DRAFT Special Publication 800-53A Revision 4, *Federal Information Systems and Organizations: Building Effective Assessment Plans* has been approved as **FINAL** by the following publication:

Publication Number:	**Special Publication 800-53A Revision 4**
Title:	**Federal Information Systems and Organizations: Building Effective Assessment Plans**
Publication Date:	**December 2014**

- Final Publication: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

- Related Information on CSRC: http://csrc.nist.gov/publications/PubsSPs.html#800-53ar4
- Information on FISMA and supporting documents can be found on the CSRC FISMA project pages: *http://csrc.nist.gov/groups/SMA/fisma/*
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted announcing Special Publication 800-53A Revision 4 release from the CSRC News page:

Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, has been approved as final.
December 12, 2014

NIST announces the release of **Special Publication 800-53A, Revision 4**, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. This update to Special Publication 800-53A contains significant changes to the 2010 version of the publication in both content and format. The changes have been driven by **four** fundamental needs of federal agencies to include:

- The need for new or updated assessment procedures for the security controls defined in NIST Special Publication 800-53, Revision 4. *Security and Privacy Controls for Federal Information Systems and Organizations*;
- The need for a more granular breakdown of assessment objectives to support continuous monitoring and ongoing authorization programs;
- The need for a more structured format and syntax for assessment procedures that can support the use of automated tools for assessment and monitoring activities; and
- The need to support assessments of security capabilities and root cause analysis of failure modes for individual security controls or groups of controls.

By addressing the above needs, organizations will have the flexibility to:

- Define specific parts of security controls requiring greater scrutiny, monitoring, or assessment;
- More effectively tailor the scope and level of effort required for assessments;
- Assign assessment and monitoring frequencies on a more targeted basis; and
- Take advantage of potential new opportunities to conduct assessments of security capabilities including analysis of control dependencies.

There have also been some significant improvements in the current security assessment procedures based on feedback from federal agencies reflecting lessons learned during the conduct of actual assessments as part of the Risk Management Framework (RMF) process. The improvements include:

- Clarification of terminology;
- Expansion of the number of potential assessment methods and assessment objects on a per-control basis; and
- A simpler decomposition of assessment objects to align more closely with security control statements.

Finally, there is a continuation of the integration of privacy issues into the Joint Task Force publications. Privacy terminology has been integrated into SP 800-53A in a manner that is complementary to and supportive of the privacy controls defined in SP 800-53, Appendix J. The privacy assessment procedures that will eventually populate Appendix J in this publication are currently under development by a joint interagency working group established by the Best Practices Subcommittee of the CIO Council Privacy Committee. The new assessment procedures, when completed, will be separately vetted through the traditional public review process employed by NIST and integrated into this publication at the appropriate time.

The changes to the current security assessment procedures in SP 800-53A should result in significant improvements in the efficiency and cost-effectiveness of control assessments for federal agencies. Efficient and cost-effective assessments are essential in order to provide senior leaders with the necessary information to understand the security and privacy posture of their organizations and to be able to make credible, risk-based information security and privacy decisions.

This publication was developed by the *Joint Task Force Transformation Initiative Working Group* with representatives from the Civilian, Defense, and Intelligence Communities to produce a *unified information security framework* for the federal government. Please note that we have made a one-time change in the revision number of SP 800-53A (skipping revision numbers 2 and 3) so we can align the current publication revision to SP 800-53, Revision 4.