

# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS


(Updated: 4/27/2020)

The following list of questions and answers is based on the questions submitted during the April 8, 2020 virtual event: “**What’s New in Draft NIST Special Publication 800-53, Revision 5.**” Some of the questions were paraphrased to combine similar questions and comments, and to provide a more generalized answer. These questions and answers are also captured in the FISMA Implementation Project FAQ page at: <https://go.usa.gov/xvxtq>

For additional questions on the SP 800-53, Revision 5, Final Public Draft (FPD), please email: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

## Contents


<b>A. Public Comment</b> .....	6
A.1) What is the public comment review period for SP 800-53, Revision 5 (FPD)? .....	6
A.2) How long is the public comment period on SP 800-53, Revision 5 (FPD)?.....	6
A.3) How can I submit comments? .....	6
A.4) Can I submit comments after the public comment review period closes? .....	6
A.5) Will my comments be addressed in the final version of the document?.....	7
A.6) Will there be a third public comment period?.....	7
A.7) Is there a possibility of a deadline extension on the final public draft of SP 800-53, Revision 5?.....	7
A.8) What kind of feedback is NIST seeking?.....	7
<b>B. Changes/Dependencies</b> .....	7
B.1) What changed in this final public draft (FPD) version from the initial public draft (IPD)??	7
B.2) Will the Privacy Framework be updated with the release of SP 800-53, Revision 5?.....	7
B.3) Will the next revision to SP 800-161 utilize SP 800-53, Revision 5 controls? .....	8
B.4) What is the relationship between SP 800-53, Revision 5 and the NIST Privacy Framework and Cybersecurity Framework (CSF)? .....	8
B.5) Will NIST CSF be updated to align with SP 800-53, Revision 5? / With the new control tables, what is the impact to the NIST CSF? .....	8
B.6) Can you identify and explain the changes with the baselines (in forthcoming SP 800-53B)? .....	8
B.7) Will the “more than HIGH” baseline continue? .....	9
B.8) Why were baselines moved to a separate (SP 800-53B) document? .....	9



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

B.9) Will supporting NIST publications be updated to align with SP 800-53, Revision 5? (Specific Virtual Event inquiries included: SP 800-171, SP 800-171A, SP 800-137, SP 800-66, SP 800-34, SP 800-128, SP 800-66, Assessment Case Project, etc.) .....	9
B.10) When will NIST SP 800-18 be updated to include Privacy Plans?.....	9
B.11) Does draft SP 800-53, Revision 5 align with FIPS 140-3? .....	9
B.12) Will password length and maximum age guidance be aligned with updates to NIST SP 800-63-3 (i.e., passwords should not expire and length of password provides strength)? ..	9
B.13) Is there any input within draft SP 800-53, Revision 5 denoting the importance of how each control impacts different OSI layers at a technical/operational level?.....	10
B.14) Will there be a realignment of the OSCAL layers to reflect changes in draft SP 800-53, Revision 5? Where can we find more information on OSCAL? .....	10
B.15) Will the controls in SP 800-53, Revision 5 be mapped to and be implemented with other standards, guidelines, requirements, tools, solutions (e.g., CDM, FedRAMP, DISA STIGs, GPOs, CSAM, MITRE ATT&CK, MARS-E, CNSSI-1253)? .....	10
B.16) Will SP 800-53, Revision 5 replace the DISA STIGs? .....	10
B.17) How does SP 800-53, Revision 5 impact the CMMC and the DFARS?.....	11
B.18) Does NIST coordinate with other entities when developing publications such as SP 800-53, Revision 5? / Are new/updated controls tested against sample industries? .....	11
B.19) NIST SP 800-53, Revision 5 links to many other documents. Has NIST considered having living documents capable of supporting dynamic updates? / Will NIST reevaluate FISMA guidance development processes with an eye to a faster release schedule to better address changes in the threat landscape? / How does NIST expect the idea of putting the publication online, and doing incremental updates to work?.....	12
B.20) Will the update to FIPS be a revision to FIPS 200 or a new FIPS document altogether (e.g., “FIPS 201”)?).....	12
B.21) Does NIST plan to do mappings of the SP 800-53 controls to other standards, guidance and other resources? .....	12
B.22) What is the new guidance for SDLC? .....	12
B.23) Why were “information system” and “organization” removed from the control text? .	13
<b>C. Publishing</b> .....	13
C.1) When will the final version of SP 800-53, Revision 5 be released? .....	13
C.2) When will related publications (e.g., SP 800-53A, SP 800-53B) be released after SP 800-53, Revision 5 is finalized? .....	13
C.3) What is the publication plan for SP 800-172 (formerly SP 800-171B)?.....	13



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

C.4) What is NIST SP 800-53A? .....	13
C.5) What is NIST SP 800-53B? .....	14
<b>D. Resources</b> .....	14
D.1) What other formats are the controls available in? / Will the controls in SP 800-53, Revision 5 be available in other formats? / Would it be possible to provide control tables in SQL format? .....	14
D.2) Is NIST planning on summarizing significant changes from the 2017 initial draft of Revision 5 to the current draft? / Is there a mapping between the controls in Revision 4 to Revision 5? .....	14
D.3) Will NIST offer more reviews and dives into controls? / Will NIST develop training on control implementation? .....	15
D.4) Does NIST have any plans to develop templates for control family policies and procedures? .....	15
D.5) Does NIST offer training where one could obtain a CEU? / Can a CEU be obtained by attending the virtual event on the draft SP 800-53, Revision 5? .....	15
D.6) Will links to online resources be included in the SP 800-53, Revision 5? .....	16
D.7) Will NIST update the available overlays in the Knowledgebase? .....	16
D.8) Will there be more questionnaire / assessment supplementals to NIST publications? .....	16
D.9) If the government shuts down, will NIST resources (including publications and supplemental materials) be still available to the public? .....	16
D.10) Is it possible for NIST to release CSV versions of SP 800-53, SP 800-53A and SP 800-53B (all Revision 5) to facilitate the integration of the new requirements into existing toolsets? .....	16
D.11) Will there be desktop tools to work with OSCAL-based data? / Can NIST provide a demonstration of OSCAL and how it can be utilized? .....	17
D.12) Will NIST provide assistance with control auditing guidance? .....	17
<b>E. Implementation/Adoption</b> .....	17
E.1) Can organizations adopt SP 800-53, Revision 5 FPD before a final version is released? .....	17
E.2) Could NIST provide a guide identifying the most important controls that should be implemented based on the type of system? / Any thoughts about recommending a Critical Control List which is a subset of controls if agencies adopt this model, and CISO is more risk tolerant? .....	17
E.3) Can this publication work by itself if an organization has not implemented the Risk Management Framework (RMF)? .....	18




# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

E.4)	Where is the implementation guidance for “O” versus “S” for organization level and system level implementation of a specific control? .....	18
E.5)	Does SP 800-53, Revision 5 distinguish between documentation requirements for the enterprise versus for every system/FISMA boundary? .....	18
E.6)	Does SP 800-53, Revision 5 provide the frequency of review or recommended review frequency controls or will that still be the responsibility of the organization to determine? .....	18
E.7)	Is data tagging only for HIGH impact systems or mandated for all systems? .....	19
E.8)	Can NIST clearly denote how the control implementation and tailoring process are tied to ERM to function properly? .....	19
E.9)	Could NIST please elaborate more on implementing control enhancements? / How about companion document with "examples" of implementation statements for control? .....	19
E.10)	Will there be guidance for developing automated tools to implement and/or review control implementations? .....	19
E.11)	How soon after SP 800-53, Revision 5 is released will organizations need to implement the new controls? / Once SP 800-53, Revision 5 is released, how much time will organizations have to make the switch from Revision 4 to Revision 5? / Will the timeframe for implementation be set to one (1) year from final OMB approval? / Alignment with NIST updates are typically required one year after release. Would the clock start after the release of SP 800-53A? / It seems like the control requirements will be dynamic. Will there be a grace period for new requirements? .....	20
<b>F.</b>	<b>Notes to Reviewers Supplement: Notional Example: NIST SP 800-53 Controls Security and Privacy Collaboration Index</b> .....	<b>20</b>
F.1)	NIST: Thank you to all those who have submitted feedback on the Collaboration Index. ....	20
F.2)	What is the Security and Privacy Collaboration Index? .....	20
F.3)	What is the driver for the Collaboration Index? .....	21
F.4)	Why are there only three control families included in the Collaboration Index? .....	21
F.5)	What feedback is NIST requesting on the Collaboration Index? .....	21
F.6)	Is the Collaboration Index applicable to all controls in draft SP 800-53, Revision 5, or only to the three families featured in the notional example (in “Notes to Reviewers Supplemental Material”)? .....	22
<b>G.</b>	<b>Control-Specific</b> .....	<b>22</b>
G.1)	Does this new release address security controls related to government use of "public" platforms such as social media sites? .....	22





# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

G.2) Is there a plan to identify controls in an overlay that map SP 800-53, Revision 5 controls to the NIST SP 800-207, *Zero Trust Architecture*?..... 22

G.3) Is there any difference between the technical controls for achieving security and privacy?..... 22

**H. General** ..... 22

H.1) Will 800-53B include baselines tailored specifically for Cloud Systems/Services and the shared security responsibility model? ..... 22

H.2) Is the CSF one of the overlays that will be included in 800-53B? ..... 23

H.3) Do you foresee development of a specific NERC CIP overlay or just the more general SP 800-82 ICS overlay?..... 23

H.4) How should IoT cybersecurity issues be addressed in the new SP 800-53, Revision 5? ..... 23

H.5) Is SCOR intended to be similar to the Open Security Architecture Control Patterns?.. 23

H.6) One of the biggest risks we are seeing is inadequate cybersecurity workforce. Is that addressed in the new families or changes?..... 24

H.7) The draft SP 800-53, Revision 5 still doesn't explain the relationship between "control" and "system requirement." Are there plans to better explain this for both developer and management roles? ..... 24

H.8) What is the difference between a control enhancement and control? Are control enhancements required? If so, why are they enhancements and not controls? ..... 24

H.9) What are the NIST SP 800-53, Revision 5 next generation controls for systems and organizations?..... 24

H.10) How can I help with updating the ICS/SCADA and manufacturing profile? ..... 25

**I. Privacy** ..... 25

I.1) What is the relationship between SP 800-53, Revision 5 and the NIST Privacy Framework and Cybersecurity Framework? ..... 25

I.2) Will NIST provide a mapping of SP 800-53, Revision 4 Appendix J privacy controls to SP 800-53, Revision 5?..... 25

I.3) What is the relationship between SP 800-53, Revision 5 privacy controls and Office of Management and Budget (OMB) privacy-related requirements? ..... 26

I.4) Are SP 800-53, Revision 5 privacy controls aligned with non-federal legal requirements (e.g., derived from the European Union General Data Protection Regulation, California Consumer Privacy Act)? ..... 26

I.5) Should privacy control assessments be performed simultaneously with or separately from security control assessments? ..... 26

(Updated: 4/27/2020)

I.6)	How do privacy controls and security controls overlap and differ? .....	26
<b>J. Supply Chain</b> .....		<b>27</b>
J.1)	For implementation of Cyber SCRM on US federal/defense programs, has NIST worked with or drafted a model data item description (DID) for C-SCRM plans?.....	27
J.2)	Other than security and privacy groups, which other groups will play a role in implementing SR and other supply chain-related controls? .....	27
<b>K. Virtual Event-Specific</b> .....		<b>27</b>
K.1)	Will there be a certificate for CEU credit? .....	27
K.2)	Can you advise if there will be a recorded video that I can watch on my own time for the following? .....	27
K.3)	Will the video and audio of the presenters answer the live questions be available in the replay? / Is it possible to provide a searchable summary of the Q&A for review? .....	28

## A. Public Comment

A.1) What is the public comment review period for SP 800-53, Revision 5 (FPD)?

The public comment period is March 16 – May 29, 2020. [\[Return to Table of Contents\]](#)

---

A.2) How long is the public comment period on SP 800-53, Revision 5 (FPD)?

The public comment period on the final public draft is 74 days (60 days + 14-day extension). [\[Return to Table of Contents\]](#)

---

A.3) How can I submit comments?


