The following information was posted with the attached DRAFT document:

NIST Announces the Final Release of SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
April 30, 2013

NIST announces the final release of **Special Publication (SP) 800-53, Revision 4**, *Security and Privacy Controls for Federal Information Systems and Organizations*. Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005. The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. In addition, Special Publication 800-53 has been expanded to include eight new families of privacy controls based on the internationally accepted Fair Information Practice Principles.

Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. This "Build It Right" strategy is coupled with a variety of security controls for "Continuous Monitoring" to give organizations near real-time information that is essential for senior leaders making ongoing *risk-based* decisions affecting their critical missions and business functions.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the concept of overlays was introduced in this revision. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

Finally, there have been several new features added to this revision to facilitate ease of use by organizations. These include:

- Assumptions relating to security control baseline development;
- Expanded, updated, and streamlined tailoring guidance;
- Additional assignment and selection statement options for security and privacy controls;

- Descriptive names for security and privacy control enhancements;
- Consolidated tables for security controls and control enhancements by family with baseline allocations;
- Tables for security controls that support development, evaluation, and operational assurance; and
- Mapping tables for international security standard ISO/IEC 15408 (Common Criteria).

The security and privacy controls in Special Publication 800-53, Revision 4, have been designed to be largely policy/technology-neutral to facilitate flexibility in implementation. The controls are well positioned to support the integration of information security and privacy into organizational processes including enterprise architecture, systems engineering, system development life cycle, and acquisition/procurement. Successful integration of security and privacy controls into ongoing organizational processes will demonstrate a greater maturity of security and privacy programs and provide a tighter coupling of security and privacy investments to core organizational missions and business functions.

A markup version of Appendices D, F, and G containing security control and security control baseline changes from SP 800-53, Revision 3 to Revision 4 will be available NLT **May 7, 2013**. There will be additional download instructions for the markup appendices provided by a subsequent notification from the FISMA Implementation Project.

An updated (April 30, 2013) FISMA Implementation Project Schedule is available at: **http://csrc.nist.gov/groups/SMA/fisma/schedule.html**.

Questions or comments can be sent to **sec-cert@nist.gov**.