BD Pro Inc.
129 Stradwick Avenue
Ottawa, Ontario, K2J 2Y9
www.bdpro.ca

30 March 2016

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
sec-cert@nist.gov

NIST SP 800-53 Revision 5 - Pre-Draft Call for Comments

Reference: SP 800-53 Revision 5 - Pre-Draft Call for Comments 18 Feb 2016

We do appreciate being given the opportunity to provide Pre-Draft suggestions or comments for the next revision of NIST Special Publication 800-53 in the requested areas:

a. Security Control Baseline Normalization;
b. Security Control Format;
c. Addition of Hyperlinks;
d. Addition of Key Words;
e. Additional Information;
f. Clarification of Information; and
g. Removal of Information.

We have been using this catalog of security controls since 2005 when the first revision was published and we have found it to be a very useful reference when identifying required safeguards needed to mitigate security risks to government and private sector enterprises, systems and applications This NIST catalog of security controls has become a de facto international standard used well beyond the originally intended US government scope.

I should also add that the revisions have kept pace with the evolving threat environment much better than other standards, however, I am not so sure about the three *security control baselines*.

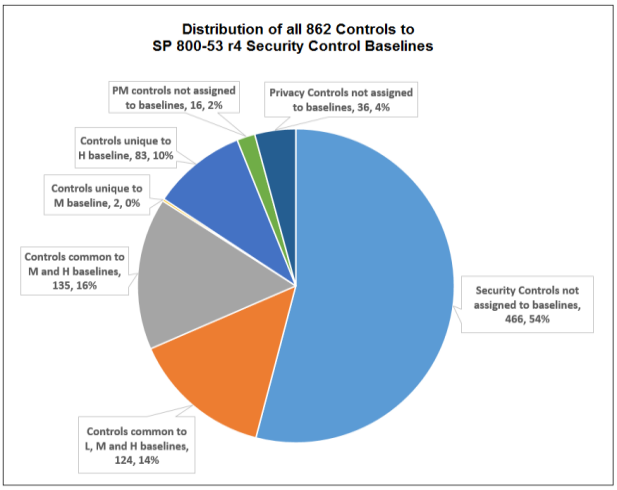
A. Security Control Baseline Normalization

The request for comments states that "… *the security control baselines provide a starting point for a tailoring process that results in an agreed upon set of security controls that are intended to provide protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems*". Feedback is sought *"regarding the relevance and appropriateness of the current security controls and control enhancements designated in each baseline -- that is, do the security controls and control enhancements in each baseline provide the appropriate starting point for tailoring that baseline?"*

A.1 Selection of Starting Point for Tailoring - Considerations

Tailoring is much more than developing an *"agreed upon set of security controls*" from the SP 800-53 catalog. It is not simply the adding and subtraction of controls from the *security control baseline* which was selected to be an *appropriate starting point*. In many cases, the starting point set of candidate security controls is very much dependent on what we used to refer to as the "*infosec boundary*" for the security risk mitigation exercise. The *infosec boundary* indicates where the **{c, i, a}** FIPS 199 categorized information assets are located. Given that many of the controls begin "*The organization …*" and that the variety and types of controls in each of the *security control baselines* (L, M and H), the implied *infosec boundaries* are very expansive for each of these three *security control baselines*.

The enterprise data systems addressed in these baselines are *assumed* to be general purpose, traditional physical facilities in networked multi-tier environments and do not address project management controls, privacy controls and security controls needed for data center virtualization, insider threats, classified information storage and transmission, advanced persistent threats (APTs), cross domain communications, mobile devices …



In general, each of the three baselines are at an enterprise level (i.e. a government agency), however the required tailoring is often needed at a lower architectural levels (i.e. business line organization, specific critical systems and information assets, operational systems and sub-systems, systems under development, physical or virtual networks, third party services, physical or virtual data centers, contracted service providers, etc …). In practice, for such lower architectural level (and *advanced persistent threat* related) risk management efforts, the starting point set of candidate security controls is often agreed to after consideration of relevant threat scenarios[1].

These candidate controls become the starting point which are then tailored to be more specific to these threat scenarios.

