The following information was posted with the attached DRAFT document:

NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments has been Released
September 18, 2012

The National Institute of Standards and Technology (NIST) announces the release of the final version of its updated risk assessment guideline, Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments. The publication, over eighteen months in the making, represents the fifth in the series of publications developed by the Joint Task Force—a partnership among NIST, the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, to create a unified information security framework for the federal government.

Risk assessments play a critical role in the development and implementation of effective information security programs and help organizations address a range of security-related issues from advanced persistent threats to supply chain concerns. The results of risk assessments are used by organizations to develop specific courses of action that can provide effective response measures to the identified risks as part of a broad-based risk management process.

The comprehensive guidance in Special Publication 800-30, Revision 1 uses the key risk factors of threats, vulnerabilities, impact to missions and business operations, and the likelihood of threat exploitation of weaknesses in information systems and environments of operation, to help senior leaders and executives understand and assess the current information security risks to their organizations and information technology infrastructures. The risk assessment guidance has been designed to have maximum flexibility so the process can meet the needs of many types of organizations and communities of interest, large and small, including for example, financial institutions, healthcare providers, software developers, manufacturing organizations, military planners and operators, and law enforcement organizations.

The risk assessment guidance is consistent with the process for managing information security risk described in NIST Special Publication 800-39 that includes framing risk, assessing risk, responding to risk and monitoring risk over time—risks to the organization’s operations (including missions, functions, image, and reputation), the organization’s critical assets, individuals who are part of the organization or who the organization serves, other entities involved in partnerships or collaborative efforts with the organization, and the Nation at large (including critical infrastructure). The guidance also supports the three-tier, enterprise-wide risk management approach which focuses on: the organization’s governance structures; the organization’s core missions/business functions, mission/business processes, and enterprise architecture; and the organization’s information systems that are essential for mission/business success. Copies of Special Publication 800-30, Revision 1, can be obtained from the NIST Computer Security Division web site at: http://csrc.nist.gov/publications.