NCSSR Changes in Detail

Last Updated: 03-Oct-2023
Based on commit: https://github.com/cabforum/netsec/commit/0d34f4ab148439130e28d4fa8128af7385fc21d3
Comparison between prod and
commit: https://github.com/cabforum/netsec/compare/c62a2f88e252de5c79b101fa3c9e9c536388639a...0d34f4ab148439130e28d4fa8128af7385fc21d3

Some remarks, questions, and requests regarding this document:
1. Would it be helpful to add heading titles to more sections? Right now, it's only 1st, 2nd, and 3rd level headings which have titles (but the 1st level is just "Requirements", so I don't really count that), and I'm inclined to think it would be helpful if at least 4th level headings had titles added.
2. For all the "ear" emoji sections, I'm explicitly requesting additional thoughts, feedback, and input.
3. For all "pencil" emoji sections, I'm explicitly requesting suggested edits or improved phrasing.
4. Both of the above are welcome for ALL sections and changes.

Introduction

Overview

Scope and Applicability:

These Network and Certificate System Security Requirements (Requirements) apply to all publicly trusted Certification Authorities (CAs) and are adopted with the intent that all such CAs and Delegated Third Parties be audited for conformity with these Requirements as soon as they have been incorporated as mandatory requirements (if not already mandatory requirements) in the root embedding program for any major Internet browsing client and that they be incorporated into the WebTrust Service Principles and Criteria for Certification Authorities, ETSI TS 101 456, ETSI TS 102 042 and ETSI EN 319 411-1 including revisions and implementations thereof, including any audit scheme that purports to determine conformity therewith.

> *This paragraph has been removed. Some form of it may return, but largely this addresses the process for first adopting the NCSSRs and is less relevant today, so should be modified to better represent their current, ongoing Scope and Applicability.*

In these Requirements, the CA is responsible for all tasks performed by Delegated Third Parties and Trusted Roles, and the CA SHALL define, document, and disclose to its auditors

a. the tasks assigned to Delegated Third Parties or Trusted Roles, and
b. the arrangements made with Delegated Third parties to ensure compliance with these Requirements, and
c. the relevant practices implemented by Delegated Third Parties.

> *This paragraph makes it clear that Delegated Third Parties are ultimately the responsibility of the CA; in order to improve readability and parseability of the NCSSRs, the requirements below typically mention only the CA, but there's **no** change to the applicability of requirements to Delegated Third Parties.*

> *Two sections have been added here: "Guiding Principle and Goal" and "Desired Outcomes".*
> *The Guiding Principle and Goal is a very short statement regarding the overarching intent of the NCSSRs, per the understanding of participants in the NSWG. There are likely improvements yet to be made to ensure this statement represents a comprehensive, consensus view of this topic.*
> *Desired Outcomes outlines some specific outcomes which the NetSec WG hopes the NCSSRs are able to achieve and*

> *which provide a framework for the changes being proposed for the NCSSRs. It's expected this would be updated semi-regularly and may also indicate when charter updates are warranted. The current language in this section is a solid first draft, but still rough in some areas and should be iterated on a bit further.*
> ✏️

Document History

Ver.	**Ballot**	**Description**	**Adopted**	**Effective***
1.0	83	Original Version Adopted	3-Aug-12	01-Jan-13
1.1	210	Misc. Changes to NCSSRs	31-Aug-17	09-Mar-18
1.2	SC3	Two-Factor Authentication and Password Improvements	16-Aug-18	15-Sep-18
1.3	SC21	The Network and Certificate Systems Security Requirements Section 3 (Log Integrity Controls)	26-Sep-19	4-Nov-2019
1.4	SC29	System Configuration Management	7-May-20	8-Jun-2020
1.5	SC28	Logging and Log Retention	10-Sep-2020	19-Sep-2020
1.6	SC39	Definition of Critical Vulnerability	16-Feb-2021	30-Mar-2021
1.7	SC41	Reformatting the BRs, EVGs, and NCSSRs	24-Feb-2021	5-Apr-2021

* Effective Date based on completion of 30-day IPR review without filing of any Exclusion Notices.

