# GAO Finds Deficiencies In Federal Bank Regulators' Examination Procedures

By Thomas A. Brooks / Jul 10, 2015

In a just released Report critical of the federal banking regulators (Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration), the Government Accountability Office (GAO) found that the regulators were deficient in their ability to properly examine depository institutions' ability to protect against cyber risks.

GAO conducted the study because it found that depository institutions have lost hundreds of millions of dollars in recent years due to cyber attacks. The GAO examined how regulators oversee institutions' efforts to mitigate cyber threats and reviewed the ability of banking agencies to share cyber threat information with one another.

Because of the expected continued increase in cyber attacks, examination of these threats by the federal regulators is a high priority. The GAO found that the regulators devoted considerable resources to oversee larger institutions, but "limited [information technology (IT)] staff resources generally means that examiners with little or no IT expertise are performing IT examinations at smaller institutions." This experience disparity may result in a greater degree of adverse examination outcomes in regional and community banks.

One GAO finding was that while federal rules call for banks' internal control standards to include reliable and timely information on activities relating to cyber security, the regulators were not "routinely collecting IT security incident reports and examination deficiencies and classifying them by category of deficiency." The GAO determined that having such information would better enable regulators to determine trends across institutions and use that information to better target its examinations at individual institutions.

The Report also found that although most regulators have the ability to examine the risks posed by institutions' third party providers, the NCUA, which regulates credit unions, does not have the legal authority to do so. The GAO noted that cyber risks that affect a depository institution can originate from weaknesses in the security practices of third party providers of IT services to an institution. It recommended that Congress authorize the NCUA to conduct examinations of third party providers.

Ensuring that depository institutions are protected from cyber attacks is of critical concern for banking regulators. An institution's best protection from cyber attacks - and follow-on legal liability - is to have a program in place that protects against financial, operational, legal and reputational risks due to unauthorized cyber incursions. Strong programs include elements that protect information by preventing, detecting, and responding to attacks.

Clark Hill attorneys have extensive experience in dealing with the financial institution regulators and have formed an interdisciplinary team to assist entities in developing cyber security plans, including addressing the new Federal Financial Institutions Examination Council Cybersecurity Assessment Tool. For further information on how best to protect against cyber incursions, please contact Tommy Brooks (202) 552 2356, tbrooks@clarkhill.com or any member of the Clark Hill Cybersecurity, Data Protection & Privacy Group.

 