Comments can be submitted via email using the comment template provided under “Supplemental Material” to [sec-cert@nist.gov](mailto:sec-cert@nist.gov). [\[Return to Table of Contents\]](#)

---

A.4) Can I submit comments after the public comment review period closes?

Submit comments via email using the comment template provided under “Supplemental Material” to [sec-cert@nist.gov](mailto:sec-cert@nist.gov). Please note that comments submitted after the public comment period may be held until the next update of the publication. [\[Return to Table of Contents\]](#)

---



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

- A.5) Will my comments be addressed in the final version of the document?  
NIST reviews each comment and recommendation submitted; the final decision about what to include in a publication resides with NIST. [[Return to Table of Contents](#)]
- 

- A.6) Will there be a third public comment period?  
There will not be a third comment period for SP 800-53. In most cases, NIST traditionally has one or two public comment periods for its publications. [[Return to Table of Contents](#)]
- 

- A.7) Is there a possibility of a deadline extension on the final public draft of SP 800-53, Revision 5?  
The public comment deadline has been extended to May 29, 2020. [[Return to Table of Contents](#)]
- 

- A.8) What kind of feedback is NIST seeking?  
NIST accepts feedback on any aspect of the publication. Stakeholder feedback provides NIST with additional inputs, views, expertise, and improves the technical content and usability. For the draft NIST SP 800-53, Revision 5 refer to the publication page: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft> for instructions on how to submit comments. [[Return to Table of Contents](#)]
- 

## B. Changes/Dependencies

- B.1) What changed in this final public draft (FPD) version from the initial public draft (IPD)?  
There are multiple differences between the IPD and the FPD of SP 800-53 Revision 5. NIST has developed a *Summary of Significant Changes* between **SP 800-53 Revision 4 and the FPD** provided under “Supplemental Material” on the [publication page](#). [[Return to Table of Contents](#)]
- 

- B.2) Will the Privacy Framework be updated with the release of SP 800-53, Revision 5?  
NIST SP 800-53 Revision 5 Initial Public Draft (IPD) was used as informative reference for the mapping of the NIST Privacy Framework sub-categories to SP 800-53 controls. The mapping is being updated for this final public draft. [[Return to Table of Contents](#)]



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

---

## B.3) Will the next revision to SP 800-161 utilize SP 800-53, Revision 5 controls?

Yes, while the research into updating [SP 800-161](#) has only recently started, the current plan is to use SP 800-53, Revision 5 controls. [[Return to Table of Contents](#)]

---

## B.4) What is the relationship between SP 800-53, Revision 5 and the NIST Privacy Framework and Cybersecurity Framework (CSF)?

The NIST Privacy Framework and Cybersecurity Framework are complementary tools for managing privacy and cybersecurity risk at the enterprise level, whereas SP 800-53 is a catalog of controls to help meet specific privacy and security requirements as well as mitigate identified risks. SP 800-53 is used as an informative reference for the Cybersecurity Framework and the Privacy Framework to support the achievement of Framework Subcategories. The mappings between SP 800-53 and the Cybersecurity Framework and the Privacy Framework will be updated. For the current mapping of SP 800-53, Revision 5 Initial Public Draft (IPD) to the Privacy Framework, visit the Privacy Framework Resource Repository (<https://www.nist.gov/privacy-framework/resource-repository>). [[Return to Table of Contents](#)]

---

## B.5) Will NIST CSF be updated to align with SP 800-53, Revision 5? / With the new control tables, what is the impact to the NIST CSF?

The NIST Cybersecurity Framework (CSF) is a living document, and is intended to be updated based on industry feedback and recommendations as well as NIST's continued goal to inform the community. To learn about the NIST CSF update process, please see: <https://www.nist.gov/cyberframework/online-learning/update-process>. [[Return to Table of Contents](#)]


---

## B.6) Can you identify and explain the changes with the baselines (in forthcoming SP 800-53B)?

Changes in forthcoming SP 800-53B will reflect the updates to the controls in SP 800-53, Revision 5, including a privacy control baseline, privacy control selection criteria, and updates to the security control baselines. [[Return to Table of Contents](#)]

---





# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

**B.7) Will the “more than HIGH” baseline continue?**

NIST SP 800-53 has historically only had three baselines: *Low*, *Moderate*, and *High*. Forthcoming draft SP 800-53B provides three security control baselines (for LOW, MODERATE and HIGH impact systems), and a privacy control baseline. [[Return to Table of Contents](#)]

---

**B.8) Why were baselines moved to a separate (SP 800-53B) document?**

The intent of separating the baselines from the main control catalog is, in addition to increasing efficiencies, to make the catalog more usable by different communities of interest. [[Return to Table of Contents](#)]

---

**B.9) Will supporting NIST publications be updated to align with SP 800-53, Revision 5? (Specific Virtual Event inquiries included: SP 800-171, SP 800-171A, SP 800-137, SP 800-66, SP 800-34, SP 800-128, SP 800-66, Assessment Case Project, etc.)**

All NIST publications are regularly evaluated to determine the need for update. As NIST publications are updated, including SP 800-53, Revision 5, NIST evaluates which additional publications will be updated on a case-by-case basis, and will update publications as “new revisions” (for significant changes) or “errata updates” (for minor changes). [[Return to Table of Contents](#)]

---

**B.10) When will NIST SP 800-18 be updated to include Privacy Plans?**

At this time, NIST is determining the best path forward how to provide guidance on privacy plans. [[Return to Table of Contents](#)]

---

**B.11) Does draft SP 800-53, Revision 5 align with FIPS 140-3?**

Yes, draft SP 800-53, Revision 5 references FIPS 140-3. [[Return to Table of Contents](#)]

---

**B.12) Will password length and maximum age guidance be aligned with updates to NIST SP 800-63-3 (i.e., passwords should not expire and length of password provides strength)?**

SP 800-53, Revision 5 (FPD) controls are aligned and consistent with SP 800-63-3. [[Return to Table of Contents](#)]

(Updated: 4/27/2020)

---

B.13) Is there any input within draft SP 800-53, Revision 5 denoting the importance of how each control impacts different OSI layers at a technical/operational level?