> *This section will be updated with the ballot and version number if this body of work progresses to ballot form.*

Definitions

> *A definition for "Air-Gapped" has been added, primarily as an outcome of discussions within the NSWG surrounding the eventual separation of requirements applicable to Root CA Systems. It is not currently in use in the draft, so may be removed in favor of a separate ballot focused solely on Root CA System requirements.*

> *A definition for "CA Infrastructure" has been added. There are 7+ types of "systems" defined in the NCSSRs, but their use is inconsistent and unclear in some cases. For example, Security Support System is defined as a system that does 8 different things, but the 8 things this system does are each described within the requirements themselves, making somewhat of a circular definition as well as creating an unnecessary defined term, since it's only used in the context of describing what it is. "CA Infrastructure" merely defines a term to encapsulate the collective set of systems elsewhere defined. The use of CA Infrastructure throughout this draft to replace a vast majority of the individual "systems" previously used is intended to:*
> *1. Simplify the assessment of the NCSSR's applicability. Most requirements apply to the CA's Infrastructure as a whole, with specific applicability to aspects of that infrastructure defined and described in-line; and*
> *2. Draw out any areas where requirements are applied in an overly broad way, so that improvements can be made to the requirement phrasing itself to clarify the intended scope of applicability*
>
> *It's plausible (and desirable, assuming agreement with the above) that we'll be able to remove some or most of the definitions of separate systems within the CA's infrastructure as their use becomes obviated by this consolidation of terminology.*
> 👂

Certificate Management System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

> *This definition has been updated into a slightly more readable and specific list, and removing "other PKI-related services".*

Common Vulnerability Scoring System (CVSS): A quantitative model used to measure the base level severity of a vulnerability (see <http://nvd.nist.gov/vuln-metrics/cvss>).

Critical Security Event: Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.

Critical Vulnerability: A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see <https://nvd.nist.gov/vuln-metrics/cvss>), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

Delegated Third Party: A natural person or legal entity that is not the CA and that operates any part of a Certificate System.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

Front End / Internal Support System: A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.

High Security Zone: A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.

> *High Security Zone has been removed both as a definition and from use within the NCSSRs.*

Issuing System: A system used to sign certificates or validity status information.

> *A definition for "Key Pair" has been added, to help provide more comprehensive coverage of the components in scope of the NCSSRs.*

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

> *This definition has been reformatted to include a numbered list, to remove the non-2119 use of "must", and clarifying the final sentence. It could still use some further enhancement, in my opinion.*
> ✏️

> *A definition for "Multi-Party Control" has been added since the term was used in the NCSSRs, but not defined.*

National Vulnerability Database (NVD): A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see <http://nvd.nist.gov/>).

> *A definition for "Network Equipment" was added to help clarify where requirements apply to the systems which make up the CA's infrastructure (CA Infrastructure) vs the other equipment used to enable connectivity and security of the CA's infrastructure (Network Equipment). The intent is that the entirety of the NCSSR's scope related to the CA's operations is encompassed by these 2 terms.*
> 👂

OWASP Top Ten: A list of application vulnerabilities published by the Open Web Application Security Project (see <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>).

Penetration Test: A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

> *A definition for “Physically Secure Environment” has been added, to replace the use of “Zones”. This alteration is primarily a result of other work within the NSWG. There is likely meaningful improvement remaining on this term, including ensuring it addresses the level of detail warranted for consistently secure CA environments, as well as addressing how this definition should interact with the possible future separation of “Root CA System”.*
>
> *For example:*
> ** In my opinion, this term and/or its use should address access control, perimeter security, video surveillance, security personnel, alarms and intrusion detection, secure storage, redundancy and resiliency, etc.*
> ** Much of this may belong in more dedicated sections of the NCSSRs rather than the definition, with a reference from the definition.*
>
> ** The 2nd bullet point of the current draft definition intimates a requirement that the CA be responsible for first conducting a Risk Assessment and second designing, building, and maintaining the Physically Secure Environment (which could be directly or more likely the CA "signing off" on those processes).*
> ** Is that the right expectation for _all_ CA Infrastructure?*
> ** I think it would be better to separate this into two environments: 1 for Root CA Systems and 1 for everything else.*
> ** It makes sense to me that criteria for Root CA Systems should be fairly prescriptive while criteria for everything else should be far less rigid and likely move away from specifying the CA's need to be involved _before_ the environment can be built (i.e. I see no reason a CA shouldn't be able to assess existing environments as meeting the criteria and their risk assessment).*
> 👂

> *A definition for “Principle of Least Privilege” has been added since the term was used in the NCSSRs, but not defined.*

> *A definition for “Private Key” has been added, to help provide more comprehensive coverage of the components in scope of the NCSSRs.*

> *A definition for “Public Key” has been added, to help provide more comprehensive coverage of the components in scope of the NCSSRs.*

> *A definition for “Requirements” has been added since the term was used in the NCSSRs, but not defined.*

> *A definition for “Risk Assessment” has been added since the term was used in the NCSSRs, but not defined.*

> *A definition of “Root CA Certificate” has been added, to help provide more comprehensive coverage of the components in scope of the NCSSRs and since the term was used in the NCSSRs, but not defined.*

> *A definition of “Root CA Private Key” has been added, to help provide more comprehensive coverage of the components in scope of the NCSSRs and since the term was used in the NCSSRs, but not defined.*

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

> *This definition was updated to use some of the newly added definitions and reformatted into a numbered list.*
> *The final item in the current draft list is potentially redundant.*
> 👂

SANS Top 25: A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see <http://www.sans.org/top25-software-errors/>).