It is noted that the companion SP 800-53A Revision 4 security assessment guide also requires tailoring of assessment procedures and states "*In a similar manner to how the security controls and privacy controls from Special Publication 800-53 are tailored for the organization's mission, business functions, characteristics of the information system, and operating environment, organizations tailor the assessment procedures …*". However, SP 800-53 security controls catalog lacks such guidance at these lower architectural levels for relevant threat scenarios.

A.1 Recommend that Revision 5 include, for risk management at lower architectural levels (and *advanced persistent threats*), more specific guidance on how to the use and tailor the *security control baselines* for relevant threat scenarios.

A.2 Security Control Baselines & Continuous Improvement Programs – Some History and Considerations

In 2002, the NSA sponsored *Information Assurance Technical Framework (IATF) Forum* developed the concept of *"robustness levels".* In general*, security robustness* of required security controls was defined as being the *strength of mechanism* and *level of assurance* of security controls as a function of the value of the asset being protected and the threat. Five *Information Values* (V1 … V5) and seven *Threat Levels* (T1 .. T7) were defined. The IATFF methodology for determining *robustness levels* of required security controls for a specific solution was quite complex and could result in up to 35 different robustness levels. DoD simplified the methodology resulting in *3 robustness levels* for security services and mechanisms (i.e. security controls): **Basic** robustness, **Medium** robustness; and **High** robustness.

In 2005, SP 800-53 (Revision 1) included the **Low**, **Moderate** and **High** *Security Control Baselines*. "*To assist organizations in making the appropriate selection of security controls for their information systems, the concept of baseline controls is introduced. Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization* (i.e. value of assets being protected) *in accordance with FIPS 199."* The concept of "*Security Control Assurance*" was introduced and high level "*Minimum Assurance Requirements*" for the Low, Moderate and High baselines were summarized in a short Appendix.

In 2009 when SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) was withdrawn, NIST stated *"SP 800-26 is superseded by NIST SP 800-53 (revision 3) and the NIST SP 800 53A (Revision 1). Agencies are required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publication 800-53A for the assessment of security control effectiveness."*

To some observers, it was concluded that NIST:

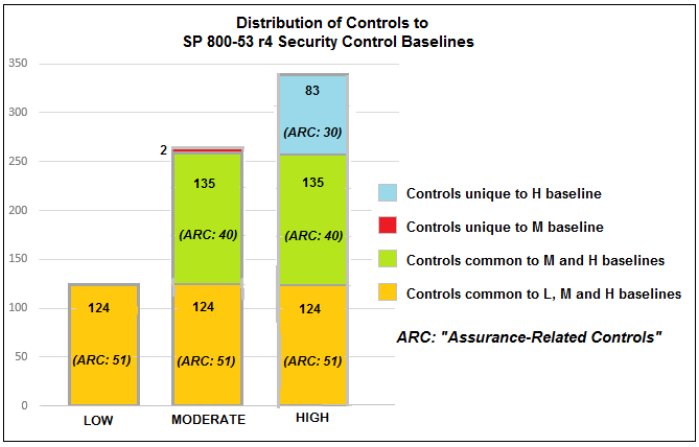
- Abandoned the complex SP 800-26 *capability maturity model* approach with "*five levels of effectiveness*" for defining organizational security requirements and assessing an organizations' security control effectiveness; and
- Abandoned the overly complex IATFF *robustness levels* for grouping of security controls. SP 800-53 (Revision 1) introduced the three *security control baselines* based only on the FIPS 199 defined value of the assets being protected and does not consider threat levels. These simplified baselines would be used to for defining

[1] A postulated set of circumstances in which a specific threat agent can mount a specific type of attack in an attempt to compromise (in one or more ways) one or more information and/or system assets.

organizational security requirements and assessing an organization's security control effectiveness.

In 2013, SP 800-53 (Revision 4) listed 121 *assurance-related controls* (ARC) for increasing the *levels of assurance* in the **Low** (51 controls), **Moderate** (91 controls), and **High** (121 controls) *security control baselines* and stated that the "*two fundamental components affecting the trustworthiness of information systems are security functionality and security assurance*." This definition of system *trustworthiness* is similar the earlier IATFF definition of system *robustness* which was based on *strength of mechanism* and *level of assurance*, however there is little consideration of *threat levels* for determining needed *trustworthiness*. There does appear to be some correlation of the original IATFF Basic, Medium and High *robustness levels* (i.e. *level of assurance* and *strength of mechanism* based) to a combination of the:

- SP 800-53A assessment criteria with specific focus on the 121 *assurance-related controls*, and
- SP 800-53 **Low**, **Moderate** and **High** *Security Control Baselines* which are based on *information value* related *impact levels*. Below is a summary of the distribution of security controls to the SP 800-53 Revision 4 *security control baselines*. The overall *strength of mechanisms* and the number of *"Assurance-related Controls"* increases from one baseline to the next.