No, there is not. Impact to OSI layers is implementation-specific, and out-of-scope for NIST. [[Return to Table of Contents](#)]

---

B.14) Will there be a realignment of the OSCAL layers to reflect changes in draft SP 800-53, Revision 5? Where can we find more information on OSCAL?

When SP 800-53, Revision 5 is updated, corresponding OSCAL files will be updated as well to reflect the final version of the catalog. Likewise, when SP 800-53B is released, NIST will provide a corresponding OSCAL profile for each baseline. For more information: <https://github.com/usnistgov/OSCAL/tree/master/content/nist.gov/SP800-53>

For more information on the Open Security Controls Assessment Language (OSCAL), visit: <https://nist.gov/oscal>

[[Return to Table of Contents](#)]

---

B.15) Will the controls in SP 800-53, Revision 5 be mapped to and be implemented with other standards, guidelines, requirements, tools, solutions (e.g., CDM, FedRAMP, DISA STIGs, GPOs, CSAM, MITRE ATT&CK, MARS-E, CNSSI-1253)?


NIST generally does not develop mappings to external standards, guidelines, requirements, tools and solutions; and does not have a role in determining how and when external organizations update their resources, publications, guidance, tools/products, and services. Please contact the respective organizations to determine their plans and timeframes for developing mappings and updating tools/solutions.

[[Return to Table of Contents](#)]

---

B.16) Will SP 800-53, Revision 5 replace the DISA STIGs?

No, SP 800-53, Revision 5 is not a replacement for DISA STIGs. SP 800-53 is a catalog of security and privacy controls that provides protective measures for systems, organizations, and individuals. STIGs are implementation guides. [[Return to Table of Contents](#)]



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

## B.17) How does SP 800-53, Revision 5 impact the CMMC and the DFARS?

The DOD Cybersecurity Maturity Model Certification (CMMC) utilizes the publicly available security controls in draft NIST SP 800-53, Revision 5. NIST is not involved in the design, development, or implementation of the CMMC model, accreditation body, or certification. For information about the CMMC program, please see:

<https://www.acq.osd.mil/cmmc/> Specific questions about the CMMC should be directed to the CMMC Program.

NIST does not have a role in implementation, assessment, or oversight of the Defense Federal Acquisition Regulation Specification (DFARS) Clause 252.204-7012. The following resources are available from the Department of Defense (DoD):

- Procurement Technical Assistance Program (PTAP) and Procurement Technical Assistance Centers (PTACs)
- Nationwide network of centers/counselors experienced in government contracting, many of which are affiliated with Small Business Development Centers and other small business programs
- Cybersecurity in DoD Acquisition Regulations page at for Related Regulations, Policy, Frequently Asked Questions, and Resources (June 26, 2017)
- DPAP Website for DFARS, Procedures, Guidance and Information (PGI), and Frequently Asked Questions
- DoDI 5230.24, Distribution Statements on Technical Documents
- DoD's Defense Industrial Base Cybersecurity program (DIB CS Program)

Questions about the DFARS can be submitted to: [osd.dibcsia@mail.mil](mailto:osd.dibcsia@mail.mil)

[\[Return to Table of Contents\]](#)

---

## B.18) Does NIST coordinate with other entities when developing publications such as SP 800-53, Revision 5? / Are new/updated controls tested against sample industries?

NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted cybersecurity standards and guidelines. Using a variety of approaches and processes (e.g., interactions with stakeholders at public forums, working with federal agencies, industry and academia), NIST works with stakeholders to identify areas where standards or guidelines are needed, evaluates proposals, and develops/updates publications. NIST also engages stakeholder organizations through its public common process, and evaluates all feedback received (at any time) as publications are updated. [\[Return to Table of Contents\]](#)



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

B.19) NIST SP 800-53, Revision 5 links to many other documents. Has NIST considered having living documents capable of supporting dynamic updates? / Will NIST reevaluate FISMA guidance development processes with an eye to a faster release schedule to better address changes in the threat landscape? / How does NIST expect the idea of putting the publication online, and doing incremental updates to work?

NIST is always evaluating new ways and methods to engage with stakeholders to develop and share timely publications, tools, and other resources. [\[Return to Table of Contents\]](#)

---

B.20) Will the update to FIPS be a revision to FIPS 200 or a new FIPS document altogether (e.g., “FIPS 201”)?

At this time, the planned update to FIPS 200 will not result in a new publication number. [\[Return to Table of Contents\]](#)

---

B.21) Does NIST plan to do mappings of the SP 800-53 controls to other standards, guidance and other resources?

NIST will release the following mappings as Supplemental Materials pending the final publication of SP 800-53, Revision 5:

- Mappings to ISO 27001 and ISO 15408
- Mappings to the NIST Cybersecurity Framework and Privacy Framework

Additional mappings are not planned at this time; NIST encourages the relevant communities of interest to develop applicable mappings and resources.

[\[Return to Table of Contents\]](#)

---

B.22) What is the new guidance for SDLC?

Draft SP 800-53, Revision 5 incorporates new, state-of-the-practice controls based on system engineering best practices which apply across the SDLC. [\[Return to Table of Contents\]](#)

---



(Updated: 4/27/2020)

## B.23) Why were “information system” and “organization” removed from the control text?

As noted in the “*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*” [<https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft-fpd-summary-of-significant-changes.pdf>], the structure of the controls was slightly modified to allow the control statements to focus on the control outcomes rather than on who is responsible for implementing them. Typical implementation of the controls is noted in Appendix D, *Control Summaries*, by the letter “S” (for controls typically implemented by the information system) and by the letter “O” (for controls typically implemented by the organization) in the *implemented by* column. [[Return to Table of Contents](#)]

---

## C. Publishing

### C.1) When will the final version of SP 800-53, Revision 5 be released?

We do not have a specific release date for the publication at this time. [[Return to Table of Contents](#)]

---

### C.2) When will related publications (e.g., SP 800-53A, SP 800-53B) be released after SP 800-53, Revision 5 is finalized?