Secure Key Storage Device: A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).

> *FIPS 140-3 was added to this definition.*
> *This definition may warrant further updates, given its use to address both Root CA Private Key storage as well as certificate-based MFA. If broken up a bit, perhaps it could also be updated to address secure enclave passkey storage or FIDO-compliant authentication.*
> 👂
> ✏️

Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Security Support System: A system used to provide security support functions, which MAY include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (Host-based intrusion detection, Network-based intrusion detection).

> *This definition has been reformatted to a numbered list.*
> *This is a definition that seems better suited as part of the core requirements, rather than a separately defined term. We should be able to obviate the need for it because of the presence of dedicated sections outlining these requirements, for example:*
> *authentication; <In section 2 of this draft ballot>*
> *network boundary control; <In section 1 of this draft ballot>*
> *audit logging; <In section 3 of this draft ballot>*
> *audit log reduction and analysis; <In section 3 of this draft ballot>*
> *vulnerability scanning; <I **think** included in draft ballot addressing updates to section 4>*
> *physical intrusion detection; <I **think** included in draft ballot addressing updates to section 4>*
> *host-based intrusion detection; and <I **think** included in draft ballot addressing updates to section 4>*
> *network-based intrusion detection. <I **think** included in draft ballot addressing updates to section 4>*
> 👂

System: One or more pieces of equipment or software that stores, transforms, or communicates data.

> *With the removal of genericized references to "systems", we may be able to remove this definition as well.*

Trusted Role: An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.

> *While I have **not** made changes to this definition, other than to remove references to removed terms related to Zones, I do believe we could modify this term to make it more readily/accurately interpretable by readers, e.g. "privileged role" or "assigned responsibility". The use of "trusted" in this term seems to imply, to me, a lack of checks and balances otherwise expected within these Requirements.*
> ✏️

Vulnerability Scan: A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

> *It's not clear that options above and beyond NVD provide useful extensions to what's allowed here.*

> *A definition for "Workstation" has been added since the term was used in the NCSSRs, but not defined.*

Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

> *Zone has been removed both as a definition and from use within the NCSSRs.*

> *The overall formatting of the NCSSRs has drastically changed. I personally — and I believe this has also been experienced by others — have encountered challenges in trying to propose changes to the NCSSRs simply because the current formatting can be difficult to work in and around. The use of lettered lists with a single, overarching RFC2119 verb tends to limit the way new requirements can be phrased while fitting into this style.*
> *The current format, whether causally or otherwise, has also resulted in a number of requirements related to a single topic being represented in multiple, disconnected sections of the NCSSRs. This duplication or separation of requirements addressing one topic has resulted in confusion and differences of interpretation around the scope of applicability of aspects of the NCSSRs.*
> *Without a central style guide within the CA/BF, I nonetheless attempted to update the formatting and style of the NCSSRs to more closely match those of other CA/BF guidelines, though I did not use RFC 3647 format at this point. Similarly, I attempted to rearrange requirements such that the outcome is a document which has requirements building on top of prior requirements, related requirements in proximity to each other, and simplification of some requirements due to various de-duplications.*
> *These changes are still very much a **draft**, and a relatively early draft at that. I've personally become convinced that a large, relatively comprehensive change is necessary for the NCSSRs to move forward meaningfully over the coming years. That doesn't mean this is a fact, nor does it mean that every single change in this draft is part of what I think is important. I am very interested in feedback for any and every aspect of this update, the earlier the better.*
>
> *Each requirement below has some additional information about how and/or where it was shifted to.*
>
> *As a final note, I worked through updates sequentially from section 1 to section 3. Thus, I think there are still some inconsistencies in how I updated language in section 1 compared to section 3. This has been left in intentionally for the moment, as I'd like to understand if there is any preference for any particular approach represented; if not, my next draft update aligns language and phrasing towards that used more in section 2 & 3.*
> 👂

1. GENERAL PROTECTIONS FOR THE NETWORK AND SUPPORTING SYSTEMS

EACH CA OR DELEGATED THIRD PARTY SHALL:

a. Segment Certificate Systems into networks based on their functional or logical relationship, for example separate physical networks or VLANs; <<1.1.1>>

> *This requirement remains the first in the NCSSRs. It's also been broken apart slightly to encompass related requirements implied by '1.f' and an additional sub-requirement has been added to provide better directional guidance on the intention of requiring such segmentation.*

b. Apply equivalent security controls to all systems co-located in the same network with a Certificate System; <<1.2.3>>

