October 18, 2016

NIST SP 800-53 Revision 5 Status Update

PROJECTED PUBLICATION DATE FOR INITIAL PUBLIC DRAFT — MARCH 28, 2017

Greetings All,

Thanks very much for the input we have received for the initial public draft of SP 800-53 Revision 5. We really appreciate all of the valuable information from those "in the field" applying the guidelines and implementing the security and privacy controls. Our publications benefit greatly from your input.

We are making significant progress on the Rev 5 update. In addition to our usual update of security and privacy control content, NIST is considering some structural and formatting changes for SP 800-53 Rev 5 and we want to keep you informed about how the revision is shaping up. Please note that the proposed changes described below have **no effect** on the actual security and privacy controls, and organizations would **not** be expected to make updates to security plans, tools, or templates outside of the normal update schedule to accommodate these changes.

Here are a few proposed changes that you will likely see in the upcoming draft:

- Removal of the term "federal" from the title and throughout the publication to the extent appropriate. This change facilitates inclusiveness for all types of organizations (e.g., state, local, and tribal governments, industry, academia) and promotes the view that security and privacy are national areas of concern, not just for the federal government. At the same time, use of the guidelines by federal organizations (or any type of organization) is unaffected.
- Replacement of the term "information system" with "system" throughout the publication. This change facilitates inclusiveness for all types of systems (e.g., industrial/process control systems, cyber physical systems, weapons systems, IoT devices, etc.), while not affecting use within "information systems."
- Movement of the Program Management control family from Appendix G into Appendix F. This change helps streamline the catalog of controls for ease of use while only changing the location of the Program Management controls within the document.
- Movement of the Privacy controls from Appendix J into Appendix F. This change helps streamline the catalog of controls for ease of use and fosters a closer relationship between privacy and security. The closer relationship in turn facilitates more robust protection of information that is commensurate with risk.
- Removal of priority sequencing codes (i.e., P0, P1, P2, P3). This change eliminates ongoing misinterpretation about the intent of the priority code designations and gives organizations complete flexibility on the implementation sequence of security and privacy controls.

- Addition of ***keywords*** to security and privacy controls to facilitate searches for specific topics or related controls.
- Addition of ***hyperlinks*** to facilitate ease of movement between the control catalog and other sections of the document including tables and references.
- Removal of the introductory terms "The organization" and "The information system" from security and privacy controls. This change offers several short-term and long-term benefits to many communities using NIST guidance. In particular, this change:
  - Makes the security and privacy controls outcome-based by focusing on the security and privacy capabilities (i.e., what needs to be done to protect the system or information and not which entity carries out the action or where it is carried out);
  - Provides greater alignment and consistency with other NIST guidance (e.g., SPs 800-160 and 800-171, and the Cybersecurity Framework);
  - Gives organizations complete flexibility on how security and privacy controls are implemented and managed by removing implied limits on responsibility;
  - Eliminates confusion and ambiguity about the specific organizational element or hierarchical level of an organization that is best suited to implement and manage security and privacy controls;
  - Fosters innovation by allowing organizations to decide on control implementation; and
  - Facilitates collaboration with the systems engineering and acquisition communities by providing an adaptable structure and content in security and privacy controls that can be used by systems and product developers, systems integrators, procurement officials, and information security personnel.

    Here are a few examples of the control structure change:

    Current (Rev 4):

    SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

    Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

    Proposed (Rev 5):

    SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

    Control: Protect the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Current (Rev 4):

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Proposed (Rev 5):

CP-6 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Current (Rev 4):

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Proposed (Rev 5):

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

Current (Rev 4):

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control Enhancements:

(1) *Identification and Authentication | Network Access to Privileged Accounts*

The information system implements multifactor authentication for network access to privileged accounts.

Proposed (Rev 5):

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control Enhancements:

(1) *Identification and Authentication | Network Access to Privileged Accounts*

Implement multifactor authentication for network access to privileged accounts.

Please direct any questions or comments to sec-cert@nist.gov with “800-53 Rev 5 Update” in the subject line.

Ron Ross
ron.ross@nist.gov

Kelley Dempsey
kelley.dempsey@nist.gov

NIST SP 800-53 Revision 5 Project