There is no release date for these related publications at this time. Historically, some of the associated documents (e.g., SP 800-53A) were released few months after the primary publication was released due to the dependency on the content of SP 800-53. [[Return to Table of Contents](#)]

---

### C.3) What is the publication plan for SP 800-172 (formerly SP 800-171B)?

The development of the Final Public Draft of NIST SP 800-172 is underway. The public comments from the Initial Public Draft are being adjudicated by the authors. We do not have a specific release date for the publication at this time. [[Return to Table of Contents](#)]

---

### C.4) What is NIST SP 800-53A?

[NIST SP 800-53A](#), ***Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans***, provides a set of

(Updated: 4/27/2020)

procedures for conducting assessments of controls employed within federal information systems and organizations. The assessment procedures in the SP 800-53A, Revision 4, are consistent with the security and privacy controls in **NIST Special Publication 800-53, Revision 4**. [[Return to Table of Contents](#)]

---

## C.5) What is NIST SP 800-53B?

NIST Special Publication 800-53B, **Control Baselines for Information Systems and Organizations** (forthcoming), will contain control baselines for federal information systems and organizations. It provides guidance for tailoring control baselines and for developing overlays to support security and privacy requirements of stakeholders and their organizations. [[Return to Table of Contents](#)]

---

## D. Resources

### D.1) What other formats are the controls available in? / Will the controls in SP 800-53, Revision 5 be available in other formats? / Would it be possible to provide control tables in SQL format?

NIST currently offers the draft controls in XML, JSON, YAML and XLS. Please see “Supplemental Materials” on the [publication page](#). [[Return to Table of Contents](#)]


---

### D.2) Is NIST planning on summarizing significant changes from the 2017 initial draft of Revision 5 to the current draft? / Is there a mapping between the controls in Revision 4 to Revision 5?

We do not have a red-lined document comparing the Initial Public Draft (IPD) released in August 2017 and the Final Public Draft (FPD) released in March 2020, and there is no mapping between the controls in Revision 4 and Revision 5 (FPD)

There are multiple differences between the IPD and the FPD of NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf>), including but not limited to:

- Addition of Supply Chain Risk Management Family (most of the controls in this family are derived from SA-12, *Supply Chain Protection*, in NIST SP 800-53 Revision 4)
- Consolidation of two privacy families and controls (August 2017: 2 privacy-focused families, Individual Participation and Privacy Authorization) into a single



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

family (March 2020: 1 privacy-focused family, Personally Identifiable Information Processing and Transparency)

- Updates of references and terminology to reflect current NIST publications and federal regulatory guidelines
- Relocation of multiple appendices (e.g., control baselines, tailoring considerations) into future NIST SP 800-53B, *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations*.

Also on the NIST SP 800-53, Revision 5 publication page

(<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft> ) underneath

“Supplemental Material,” you will find a document detailing significant changes between NIST SP 800-53 Revision 4 and NIST SP 800-53, Revision 5 FPD.

[\[Return to Table of Contents\]](#)

---

### D.3) Will NIST offer more reviews and dives into controls? / Will NIST develop training on control implementation?

NIST does not develop training on control implementation as implementation is organization-specific. [\[Return to Table of Contents\]](#)

---

### D.4) Does NIST have any plans to develop templates for control family policies and procedures?

NIST does not generally develop templates; however, some of the publications referenced for specific controls include example templates. [\[Return to Table of Contents\]](#)


---

### D.5) Does NIST offer training where one could obtain a CEU? / Can a CEU be obtained by attending the virtual event on the draft SP 800-53, Revision 5?

Attendees are encouraged to self-report training credits to their certifying authority.

The International Association of Privacy Professionals (IAPP) has approved up to 2 CPE credits for attending this virtual event. Refer to original event page for additional information <https://go.usa.gov/xd7Vg>.

[\[Return to Table of Contents\]](#)



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

D.6) Will links to online resources be included in the SP 800-53, Revision 5?  
Online resources can be found on the NIST Risk Management Framework (RMF) site at: <https://nist.gov/rmf>. [\[Return to Table of Contents\]](#)

---

D.7) Will NIST update the available overlays in the Knowledgebase?  
Overlays will be updated as they are received and evaluated. Refer to the NIST Security Control Overlay Repository (SCOR): <https://csrc.nist.gov/Projects/risk-management/scor>. [\[Return to Table of Contents\]](#)

---

D.8) Will there be more questionnaire / assessment supplementals to NIST publications?

NIST has developed a suite of publications that support implementation of the Risk Management Framework (RMF) as described in NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*.

[\[https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final\]](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final) [\[Return to Table of Contents\]](#)

---

D.9) If the government shuts down, will NIST resources (including publications and supplemental materials) be still available to the public?

Should the government shut down, impact to NIST and NIST services -- including those associated with the dissemination of security and privacy guidance -- will be evaluated, and a decision will be made at that time regarding what services remain operational.

[\[Return to Table of Contents\]](#)

---

D.10) Is it possible for NIST to release CSV versions of SP 800-53, SP 800-53A and SP 800-53B (all Revision 5) to facilitate the integration of the new requirements into existing toolsets?

A link to a spreadsheet containing draft SP 800-53, Revision 5 controls can be found on the publication's page at: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft>

CSV versions of the current SP 800-53 and SP 800-53A Revision 4 can be found on the SP 800-53 database at: <https://nvd.nist.gov/800-53>

Please note that efforts are underway to integrate OSCAL into the development of 800-53 data sets.

[\[Return to Table of Contents\]](#)



(Updated: 4/27/2020)

---

## D.11) Will there be desktop tools to work with OSCAL-based data? / Can NIST provide a demonstration of OSCAL and how it can be utilized?

The NIST Open Security Controls Assessment Language (OSCAL) team can be reached at: <https://pages.nist.gov/OSCAL/contribute/contact/>

For more information on the OSCAL project at nist, visit: <https://nist.gov/oscal>

[\[Return to Table of Contents\]](#)

---

## D.12) Will NIST provide assistance with control auditing guidance?

After SP 800-53, Revision 5 is finalized, NIST will be releasing an update to the SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, to provide guidance on conducting control assessments. [\[Return to Table of Contents\]](#)

---

## E. Implementation/Adoption

### E.1) Can organizations adopt SP 800-53, Revision 5 FPD before a final version is released?


Organizations may elect to use the content of any NIST publication; however, SP 800-53, Revision 5 is in draft, and the controls are subject to change. [\[Return to Table of Contents\]](#)

---

### E.2) Could NIST provide a guide identifying the most important controls that should be implemented based on the type of system? / Any thoughts about recommending a Critical Control List which is a subset of controls if agencies adopt this model, and CISO is more risk tolerant?