> *This requirement is relatively unchanged, but it has been shifted to the end of the 1.2 requirements as a "capstone" so that the requirements read (imo) more sequentially, e.g. "here's what you have to do. here's where you have to do it."*

c. Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks; <<1.2.1>>

> *As mentioned above for the definition of Physically Secure Environment, this requirement should likely change to ensure the NCSSRs have clarified that the level of security expected of the Root CA System is greater than that of the rest of the CA Infrastructure; my current draft and the current NCSSRs effectively require almost the same security for almost everything (meaning that it's difficult, if not impossible, to clearly differentiate the expectations for Root CA Systems compared to all other "systems").*
> 👂

d. Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone; <<1.2.1>>

> *This requirement has been combined with the preceding one; as noted, this should be addressed further and I believe the most appropriate way to address this in a way that's maintainable is to fully remove Root CA Systems from the scope of the NCSSRs (or at least what is typically viewed as the NCSSRs today). That extension of scope for this draft was determined excessive, so for the moment I have combined the requirements in an arguably less optimized way.*

e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks; <<1.2.2>>
f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; <<1.2.2>>
g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party; <<1.2.2>>

> *The above 3 requirements (1.e, 1.f, and 1.g) have been combined into one section with two requirements. The wording has also been updated to hopefully simplify and clarify the requirements. That said, I'm not entirely satisfied with the second requirement's structure, however the fix I'd like (removing the first item from the numbered list, replacing it with a more simple phrase to the effect of "anything else is disabled") would potentially have a more meaningful impact on CAs currently complying with the NCSSRs than desired.*
>
> *Something more could be added here to address further the existence and expected properties of connections between the CA's infrastructure and external infrastructure, e.g. "Connections between CA Infrastructure and non-CA Infrastructure MUST be secured within a demarkation zone and SHOULD be minimized.", but I wasn't enthusiastic about that language so have left it out.*
> ✏️

h. Ensure that the CA's security policies encompass a change management process, following the principles of documentation, approval and review, and to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems follow said change management process; <<1.3>>

> *This is the first requirement related to a CA's use of a change management process, but section 3.a explicitly references the same and 2.a implicitly requires what is effectively a change management process. I've thus combined all the references to change management into Section 1.3 of this draft*
> *I have currently kept this requirement in Section 1, but do not feel it actually belongs in any of the sections I've touched in this draft (Infrastructure, Access Control, Audit Logs). I think I would prefer separating this into its own new section, but felt that may be a bigger shift than deemed acceptable.*
> *Aside from the collapsing requirements from 3 sections into, and figuring out where best to fit, these requirements, the draft also more explicitly outlines expectations for a CA's change management process (though hopefully in a way that's compatible with what CAs are already doing and requires no or minimal changes).*
>
> *The intent with the phrasing of 1.3 in this draft is that CAs may continue to utilize separate change management processes for 1.h, 2.a, and 3.a, but there are also likely efficiency gains to combining some aspects of them, which will hopefully be more obviously allowed with these changes.*
>
> *One item pending for this change is to review WebTrust and ETSI criteria to determine if there's meaningful difference between those and this draft.*
> 👂

i. Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System’s security; <<2.2.1>>

> *Organizationally, I shifted this (and the following 2 requirements) into Section 2, following the requirements for managing Trusted Roles.*
> *Structurally, the current requirement is vague (as neither “administration access” nor “accountability” is defined) and consequently seemingly difficult to measure/enforce. I opted to focus the requirement on what seems to be its core value: managed limitations of access. I also pulled in the requirement currently represented in 2.e requiring configuration of access privileges to observe the principle of least privilege (also now a defined term) as that does not seem meaningfully different from what this requirement states (“grant access” vs “configure access privileges”).*
> *This approach ultimately resulted in combining 1.i, 2.c, and a part of 2.e into one requirement.*

j. Implement Multi-Factor Authentication to each component of the Certificate System that supports Multi-Factor Authentication; <<2.2.3>>

> *Organizationally, this has been shifted into a subsection of 2.2 “Access Management”, combining 1.j with 2.m and 2.n, all of which require MFA usage separately. However, when taking these 3 requirements collectively, the resultant requirement is rather simpler. This includes the removal of the clause which currently heavily limits the reliability of the current requirements, i.e. “that supports Multi-Factor Authentication”.*
> *The combination with 2.m also extends the new 2.2.3 to include requirements for Multi-Party Control (now a defined term).*

k. Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person’s authorization to administratively access that account on the Certificate System is changed or revoked; and <<2.2.1.3>>