Conclusions – Just as the IATFF *robustness levels* and the SP 800-26 *capability maturity model* based "*levels of effectiveness"* were likely deemed to be overly complex to effectively implement in organizations' *continuous security improvement* programs, the current assessment system is also becoming overly complex to implement effectively.

A.2.1 Recommend that the security controls in SP 800-53 Revision 5 be much more tightly coupled with assessment criteria in SP 800-53A Revision 5 in order that levels of compliancy with *security control baselines* can be more easily leveraged in enterprise continuous security improvement programs.

Implementation options to consider are:

- Introducing hyperlinks between controls in SP 800-53 and the related assessment criteria in SP 800-53A (and vice-a-versa);
- Providing more guidance in both SP 800-53 and SP 800-53A on how to use (in a standard manner) **Low**, **Moderate** and **High** *security control baselines, assurance-related controls* and related compliancy levels in an organization's continuous security improvement program; and
- Introduce guidance for adequate consideration of likely threat scenarios for determining needed *assurance-related controls* to mitigate risks.

A.2.2 Recommend that a Pre-Draft call for Comments be initiated by NIST for Revision 5 of SP 800-53A.

A.3 Tailoring of Security Control Baselines for Advanced Persistent Threats (APT)

The Introduction to SP 800-53 Revision 4 states that:

- this "*catalog of security controls can be effectively used to protect information and information from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios*."; and
- *"as missions/business functions become susceptible to advanced persistent threats by high-end adversaries, increased levels of assurances may be required."*

The Section 3.2 guidance for **Selecting Security Control Baselines**, states that:

- *"there are also some possible situations that are specifically not addressed in the baselines. These include: … Advanced persistent threats (APTs) … within organizations."*
- ***Situations Requiring Potential Baseline Supplementation*** include "*Advanced Persistent Threat".* However, "*security control baselines do not assume that the current threat is one where adversaries have achieved a significant foothold and presence within organizations and organizational information systems*". (The SP 800-53 baselines assume that organizations are not dealing with *Advanced Persistent Threats*).

- "*To more fully address the advanced persistent threat, concepts such as insider threat protection (CM-5 (4)), heterogeneity (SC-29), deception (SC-26 and SC-30), non-persistence (SC-25 and SC-34), and segmentation (SC-7 (13)) can be considered"* for supplementing or augmenting the *security control baselines*. (None of these seven controls are currently allocated to either of the three *security control baselines*.)

Within Appendix F (Security Control Catalog), none of the controls in the catalog, including the seven controls discussed in Section 3.2, are specifically designed or highlighted as being needed to help mitigate APT risks. However, the Supplemental Guidance of five controls (AC-6 (9), SA-12 (5), SC-30 (3), SI-14 and PM-16) does provide some high-level APT related guidance. AC-6 (9) is the only control which is included in *security control baselines* (**Moderate** and **High**).

Conclusions - The guidance provided for selecting controls for mitigating APT risks to organizations and organizational information systems is very limited and high-level in SP 800-53 Revision 4. In general, this is not a serious concern for experienced senior security practitioners who have the knowledge of APT threats, phases and typical targeted vulnerabilities, etc… and have related experience identifying candidate controls for mitigating the likely risks in the phases of APT attacks. However, for less experienced security practitioners, there is a need for much more focused and standardized guidance to be documented in SP 800-53 Revision 5. There a need that this guidance for selecting candidate security controls be granular enough so that controls can be selected to mitigate risks at each of the seven *phases* (aka *stages*, *kill chain*, *attack life cycle*, …) in various *advanced persistent threat* scenarios:

a. Intelligence gathering, reconnaissance and social engineering;
b. Initial intrusion (includes use of zero day vulnerabilities) of user or administration client-side endpoints;
c. Customized malware and utilities installation (includes capture of domain admin credentials);
d. Command and control communications;
e. Lateral movement and persistence in target environment (includes capture of user credentials and privilege escalation);
f. Critical assets and data discovery (includes maintaining persistence and covering tracks); and
g. Compromised data exfiltration.