The selection and implementation of controls is a risk-based process for the implementing organization that takes into account many factors (i.e., the organizational risk management strategy, risk tolerance, mission/business functions, types of information and systems, threats and vulnerabilities to the system and organization).

We encourage communities of interest to consider developing overlays for specific information technology areas or for unique circumstances/environments. Overlays



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

provide an opportunity to build consensus across communities of interest and develop security plans for organizational systems that have broad-based support for very specific circumstances, situations, and/or conditions. To support development and sharing of overlays, NIST provides the NIST Security Control Overlay Repository (SCOR) <https://csrc.nist.gov/Projects/risk-management/scor>, a platform for stakeholders to voluntarily share security control overlays. [\[Return to Table of Contents\]](#)

---

### E.3) Can this publication work by itself if an organization has not implemented the Risk Management Framework (RMF)?

NIST encourages organizations to utilize a risk-based framework (e.g., Risk Management Framework); however, NIST also recognize that organizations may have different approaches to selecting/implementing controls. [\[Return to Table of Contents\]](#)

---

### E.4) Where is the implementation guidance for “O” versus “S” for organization level and system level implementation of a specific control?

Refer to draft NIST SP 800-53, Revision 5, Appendix D Control Summaries. [\[Return to Table of Contents\]](#)

---


### E.5) Does SP 800-53, Revision 5 distinguish between documentation requirements for the enterprise versus for every system/FISMA boundary?

The selection and implementation of controls is risk-based and organization-specific. If the organization and system are utilizing the risk management methodology in NIST SP 800-37, Revision 2, common controls are identified in the Organization-Level Prepare Step (Task P-5). To assist organizations, NIST provides a listing of the controls and control enhancements, and notes if they are typically implemented by a system through technical means or by the organization (i.e., by an individual through non-technical means). Refer to draft SP 800-53, Revision 5, Appendix D. [\[Return to Table of Contents\]](#)

---

### E.6) Does SP 800-53, Revision 5 provide the frequency of review or recommended review frequency controls or will that still be the responsibility of the organization to determine?

The determination of control review frequency (i.e., control monitoring) is part of the organization’s information security continuous monitoring strategy, and is a risk-based decision for each organization. For guidance on Information Security Continuous



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

Monitoring for Federal Information Systems and Organizations, refer to NIST SP 800-137 and SP 800-37. [\[Return to Table of Contents\]](#)

---

E.7) **Is data tagging only for HIGH impact systems or mandated for all systems?**  
Controls selected for LOW, MODERATE and HIGH impact systems will be published in SP 800-53B, *Control Baselines for Information Systems and Organizations*. [\[Return to Table of Contents\]](#)

---

E.8) **Can NIST clearly denote how the control implementation and tailoring process are tied to ERM to function properly?**

Control selection and tailoring are addressed by SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [<https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>]; and by the forthcoming SP 800-53B, *Control Baselines for Information Systems and Organizations*. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [<https://csrc.nist.gov/publications/detail/sp/800-39/final>] provides guidance on enterprise-wide information security risk management. [\[Return to Table of Contents\]](#)

---

E.9) **Could NIST please elaborate more on implementing control enhancements? / How about companion document with "examples" of implementation statements for control?**

Implementation of controls and control enhancements will vary; NIST does not dictate how controls are implemented. [\[Return to Table of Contents\]](#)

---

E.10) **Will there be guidance for developing automated tools to implement and/or review control implementations?**

NIST Interagency Report (NISTIR) 8011, *Automation Support for Security Control Assessments*, provides guidance to support automated assessment of most of the security controls in NIST SP 800-53, which may assist in the development of automation tools to implement and/or review control implementations. For more information: NISTIR 8011 Volume 1: Overview [<https://csrc.nist.gov/publications/detail/nistir/8011/vol-1/final>]; Volume 2: Hardware Asset Management [<https://csrc.nist.gov/publications/detail/nistir/8011/vol-2/final>]; Volume 3: Software Asset Management [<https://csrc.nist.gov/publications/detail/nistir/8011/vol-3/final>]; and Volume

(Updated: 4/27/2020)

4: Software Vulnerability Management (releasing in April 2020). [\[Return to Table of Contents\]](#)

---

E.11) How soon after SP 800-53, Revision 5 is released will organizations need to implement the new controls? / Once SP 800-53, Revision 5 is released, how much time will organizations have to make the switch from Revision 4 to Revision 5? / Will the timeframe for implementation be set to one (1) year from final OMB approval? / Alignment with NIST updates are typically required one year after release. Would the clock start after the release of SP 800-53A? / It seems like the control requirements will be dynamic. Will there be a grace period for new requirements?

NIST does not determine the timeline for federal agency implementation of NIST publications. Please refer to OMB Circular A-130, regarding implementation timeframes. [\[Return to Table of Contents\]](#)

---

## **F. Notes to Reviewers Supplement: Notional Example: NIST SP 800-53 Controls Security and Privacy Collaboration Index**

F.1) NIST: Thank you to all those who have submitted feedback on the Collaboration Index.

Collaboration Index feedback is being captured in the comments on the draft NIST SP 800-53, Revision 5. [\[Return to Table of Contents\]](#)

---

F.2) What is the Security and Privacy Collaboration Index?