> *This has been moved down under a subsection of 2.2 “Access Management” and combined with 2.i which similarly sets requirements for altering authentication credentials under certain conditions and within certain timeframes.*
> *With this combining, I kept the two described scenarios separate. This leaves the NCSSRs with a required timeframe for removing access after an individual leaves a CA’s employment/contract, but without an explicit timeframe for removing access after authorizations empowering an authentication credential are changed/removed.*
> *It seems it may be possible to further combine these scenarios so that a single process can address all changes in authorizations, removing the implicit zero-second expectation currently present for half the draft 2.2.1.3’s requirements. This is especially warranted, in my opinion, since the broader requirement related to changed authorization arguably encompasses at least some of the more specific requirement related to changes in employment/contracts, potentially creating a scenario where CAs are non-compliant if authentication credentials aren’t changed or revoked at the same instant as associated authorizations are changed or revoked.*
> 👂

l. Apply recommended security patches to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

> *This requirement has not been included in the current draft as its enforced requirements are currently represented in the draft ballot NS-002, moving this requirement into section 4.*

2. TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS

EACH CA OR DELEGATED THIRD PARTY SHALL:

a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them; <<1.3>>

> *As mentioned above for 1.h, this requirement has been moved to Section 1.3 “Change Management” and consolidated with other requirements in the NCSSRs which expect a formal change management process to be established and followed.*

b. Document the responsibilities and tasks assigned to Trusted Roles and implement “separation of duties” for such Trusted Roles based on the security-related concerns of the functions to be performed; <<2.1>>

> *This requirement is the introduction to Section 2 “Access Control” and should intentionally set the stage that a primary*

> *component of a CA's control of access to its infrastructure relies on documenting the roles the CA's personnel have. The requirement has been broken apart to separately define the scope for which Trusted Roles must be established (implied currently by 2.b, but not stated explicitly) and the requirement that the "properties" of a given Trusted Role be documented. The requirement has also expanded to encompass aspects of 2.e and 2.m which overlap with 2.b's mandate.*
>
> *It may also be worthwhile to expand, either here or in 1.3, on expectations around timelines for when a change is made and when the documentation required here is updated, e.g. "If changes occur to a Trusted Role's responsibilities, privileges, or access, such documentation MUST be updated prior to the change taking effect.". I think this is already covered by 1.3, but explicit clarity may be valuable to implementing and assessing parties.*
>
> *As it's come up in discussion, I'll also highlight that there's nothing in the NCSSRs which prevents a CA from assigning potentially conflicting Trusted Roles to an individual, e.g. allowing the same individual to gather validation evidence documents and also review/approve the data for use within a certificate. This is intentional and currently assumed that any such limitations would be documented in a policy document with a broader scope than the NCSSRs, such as the TLS or S/MIME BRs.*
>
> 👂

c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; <<2.2.1>>

> *As mentioned above for 1.i, this requirement has been combined with 2.c and a part of 2.e, hopefully resulting in a simpler — and easier to confidently implement — requirement. For this requirement specifically, the removal of definitions for and use of "Zones" necessitated altering what this requirement is limiting access to for Trusted Roles.*

d. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; <<2.1.1>>

> *Similar to 1.i, this requirement seems inherently difficult to measure, if not also implement. I would be open to altering to better reflect the intended outcome of this requirement, e.g. "The CA MUST ensure responsibilities, privileges, and access assigned to a Trusted Role are only performed or used by personnel assigned to an associated Trusted Role."*
> *More concretely, my interpretation of the current requirement is that it's expected to prevent the things a Trusted Role is responsible for from being done by someone without that Trusted Role assignment, so reorienting on the components of the Trusted Role, rather than the actions of personnel, seems to me to be a more measurable outcome.*
>
> 👂

e. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems; <<2.1, 2.2.1>>

> *As mentioned with 1.i, the aspect of this requirement associated with accessing CA Infrastructure has been combined with 1.i and 2.c. The remaining, somewhat implicit, requirement that Trusted Roles be defined in accordance with the principle of least privilege was combined with related requirements in 2.1. This was done because defining a Trusted Role is a prerequisite to granting access, so it made sense to me to clarify that directly in the associated section.*

f. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems (for accountability purposes, group accounts or shared role credentials SHALL NOT be used); <<2.2.1.1, 2.2.1.2>>

> *This requirement was separated into its two component pieces and placed under a subsection of 2.2 "Access Management", but otherwise largely unchanged in core requirement.*

g. If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, implement the following controls: <<2.2.4>>

- For accounts that are accessible only within Secure Zones or High Security Zones, require that passwords have at least twelve (12) characters;
- For authentications which cross a zone boundary into a Secure Zone or High Security Zone, require Multi-Factor

Authentication. For accounts accessible from outside a Secure Zone or High Security Zone require passwords that have at least eight (8) characters and are not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with subsection k;

- When developing password policies, CAs SHOULD take into account the password guidance in NIST 800-63B Appendix A.
- Frequent password changes have been shown to cause users to select less secure passwords. If the CA has any policy that specifies routine periodic password changes, that period SHOULD NOT be less than two years. Effective April 1, 2020, if the CA has any policy that requires routine periodic password changes, that period SHALL NOT be less than two years.