A.3.1 Recommend that Supplemental Guidance for relevant controls specifically indicate that use of this control, in conjunction with other {*list: relevant ID codes*} controls, can help mitigate risks in the {*indicate relevant phase(s): Intelligence Gathering, Initial Intrusion, Malware Installation, Command and Control, Lateral Movement, Data Discovery or Data Exfiltration*} phase of *Advanced Persistent Threat* (APT) attacks.

A.3.2 Recommend that the definition of *Advanced Persistent Threat* in Appendix B (Glossary) be updated to include high-level details of the typical phases in such an attack. There is also a need for the Glossary to introduce standard definitions for key APT protection related terminology such as: *Attack Life Cycle*, *Command and Control Servers*, *Indicators of Compromise (IOC), Next Generation Firewalls (NGFW), Non-signature based defenses, Virtual Execution Sandboxes, Zero-day attacks …* etc. (Much of the APT protection related terminology is already being used in individual SP 800-53 r4 security controls. However, including agreed definitions within a NIST glossary would be helpful to organizations, security professionals, product vendors, … etc.)

A.3.3 Recommend that *Advanced Persistent Threat* related controls be specifically addressed in at least the **High** *security control baseline*.

B. Security Control Format

B.1 Recommend that the "*the organization …*" preamble used in security controls not be changed to a more outcome based format. The current wording has not been a problem and it does emphasize that the officers of the organization are responsible for outcomes. However, if problems have been experienced, recommend that appropriate contextual guidance be provided at the beginning of Appendix F (Security Control Catalog).

B.2 Recommend that the conventions for control identifiers be modified to allow sorting and easier use as unique indexes in tables, relational databases, and spreadsheets. Such unique identifiers will assist in generating specialized database reports such as cross tabulation *("crosstab*") of controls with relevant threat scenarios. In general, pad with zeros, where needed, to allow sorting.

Current	Recommended
AC-1	AC-01
AC-3 (9)	AC-03 (09)
AC-3 (10)	AC-03 (10)
AC-16 (1)	AC-16 (01)

B.3 Recommend that Appendix G Program Management Controls (PM-1 … etc) be incorporated into Appendix F (Security Control Catalog). These controls are SDLC and risk management related security controls and should be clearly included in the catalog.

In support of this recommendation, it is noted that:

- DoD FedRAMP privacy SP 800-53 based *overlays* clearly include PM controls;

- SP 800-82 for ICS / SCADA systems states: "*The PM-family is deployed organization-wide, supporting the information security program. It is not associated with security control baselines and is independent of any system impact level*"; and
- CNSSI-1253 for National Security Systems states that the PM controls are "*Common controls deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any impact levels*".

B.4 Recommend that Appendix J Privacy Control Catalog (AP, AR, DI, DM, … UL) be incorporated into Appendix F (Security Control Catalog). Notwithstanding the longstanding debates in this area, privacy controls are also important security controls in the context of social engineering and modern *advanced persistent threats* (APT).
See related recommendation G.5.

In support of this recommendation, it is noted that:

- DoD FedRAMP privacy SP 800-53 based overlays include these privacy controls;
- SP 800-82 for ICS / SCADA systems states: "*The privacy controls are intended primarily for use by an organizations Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, information system developers, and information security personnel to determine how best to incorporate effective privacy protections and practices within those programs and/or systems*"; and
- CNSSI-1253 for National Security Systems does not associate privacy controls with *security control baselines*. However, recommended parameter assignments are provided for AR-1, AR-4, AR-5, DI-1, DI-1 (2), DM-1, DM-2, IP-4 (1) and SE-1.

If incorporation into the main catalog is approved, the conventions for privacy control identifiers would need to be modified in a manner such as indicated below.