The Security and Privacy Collaboration Index is included in the Notes to Reviewers Supplement. The Collaboration Index is a notional example and is a starting point to facilitate discussion between security and privacy programs within organizations since the degree of collaboration needed for control implementation for specific systems depends on many factors. The index is intended to indicate the degree of collaboration between security and privacy programs for each control. [\[Return to Table of Contents\]](#)

---



(Updated: 4/27/2020)

### F.3) What is the driver for the Collaboration Index?

The integration of security and privacy controls into one catalog recognizes the essential relationship between security and privacy objectives. Control implementation can often underscore this relationship. For example, security and privacy objectives are aligned in many circumstances, and therefore, the implementation of a particular control can support achievement of both sets of objectives. However, there are also circumstances when controls are implemented differently to achieve the respective objectives, or the method of implementation can impact the objectives of the other program. Thus, it is important that security and privacy programs collaborate effectively with respect to the implementation of controls to ensure that both programs' objectives are met appropriately and assigned responsibilities are carried out. [\[Return to Table of Contents\]](#)

---

### F.4) Why are there only three control families included in the Collaboration Index?

For purposes of review and comment, three control families are identified as **notional examples** – Access Control (AC), Program Management (PM), and Personally Identifiable Information Processing and Transparency (PT). [\[Return to Table of Contents\]](#)

---

### F.5) What feedback is NIST requesting on the Collaboration Index?

NIST seeks the feedback on the following areas, as well as **any other input** on the Collaboration Index:

- Does an implementation collaboration index for each control provide meaningful guidance to both privacy and security professionals? If so, how? If not, what are potential issues and concerns?
  - Which option (3-gradiant scale or 5-gradient scale) is preferred and why?
  - Are there other recommendations for a collaboration index?
  - Are there recommendations on other ways to provide more guidance on collaboration?
  - Are there recommendations for how the collaboration index should be integrated with the controls? For example, should the collaboration index be included as an Appendix to SP 800-53, included as a section of the control, included in related publication, or some other method? [\[Return to Table of Contents\]](#)
-

(Updated: 4/27/2020)

F.6) Is the Collaboration Index applicable to all controls in draft SP 800-53, Revision 5, or only to the three families featured in the notional example (in “Notes to Reviewers Supplemental Material”)?

NIST is currently conceptualizing the Collaboration Index. Collaboration Index feedback is being captured in the comments on the draft NIST SP 800-53, Revision 5. [\[Return to Table of Contents\]](#)

---

## G. Control-Specific

G.1) Does this new release address security controls related to government use of "public" platforms such as social media sites?

Yes. There are multiple controls and control enhancements that address social media (e.g., AC-23, *Data Mining Protection*). [\[Return to Table of Contents\]](#)

---

G.2) Is there a plan to identify controls in an overlay that map SP 800-53, Revision 5 controls to the NIST SP 800-207, *Zero Trust Architecture*?

There are discussions to create an overlay, but no estimated timeline for completion. [\[Return to Table of Contents\]](#)

---

G.3) Is there any difference between the technical controls for achieving security and privacy?

The integration of security and privacy controls into one catalog recognizes the essential relationship between security and privacy objectives. [\[Return to Table of Contents\]](#)

---

## H. General

H.1) Will 800-53B include baselines tailored specifically for Cloud Systems/Services and the shared security responsibility model?

No. NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* (forthcoming), will contain control baselines for federal information systems and organizations. It provides guidance for tailoring control baselines and for developing overlays to support security and privacy requirements of stakeholders and their

(Updated: 4/27/2020)

organizations. We encourage communities of interest to consider developing overlays for specific information technology areas or for unique circumstances/environments. For more information about overlays, see: <https://csrc.nist.gov/Projects/risk-management/scor> [[Return to Table of Contents](#)]

---

## H.2) Is the CSF one of the overlays that will be included in 800-53B?

No. NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* (forthcoming), will contain control baselines for federal information systems and organizations. It provides guidance for tailoring control baselines and for developing overlays to support security and privacy requirements of stakeholders and their organizations. [[Return to Table of Contents](#)]

---

## H.3) Do you foresee development of a specific NERC CIP overlay or just the more general SP 800-82 ICS overlay?

Organizations are encouraged to develop an overlay and submit it to the NIST Security Control Overlay Repository (SCOR) <https://csrc.nist.gov/Projects/risk-management/scor>. [[Return to Table of Contents](#)]

---

## H.4) How should IoT cybersecurity issues be addressed in the new SP 800-53, Revision 5?


This publication is technology neutral and can be applied to multiple system and platforms. Controls identified in this publication can be applied to any technology, sector, system or platform. [[Return to Table of Contents](#)]

---

## H.5) Is SCOR intended to be similar to the Open Security Architecture Control Patterns?

The NIST Security Control Overlay Repository (SCOR) <https://csrc.nist.gov/Projects/risk-management/scor> provides stakeholders a platform for voluntarily sharing security control overlays. An overlay is a fully-specified set of controls, control enhancements, and a supplemental guidance derived from the application of tailoring guidance to control baselines. It has a different purpose and scope than the Open Security Architecture Control Patterns. [[Return to Table of Contents](#)]

---



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

H.6) One of the biggest risks we are seeing is inadequate cybersecurity workforce. Is that addressed in the new families or changes?

This is currently out of the scope for draft NIST SP 800-53, Revision 5. Refer to the NIST National Initiative for Cybersecurity Education (NICE) <https://www.nist.gov/itl/applied-cybersecurity/nice> for more information on cybersecurity workforce. [[Return to Table of Contents](#)]

---

H.7) The draft SP 800-53, Revision 5 still doesn't explain the relationship between "control" and "system requirement." Are there plans to better explain this for both developer and management roles?

Refer to NIST Special Publication 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>) Section 2.6, *Requirements and Controls*, for additional information. [[Return to Table of Contents](#)]

---

H.8) What is the difference between a control enhancement and control? Are control enhancements required? If so, why are they enhancements and not controls?

Refer to NIST SP 800-53, Revision 5 (FPD) Section 2.2 Structure and Organization for additional information. [[Return to Table of Contents](#)]

---

H.9) What are the NIST SP 800-53, Revision 5 next generation controls for systems and organizations?