> *This requirement is somewhat awkward in the current document structure, but hopefully fits better within the updated section 2.2.4. The requirement has been moved towards the end of the 2.2 "Access Management" section, as it seemed appropriate to follow Workstation and MFA/MPC requirements, but it's certainly reasonable that it should be located elsewhere if there are opinions on the matter.*
> *The requirement has also been rephrased into 4 discrete requirements intended to:*
> *1. Remove prose not related to requirements;*
> *2. Reformat to align with draft document style; and*
> *3. Consolidate or remove duplicative requirements*
> *Separately, I've included the removal of the clause which currently heavily limits the reliability of the current requirements, i.e. "where technically feasible".*
> 👂

h. Have a policy that requires Trusted Roles to log out of or lock workstations when no longer in use; <<2.2.2>>
i. Have a procedure to configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user (the CA or Delegated Third Party MAY allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock); <<2.2.2>>

> *The above 2 requirements (2.h and 2.i) have been combined into a section (2.2.2) dedicated to requirements for Workstations (now a defined term).*
> *When starting on updates to this, these 2 requirements seemed somewhat out of place and difficult to "fix", i.e. restate in a way that addresses their intended function (making sure employee laptops/desktops aren't totally insecure) without unintentionally downgrading security by requiring modes of operation which have been potentially supplanted by superior security features.*
> *It was also somewhat unclear to me whether the intended scope matches the language, given the lack of definiton for "workstation". For this draft, I assumed a relatively broad scope, and so attempted to phrase the requirements in such a way as to limit the unnecessary applicability of the requirement to devices which don't present a risk needing to be addressed.*
> *The current wording of 2.h also could oddly read to required personnel in Trusted Roles to log out of or lock* ***any*** *workstation they encounter which is not in use; that's perhaps not the worst policy, but I think it leads to unexpected outcomes and so clarified the language to scope their responsibilities to their own Workstation(s).*
> *Finally, the parenthetical in 2.i seemed problematic and worth addressing, as it effectively negates any reliable/consistent value in the other requirements while introducing a caveat that complicates assessment of compliance.*
> *The result is likely a slight reduction in specificity and loosening of requirements overall, but hopefully with the result of greater consistency in results and higher confidence in assessment measurements.*

j. Review all system accounts at least every three (3) months and deactivate any accounts that are no longer necessary for operations; <<2.2.1.4>>

> *This requirement has been shifted up overall to sit within the requirements which address how access to CA Infrastructure or Network Equipment needs to be managed. The requirement was also split apart into two discrete requirements representing the current one, the first addressing the need to review and the second addressing the need to deactivate identified unnecessary accounts. This was done to allow for more direct/surgical changes to the separate aspects of the*

> *requirement in the future, based on discussion in the NSWG regarding the modernity and applicability of the current review requirement.*
>
> *While I have not drafted changes to this effect, I believe it would be worth expanding on the goals/outcomes expected of the review, for example:*
> *This review MUST:*
>
> 1. *ensure each account's necessity to the CA Infrastructure;*
> 2. *ensure each account meets these Requirements;*
> 3. *deactivate or remove any account which is not necessary; and*
> 4. *update, deactivate, remove, or otherwise remediate any account which does not meet these Requirements.*
>
> *Alternatively, this second half of the requirement is quite similar in aspects to 1.k and 2.l, which seems another possibility for consolidating the overall set of actions/processes which a CA is expected to implement (i.e. require a review, but any of its findings feed into the (slightly expanded by this) requirement that necessitates changing/revoking authentication when authorizations change).*
>
> *Finally, I also wonder whether Network Equipment should be included in scope of this requirement; I've included it currently, but would like to hear arguments for such accounts not needing to be in scope.*
> 💡

k. Lockout account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure; <<2.2.1.5>>
Is supported by the Certificate System,
Cannot be leveraged for a denial of service attack, and
Does not weaken the security of this authentication control;

