AN A.S. PRATT PUBLICATION
NOVEMBER 2017
VOL. 3 • NO. 11

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 3 NUMBER 11 NOVEMBER 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

NIST Releases Fifth Revision of Special Publication 800-53

By Susan B. Cassidy, Jennifer R. Martin, and Catlin M. Meade*

The authors of this article discuss the National Institute of Standards and Technology's proposed update to Special Publication 800-53, which provides information security standards and guidelines, for implementation on federal information systems under the Federal Information Systems Management Act of 2002.

The National Institute of Standards and Technology ("NIST") released on August 15, 2017 its proposed update to Special Publication ("SP") 800-53.[1] NIST SP 800-53, which was last revised in 2014, provides information security standards and guidelines, including baseline control requirements, for implementation on federal information systems under the Federal Information Systems Management Act of 2002 ("FISMA"). The revised version will still apply only to federal systems when finalized, but one of the stated objectives of the revised version is to make the cybersecurity and privacy standards and guidelines accessible to non-federal and private sector organizations for voluntary use on their systems.

THE PROPOSED REVISION

In its announcement[2] of the draft revision, NIST explains that the update

> responds to the need by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations, a comprehensive set of safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices.

---

* Susan B. Cassidy is a partner at Covington & Burling LLP advising clients on the complex rules and regulations imposed on government contractors, with a special emphasis on the defense and intelligence sectors. Jennifer R. Martin is of counsel in the firm's Data Privacy & Cybersecurity practice, and leads the firm's West Coast Cybersecurity practice. Catlin M. Meade is an associate at the firm advising clients on cybersecurity, privacy, and government contracts matters. The authors may be reached at scassidy@cov.com, jrmartin@cov.com, and cmeade@cov.com, respectively.

[1] http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf.

[2] http://csrc.nist.gov/publications/PubsDrafts.html#800-53r5.

In particular, a key purpose of the update process was to assess the relevance and appropriateness of the current security controls and control enhancements designated for each baseline (low, moderate, and high) to ensure that protections are commensurate with the harm that would result from a compromise of applicable government data and systems. In addition, the revised guidelines recognize the need to secure a much broader universe of "systems," including industrial control systems, IoT devices, and other cyber physical systems, than the "information systems" that were the focus of the prior iterations of SP 800-53. Relatedly, the revised publication also identifies those controls that are both security and privacy controls, as well as those controls that are the primary responsibility of privacy programs.

THE KEY CHANGES

This stated purpose, and expanded scope of the updated guidelines, is evident in some of the key changes to NIST SP 800-53, which include:

- Removing the term "federal" from the title and throughout the publication to deemphasize the federal focus of the publication and to encourage use of the guidelines by state, local, and tribal governments, as well as private sector organizations.
- Replacing the term "information system" with "system" throughout the publication to expand the scope of the guidelines in recognition of the threats to all types of systems (*e.g.*, industrial/process control systems, cyber physical systems, weapons systems, IoT devices, etc.).
- Adding and integrating privacy controls directly into the existing security control catalog. For example, control CM-4 SECURITY IMPACT ANALYSIS, has been changed as follows:

  > Control: ~~The organization a~~Analyzes changes to the ~~information~~ system to determine potential security *and privacy* impacts prior to change implementation.

- Changing the structure of the controls to make them more outcome-based by removing introductory term (such as "the organization" and "the information system") from the controls to focus on the capabilities, provide greater alignment with other NIST guidance and the NIST Cybersecurity Framework, and to reduce ambiguity. For example, control IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATION USERS), has been changed as follows:

  > Control: ~~The information system u~~*U*niquely identify~~ies~~ and authenticates organizational users (or processes acting on behalf of organizational users).

- Mapping the security and privacy controls of NIST SP 800-53 to international security and privacy standards, including ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 15408 (Common Criteria), and OMB Circular A-130 for ease of use by public and private entities. (Appendix I contains the mapping).
- Removing priority sequencing codes (*i.e.*, P0, P1, P2, P3) to eliminate confusion about the priority code designations and provide flexibility in the implementation of security and privacy controls.
- The revised guidelines also recognize that the controls and their applicability depend on specific technologies, environments, and business functions, and makes it easier for organizations to analyze the applicability of each control by: physically separating the control selection process from the catalog of controls; including tailoring considerations as a separate appendix (see Appendix G); adding control keywords to help users develop security and privacy plans and tailor the controls to their systems; and adding hyperlinks to help navigate through the document and access other related publications.

OMB CIRCULAR A-130

This update also represents a step in implementing OMB Circular A-130,[3] which was issued by the Obama administration in July 2016 and requires all federal agencies to adopt a risk-based approach to managing information and networks. The Circular includes two appendices, one on data security and another on privacy protections, which together provide guidance to federal agencies on managing information resources and personally identifiable information ("PII"). The NIST SP 800-53 revisions are responsive to the requirements imposed by the Circular, including mapping the Circular's privacy requirements to related controls in the publication.

NIST SP 800-53A

Typically, contractors that operate information systems on behalf of the government are also required to implement protections on those systems consistent with NIST SP 800-53. However, before agencies (and contractors) can implement the revised NIST SP 800-53, NIST will need to update NIST SP 800-53A,[4] "Assessing Security and Privacy Controls in Federal Information Systems and Organizations" to match the final NIST SP 800-53 security controls adopted by NIST.

---

[3] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

ADDITIONAL TASKS

The Department of Defense ("DOD") will have a number of additional tasks including:

- Publishing a revised edition of Committee on National Security Systems ("CNSS") Instruction 1253, "Security Categorization and Control Selection for National Security Systems." CNSS 1253 provides guidance on implementing (and tailoring) the security controls from NIST SP 800-53 for use in the DOD National Security System environment.
- Incorporating the new/revised security controls into the eMASS database. The eMASS computer application is managed by the Defense Information Systems Agency ("DISA") and is used as a tool when implementing the NIST Risk Management Framework ("RMF") for DOD information systems.

NEXT STEPS

NIST sought customer feedback regarding the relevance and appropriateness of the current security controls and control enhancements designated in each baseline, and that comment period ended on September 12, 2017. NIST has also published a markup of the security controls[5] showing the changes between revision four and proposed revision five. NIST has stated that it expects to release a final draft in October 2017, and for the final version to be published no later than December 29, 2017.

---

[5] http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft-controls-markup.pdf.