Current	Recommended	Privacy Controls
	PI-01	Privacy Controls Policies and Procedures
AP	PI-02	Authority and Purpose
AP-1	PI-02 (01)	Authority and Purpose / Authority to Collect
AP-2	PI-02 (02)	Authority and Purpose / Purpose Specification
AR	PI-03	Accountability, Audit, and Risk Management
AR-1	PI-03 (01)	Accountability, Audit, and Risk Management / Governance and Privacy Program
AR-2	PI-03 (02)	Accountability, Audit, and Risk Management / Privacy Impact and Risk Assessment
AR-3	PI-03 (03)	Accountability, Audit, and Risk Management / Privacy Requirements for Contractors & Service Providers
AR-4	PI-04 (04)	Accountability, Audit, and Risk Management / Privacy Monitoring and Auditing
AR-5	PI-04 (05)	Accountability, Audit, and Risk Management / Privacy Awareness and Training
AR-6	PI-04 (06)	Accountability, Audit, and Risk Management / Privacy Reporting
AR-7	PI-04 (07)	Accountability, Audit, and Risk Management / Privacy-Enhanced System Design and Development
AR-8	PI-04 (08)	Accountability, Audit, and Risk Management / Accounting of Disclosures
DI	PI-05	Data Quality and Integrity
DI-1	PI-05 (01)	Data Quality and Integrity / Data Quality
DI-2	PI-05 (02)	Data Quality and Integrity / Data Integrity and Data Integrity Board
DM	PI-06	Data Minimization and Retention
DM-1	PI-06 (01)	Data Minimization and Retention / Minimization of Personally Identifiable Information
DM-2	PI-06 (02)	Data Minimization and Retention / Data Retention and Disposal
DM-3	PI-06 (03)	Data Minimization and Retention / Minimization of PII Used in Testing, Training, and Research
IP	PI-07	Individual Participation and Redress
IP-1	PI-07 (01)	Individual Participation and Redress / Consent
IP-2	PI-07 (02)	Individual Participation and Redress / Individual Access
IP-3	PI-07 (03)	Individual Participation and Redress / Redress
IP-4	PI-07 (04)	Individual Participation and Redress / Complaint Management
SE	PI-08	Security
SE-1	PI-08 (01)	Security / Inventory of Personally Identifiable Information
SE-2	PI-08 (02)	Security / Privacy Incident Response
TR	PI-09	Transparency
TR-1	PI-09 (01)	Transparency / Privacy Notice
TR-2	PI-09 (02)	Transparency / System of Records Notices and Privacy Act Statements
TR-3	PI-09 (03)	Transparency / Dissemination of Privacy Program Information
UL	PI-10	Use Limitation
UL-1	PI-10 (01)	Use Limitation / Internal Use
UL-2	PI-10 (02)	Use Limitation / Information Sharing with Third Parties

B.5 Recommend that prioritization and allocation of controls to *security control baselines* be recorded for each security control in a tabular manner rather than in the one-row summary table at the end of control groupings in the Appendix F (Security Control Catalog).
See related recommendation G.2.

B.6 Recommend that *Assurance-Related Controls* be recorded for relevant security controls in a tabular manner in Appendix F (Security Control Catalog), rather than in the Low-Impact, Moderate-Impact and High-Impact tables in the Appendix E (Assurance and Trustworthiness).
See related recommendation G.4.

Below is an example of how priorities, baseline allocations and *assurance-related controls (ARC)* could be identified in the recommended tabular format in the Appendix F (Security Control Catalog).

CM-7 (4) Configuration Management / Least Functionality / Unauthorized Software / Blacklisting The organization: (a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency]. Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred	P1 M
CM-7 (5) Configuration Management / Least Functionality / Authorized Software / Whitelisting The organization: (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency]. Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.	P1 H

CM-8 Configuration Management / Information System Component Inventory

CM-8 Configuration Management / Information System Component Inventory The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency]. Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5. References: NIST Special Publication 800-128.	P1 L M H ARC
CM-8 (1) Configuration Management / Information System Component Inventory / Updates During Installations / Removals The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	P1 M H ARC

C. Addition of Hyperlinks

C.1 Recommend addition of external hyperlinks between controls in the SP 800-53 Revision 5 document and the related assessment criteria in the companion SP 800-53A Revision 5 document (and vice-a-versa).

C.2 Recommend that internal hyperlinks within the SP 800-53 Revision 5 document not be introduced.

If the number of existing appendices were reduced (See recommendations G.3, G.4 and G.5) and details consolidated (See recommendation B.3, B.4, B.5 and B.6) in Appendix F (Security Control Catalog), there would be significantly reduced need for any internal hyperlinks.