> *This requirement seems largely neutralized by the multiple provisions allowing CAs to not enforce it that I'm not sure it's very useful or provides meaningful value to the NCSSRs.*
> *For example, I would posit that _by definition_ *any and every* automatic lockout function *can* be used to cause a denial of service, using the Oxford definition (since we don't have one) of "an interruption in an authorized user's access to a computer network"*
>
> *There is currently no specification or guidance around how long the lockout should be for or within what timeframe applicable failed attempts need to occur.*
> *As a potentially extreme example, since the NCSSRs don't currently say the lockout is in any way temporary or even reversible, is it reasonable to interpret this as requiring CAs to indefinitely lock out accounts after 5 failed access attempts? Further, since no timeframe is defined, as currently worded the requirement is that "If 5 failed access attempts occur* ***ever****, lockout account access* ***forever****."*
>
> *Despite its extremity, I consider the above a valid (and potentially* ***necessarily*** *risk-averse) interpretation. Further, I would expect every CA to then consider this as either being able to cause a denial of service or a weakening of the authentication control and, therefore, not required to be implemented? Or, if they do implement it (which, in reality, I suspect most CAs do in some way), they may likely do so in a way that differs from the above reading of the requirement, which circles back to my hypothesis that this requirement may not being meaningful in practice.*
>
> *Less importantly, I'm also not sure I understand the intent resulting from stripping out intermediary language, i.e. "lock out account[s] provided [it] does not weaken the security of [locking out account access]".*
>
> *With that, this requirement has been updated to more generically address the desired outcomes of this requirement as I understand them (minimize the susceptibility of CA Infrastructure to* ***unauthorized*** *access, particularly through repeated, failed attempts to authenticate). I've also included 2 SHOULD statements and otherwise removed the provisions which allow a CA to avoid this requirement entirely (if they're of a mind to), with the intention that the more generic language will allow compliance without compromising continued use of the CA's own risk assessment-based access controls.*

> *I considered, but discarded, including examples of typical measures, like account lockout policies, rate limiting, and IP blocking.*
> *Further, there seems potential unrealized value in tying the goal of this requirement more directly to the MFA requirements of 2.2.3, the Password Complexity requirements of 2.2.4, and the monitoring/logging requirements in section 3.1.1 (i.e. a lockout policy is great, but if not monitoring for systems that trigger a lockout, then the bigger picture may be missed).*
> 👂

l. Implement a process that disables all privileged access of an individual to Certificate Systems within twenty four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party; <<2.2.1.3>>

> *As mentioned with 1.k, this requirement has been placed into the same section as 1.k's requirement to (hopefully) improve document cohesion.*

m. Enforce Multi-Factor Authentication OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems; <<2.1, 2.2.3>>

> *As mentioned with 1.j, this requirement has predominantly been combined with 1.j and 2.n into 2.2.3. However, given the implied necessity to consider these requirements when defining Trusted Roles, a small tie-in has also been added to 2.1.*

n. Enforce Multi-Factor Authentication for all Trusted Role accounts on Certificate Systems (including those approving the issuance of a Certificate, which equally applies to Delegated Third Parties) that are accessible from outside a Secure Zone or High Security Zone; and <<2.2.3>>

> *As mentioned with 1.j, this requirement has been combined with 1.j and 2.m into 2.2.3.*

o. Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: <<2.2.5>>
the remote connection originates from a device owned or controlled by the CA or Delegated Third Party,
the remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication, and
the remote connection is made to a designated intermediary device
i. located within the CA's network, ii. secured in accordance with these Requirements, and iii. that mediates the remote connection to the Issuing System.

> *This requirement has mostly been reformatted into a nested list and updated to use newly defined terms (e.g. "Requirements").*
> *I think there is still room for improvement on this requirement (e.g. it's not clear to me that "mediates" is used in a way that results in consistent interpretation/implementation).*
> *Aside from that, it's not entirely clear that the limitations set here are balanced to be entirely appropriate/necessary for the security of the CA Infrastructure; I'm not sure in what way exactly, but it seems like something here could be removed with no decrease in security.*
> *It also strikes me as slightly odd that we don't reference VPNs in context of a requirement that seems to be clearly talking about the properties of a VPN. I think that's appropriate to ensure the requirement isn't overly specific, but it would perhaps be helpful to implementers to have an example provided on which to ground their reading of the requirements.*
> ✏️

3. LOGGING, MONITORING, AND ALERTING

CERTIFICATION AUTHORITIES AND DELEGATED THIRD PARTIES SHALL:

a. Implement a System under the control of CA or Delegated Third Party Trusted Roles that continuously monitors, detects, and alerts personnel to any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems unless the modification has been authorized through a change management process. The CA or Delegated Third Party shall respond to the alert and initiate a plan of action within at most twenty-four (24) hours; <<1.3, 3.1.1, 3.2.1, 3.2.2, 3.2.3 and 3.2.3.1>>