NIST Special Publication 800-53 presents a proactive and systemic approach to developing comprehensive safeguarding measures for all types of computing platforms. Those safeguarding measures include the security and privacy controls to protect the critical and essential mission and business operations of organizations, the organization's high value assets, and the personal privacy of individuals. The objective is to manage mission, business, and system risks for organizations, making the systems we depend on more penetration-resistant to cyber-attacks; limiting the damage from those attacks when they occur; making the systems cyber-resilient and survivable; and protecting the security and privacy of information. [[Return to Table of Contents](#)]

---



(Updated: 4/27/2020)

- H.10) How can I help with updating the ICS/SCADA and manufacturing profile? NISTIR 8183, Revision 1 is currently out for public comment until May 4, 2020. Please see: <https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/draft> for the publication and how to submit comments. For specific questions, please contact: [CSF\\_Manufacturing\\_Profile\\_Implementation@nist.gov](mailto:CSF_Manufacturing_Profile_Implementation@nist.gov). [[Return to Table of Contents](#)]
- 

## I. Privacy

- I.1) What is the relationship between SP 800-53, Revision 5 and the NIST Privacy Framework and Cybersecurity Framework?

The NIST Privacy Framework and Cybersecurity Framework are complementary tools for managing privacy and cybersecurity risk at the enterprise level, whereas SP 800-53 is a catalog of controls to help meet specific privacy and security requirements as well as mitigate identified risks. SP 800-53 is used as an informative reference for the Cybersecurity Framework and the Privacy Framework to support the achievement of Framework Subcategories. The mappings will be updated. For the current mapping of SP 800-53, Revision 5 Initial Public Draft (IPD) to the Privacy Framework, visit the Privacy Framework Resource Repository at: <https://www.nist.gov/privacy-framework/resource-repository>. [[Return to Table of Contents](#)]

---

- I.2) Will NIST provide a mapping of SP 800-53, Revision 4 Appendix J privacy controls to SP 800-53, Revision 5?

NIST understands that many existing privacy programs have been built around Appendix J of SP 800-53, Revision 4. In Revision 5, the controls from Appendix J have been reorganized, reframed, and expanded upon. NIST plans to provide more materials to help organizations determine which controls in SP 800-53, Revision 5 align with Appendix J controls to make this change easier. At this time, NIST has provided a table which demonstrates a general distribution of Appendix J controls content across Revision 5 Final Public Draft control families (see slide 12 of the *“What’s New in Draft NIST Special Publication 800-53, Revision 5”* presentation: <https://www.nist.gov/document/sp80053-speaker-presentaton>). [[Return to Table of Contents](#)]

---

(Updated: 4/27/2020)

I.3) What is the relationship between SP 800-53, Revision 5 privacy controls and Office of Management and Budget (OMB) privacy-related requirements?

SP 800-53, Revision 5 privacy controls provide agencies with a catalog of controls that can be used to meet federal privacy requirements, including those articulated in OMB policy. As applicable, controls include references to policies such as OMB Circular A-130, among others. Agencies should not assume that implementation of SP 800-53, Revision 5 privacy controls will meet all OMB privacy-related requirements. Agencies may need to take additional measures. [\[Return to Table of Contents\]](#)

---

I.4) Are SP 800-53, Revision 5 privacy controls aligned with non-federal legal requirements (e.g., derived from the European Union General Data Protection Regulation, California Consumer Privacy Act)?

NIST Special Publications are primarily designed to provide guidance for federal agencies; nonetheless, many controls can be used to support compliance with non-federal requirements. Although NIST does not plan to develop mappings to non-federal law, regulation, or policy, NIST welcomes such contributions from the community to the Privacy Framework Resource Repository at <https://www.nist.gov/privacy-framework/resource-repository>. [\[Return to Table of Contents\]](#)

---

I.5) Should privacy control assessments be performed simultaneously with or separately from security control assessments?

There is no single way to sequence privacy and security control assessments. In determining the sequence, organizations may find it helpful to consider the objectives for which the controls were implemented. Where controls were implemented to achieve complementary privacy and security objectives or where tradeoffs were made between privacy and security objectives, a coordinated control assessment may support the best outcome. Where privacy and security objectives were independent from each other, the sequence of assessments may not matter. NIST strongly encourages privacy and security programs to collaborate on control selection, implementation, and assessments to determine what is most appropriate for a given system. [\[Return to Table of Contents\]](#)

---

I.6) How do privacy controls and security controls overlap and differ?

Security and privacy program objectives can overlap, for example, with respect to the security of personally identifiable information; therefore, controls selected to meet both security and privacy objectives can be considered both security and privacy controls. Still, privacy controls may be implemented for objectives unrelated to security and vice versa. For a Venn diagram representation of this relationship, see

(Updated: 4/27/2020)

<https://www.nist.gov/blogs/cybersecurity-insights/welcome-world-nist-privacy-framework-10>. [[Return to Table of Contents](#)]

---

## J. Supply Chain

J.1) For implementation of Cyber SCRM on US federal/defense programs, has NIST worked with or drafted a model data item description (DID) for C-SCRM plans?

No, NIST has not worked with or drafted a model DID; however, as we proceed with our research and development of draft SP 800-161, Revision 1, we will seek to determine the feasibility and demand for a model DID SCRM Plan. [[Return to Table of Contents](#)]

---

J.2) Other than security and privacy groups, which other groups will play a role in implementing SR and other supply chain-related controls?

A SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, and other relevant functions. [[Return to Table of Contents](#)]

---

## K. Virtual Event-Specific

K.1) Will there be a certificate for CEU credit?

Attendees are encouraged to self-report training credits to their certifying authority. The International Association of Privacy Professionals (IAPP) has approved up to 2 CPE credits for attending this virtual event. Refer to original event page for additional information <https://go.usa.gov/xd7Vq>. [[Return to Table of Contents](#)]

---

K.2) Can you advise if there will be a recorded video that I can watch on my own time for the following?

Yes, the recording is available at: <https://www.nist.gov/news-events/events/2020/04/virtual-event-whats-new-draft-nist-special-publication-800-53-revision-5> [[Return to Table of Contents](#)]

---



# DRAFT SP 800-53 REVISION 5 FREQUENTLY ASKED QUESTIONS

(Updated: 4/27/2020)

K.3) Will the video and audio of the presenters answer the live questions be available in the replay? / Is it possible to provide a searchable summary of the Q&A for review?

Yes, all questions that were asked and answered during the live presentation as well as questions that were answered after the event. Both sets of questions and answers are included in this updated FAQ. [\[Return to Table of Contents\]](#)

---