28-2014

U.S. Secret Service Electronic Crimes Task Force (ECTF)

The Electronic Crimes Task Force teams local, state and federal law enforcement personnel with prosecutors, private industry, and academia to maximize what each has to offer in an effort to combat cyber criminal activity. For more information on the Electronic Crimes Task Forces please visit www.secretservice.gov/ectf.shtml.

FBI InfraGard

InfraGard is an information sharing forum between the FBI and the private sector. InfraGard operates more than 60 chapters that conduct local meetings pertinent to their area. Information about InfraGard may be obtained at www.infragard.org.

Regional Coalitions

The financial services sector has several regional coalitions established to enhance partnerships between private sector companies and state, local or regional governments. To find a regional coalition near you, please visit www.rpcfirst.org.

Information Sharing and Analysis Centers (ISACs)

Information Sharing and Analysis Centers provide risk mitigation information, incident response, alerts and facilitate information sharing among members. To find out more about the ISAC model, visit the National Council of ISACs at www.isaccouncil.org.

Financial institutions also are reminded that they may obtain information specific to products or applications they use at the applicable vendor websites. Additionally, financial institutions that utilize third party service providers should check with their provider about the existence of user groups that also could be valuable sources of information.

# # #