D. Addition of Key Words

D.1 Recommend that key words not be included for each security control. The existing search capability of PDF documents is adequate.

E. Additional Information

See recommendations above for **Security Control Baseline Normalization**.

F. Clarification of Information

See recommendations above for **Security Control Baseline Normalization**.

G. Removal of Information

G.1 Recommend that "*P0*" priority zero indicators be removed and not be associated with controls. It is stated that "*Priority Code 0 [P0] indicates the security control is not selected in any baseline*" which does not need to be stated because it is already readily apparent for such controls.

G.2 Recommend that the Priority and Baseline Allocation summary at end of security control groupings be removed, and that this information be recorded in a tabular manner in the Appendix F (Security Control Catalog) as indicated in above B.4 recommendation.

Priority and Baseline Allocation:

P1	LOW CM-7	MOD ~~CM-7 (1) (2) (4)~~	HIGH CM-7 (1) (2) (5)

G.3 Recommend that Appendix D (Security Control Baselines – Summary) be removed, and that details related to prioritization and assignment of controls to the three *security control baselines* be recorded in a tabular manner in the Appendix F (Security Control Catalog) as indicated in above B.5 recommendation.

Appendix D, Security Control Baselines - Summary, Table D-2

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11

G.4 Recommend that Appendix E (Assurance and Trustworthiness) be removed, and that the narrative guidance be incorporated into Section 2.6 (The Fundamentals / Assurance and Trustworthiness) and that "*Assurance-related controls*" for Low-Impact, Moderate-Impact and High-Impact systems in the Appendix E tables be recorded in a tabular manner in the Appendix F (Security Control Catalog).
See related B.6 recommendation.

TABLE E-3: ASSURANCE-RELATED CONTROLS FOR HIGH-IMPACT SYSTEMS[103]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2 (2), AT-3, AT-4	PE	PE-1, PE-6, PE-6 (1), **PE-6 (4)**, PE-8
AU	AU-1, AU-6, AU-6 (1), AU-6 (3), **AU-6 (5)**, **AU-6 (6)**, AU-7, AU-7 (1), **AU-10**	PL	PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8
CA	CA-1, CA-2, CA-2 (1), **CA-2 (2)**, CA-3, CA-5, CA-6, CA-7, CA-7 (1), **CA-8**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2 (1), **CM-2 (2)**, CM-2 (3), CM-2 (7), CM-3, **CM-3 (1)**, CM-3 (2), CM-4, **CM-4 (1)**, CM-8, CM-8 (1), **CM-8 (2)**, CM-8 (3), **CM-8 (4)**, CM-8 (5)	RA	RA-1, RA-3, RA-5, RA-5 (1), RA-5 (2), **RA-5 (4)**, RA-5 (5)
CP	CP-1, CP-3, **CP-3 (1)**, CP-4, CP-4 (1), **CP-4 (2)**	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	SC	SC-1, SC-2, **SC-3**, **SC-7 (18)**, **SC-7 (21)**, **SC-24**, SC-39
IR	IR-1, IR-2, **IR-2 (1)**, **IR-2 (2)**, IR-3, IR-3 (2), IR-5, **IR-5 (1)**	SI	SI-1, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-5, **SI-5 (1)**, **SI-6**, SI-7, SI-7 (1), **SI-7 (2)**, **SI-7 (5)**, SI-7 (7), **SI-7 (14)**, SI-10, SI-16
MA	MA-1		

G.5 Recommend that Appendix J (Privacy Control Catalog) be removed, and that narrative guidance be incorporated into a new section in Chapter Two (The Fundamentals) and that the privacy controls be incorporated into the Appendix F (Security Control Catalog).
See related B.4 recommendation.

G.6 Recommend that Appendix G (Information Security Programs) be removed, and that narrative guidance be incorporated into a new section in Chapter Two (The Fundamentals) and that the program management (PM) controls be incorporated into the Appendix F (Security Control Catalog).
See related B.3 recommendation.

Thank you for providing the opportunity to provide input for the improvement of a most useful NIST Special Publication.

Yours sincerely,

Bill Dziadyk, MSc, P.Eng.
President
BD Pro Inc.