Summary of Significant Changes Between NIST Special Publication (SP) 800-53, Revision 4 and the Final Public Draft (FPD) of NIST SP 800-53, Revision 5

Draft NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, represents a multi-year effort to develop the next generation security and privacy controls. The significant changes to the publication (from Revision 4) include:

- **Creating security and privacy controls that are more *outcome-based* by changing the structure of the controls.** The technical content of the control remains unchanged as a result of making the control statement more outcome-focused. Using AC-3, Access Enforcement, as an example:

NIST SP 800-53, Revision 4, AC-3:	**NIST SP 800-53, Revision 5, AC-3:**
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

  Appendix D, *Control Summaries* in Revision 5, indicates if a control or control enhancement is typically implemented by an information system through technical means with an "S" in the *implemented by* column. A control or control enhancement that is typically implemented by an organization (i.e., by an individual through nontechnical means) is indicated by an "O" in the *implemented by* column. A control or control enhancement that can be implemented by an organization or a system or a combination of the two, is indicated by an "O/S".

- **Adding two new control families for privacy and supply chain risk management.** The *Personally Identifiable Information Processing and Transparency* family addresses privacy risk management and the *Supply Chain Risk Management* family leverages and expands on technical concepts from the Revision 4 control, SA-12, Supply Chain Protection.

- **Fully integrating privacy controls into the security control catalog, creating a consolidated and unified set of controls.** NIST SP 800-53, Revision 4 added an appendix of privacy controls and related implementation guidance (Appendix J) based on the Fair Information Practice Principles. Revision 5 continues the incorporation of privacy into the control catalog by expanding the suite of privacy controls and moving them from an appendix into the fully integrated main catalog through integration with relevant security controls and a new family, *Personally Identifiable Information Processing and Transparency*. The expanded control catalog also includes specific references to OMB's guidance on breach response and the Foundations for Evidence-Based Policymaking Act of 2018.

- **Integrating the Program Management control family into the consolidated catalog of controls**. To facilitate ease of use and uniform presentation of control families, the Program Management (PM) family of controls was incorporated into the main control catalog.

- **Separating the control selection *process* from the *controls*—allowing controls to be used by different communities of interest.** Different organizations may elect to use different processes to select applicable controls. Revision 5 no longer includes selection guidance for the controls; that guidance can be found NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

- **Separating the control catalog from the control baselines**. To further support the use of Revision 5 by different communities of interest, the control baselines have been moved to NIST

SP 800-53B, *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations*, projected for publication in 2020. SP 800-53B also provides guidance for tailoring control baselines and for developing overlays to support security and privacy requirements of stakeholders and their organizations.

- **Promoting alignment with different risk management and cybersecurity approaches and lexicons, including the NIST Cybersecurity and Privacy Frameworks.** By separating the control selection process from the controls, the controls can be used to support other cybersecurity lexicons and risk management approaches.
- **Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks.** A new section in Chapter Two, Security and Privacy Controls has been added.
- **Incorporating new, state-of-the-practice controls based on threat intelligence, empirical attack data, and systems engineering and supply chain risk management best practices.** New controls in Revision 5:
  - Strengthen security and privacy governance and accountability;
  - Support secure system design; and
  - Support cyber resiliency and system survivability.
- **Supplemental Resources will be made available online pending final publication of SP 800-53, Revision 5.** Examples of supplemental resources include:
  - Mappings to ISO 27001 and ISO 15408;
  - Mappings to the NIST Cybersecurity and Privacy Frameworks;
  - Control and control enhancement keywords; and
  - SP 800-53 controls in machine-readable format (using Open Security Controls Assessment Language [OSCAL]).

A red-lined version of changes between Revision 4 and the Revision 5 ***will not*** be developed.