> *This requirement, perhaps more than any other, encompasses a large number of discrete requirements jammed together in way that doesn't make it obvious how much is going on — and which I found challenging to parse all at once.*
> *I broke the component which brings this requirement under scope of a change management process off to be included in the more directly applicable Section 1.3.*
> *I then broke apart and described separately the requirement to implement a system (which I genericized to "policies and procedures" as a single system may not be typically applicable to comprehensively monitoring as described here) into section 3.1.1, and combined the requirements of 3.b to represent the expectations related to setting up monitoring and logging.*
> *I then separated out the detection and alerting components, fitting them into subsections of 3.2 dealing with Audit Log Processing and Alerting and combining where relevant with overlapping requirements of 3.c, 3.d, and 3.g.*
>
> *Ultimately, pieces of this requirement ended up strewn across almost all of Section 3, but I think the overall outcome is more comprehensible regarding how all the requirements fit together to result in a useful component of the CA's infrastructure. Care was taken (or at least attempted) to remove possible conflicts or reliance on external requirements, such as the TLS BRs, to ensure the broader applicability of these requirements within and without the Forum.*
>
> *The primary area I identified to further improve this section is to better document the potential utilization of these logs, however I avoided attempting to tackle this as I feared it would result in documentation of details better suited to more specific requirements, such as the TLS or S/MIME BRs.*
> 👂

b. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity, and enable those systems to log and continuously monitor the events specified in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; <<3.1.1 and 3.1.1.1>>

> *The first part of this requirement was combined with a small portion of 3.a in 3.1.1. The second half of the requirement was then separated into 3.1.1.1 to separate requirements dealing with identification of logging/monitoring capabilities from requirements dealing with enablement of those capabilities.*
> *Finally, a pair of SHOULD statements was added to 3.1.1 to further clarify the intention behind separately identifying logging/monitoring capabilities (i.e. doing so is part of the CA's overarching policies and procedures related to audit logs and their use) based on an assumption that these activities are already done by CAs, but don't necessarily need to be normatively required. While these are SHOULDs, they're also arguably required by the confluence of 3.a, 3.b, 3.f, etc.*

c. Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events; <<3.2.1, 3.2.2, 3.2.3>>

> *This requirement starts the portion of Section 3 dealing with processing audit logs, however I'm also breaking this requirement apart to improve clarity around the various currently-included components (i.e. processing, alerting, following up).*
> *Further, because of the interaction between 3.a and 3.c, the expectation documented is that audit log processing results in identifying possible unauthorized changes to CA infrastructure as well as Critical Security Events. The separation of these outcomes did not seem additive to the document's utility; in fact, it seemed confusing as to why multiple systems might seemingly be expected for something that could be (but isn't required to be) handled within one context.*

d. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events; <<3.2.3 and 3.2.3.1>>

> *This requirement has been combined with the alerting requirements of 3.a, 3.c, and 3.e, while also attempting to address some of the vagueness of the requirement to "follow up".*

e. Monitor the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days. <<3.1.2>>

> *This requirement was moved up to fit within the logging and monitoring portion of Section 3, in 3.1.2. The first part of this section matches relatively closely with the current 3.e, except in one way expounded on further below.*
>
> *The second part of 3.1.2 adds an explicit requirement for what is currently implied, that is that integrity monitoring be configured "in a manner sufficiently effective to identify possible audit log compromise." This was done because 3.g's reference to 3.e makes it seem that alerts originating not from processing audit logs, but from ensuring audit log integrity should also be included in the same "pipeline" as the 2 classes of alerts that come from processing audit logs. Though there's a requirement to ensure audit log integrity, there's not really a requirement to do something which results in identifying when audit log integrity is compromised, so there's no origin for the "identification" (which, when it occurs, otherwise results in the "alert" which results in the "response" which results in the "plan of action"). Hence, I added that missing "bridge" to 3.1.2.*
>
> *For the change between 3.e and 3.1.2, I've intentionally not included the "system is online" requirement based on the following assumption(s):*
>
> *1. we'll be moving the Root CA System requirements to their own section or possibly even document (as, at that point, we're not really talking about a network — we're talking about a _lack_ of a network — and we're not really talking about a security system — we're talking very specifically about a much narrower scope, the Root CA System, which is far from anything resembling a general security system (Though I'll admit I also don't recall if separating it into its own document has already been discussed and rejected by majority consensus));*
>
> *2. none of the other parts of CA Infrastructure are kept inherently, persistently, or in a default state of "offline", like a Root CA System;*
>
> *3. the phrase in the current requirements "if a human review is utilized and the system is online" was/is intended to specifically (or at least primarily) refer to the Root CA System; and*
>
> *4. while I don't think it'd be the best idea to _mandate_ that a manual review be performed on (inherently, persistently, and in a default state of) offline Root CA Systems, it doesn't seem preternaturally *bad* to _allow_ the CA to monitor their logs in such a way — I don't think it's terribly uncommon for larger CAs with many service offerings to perform an offline key ceremony at least as frequently as monthly.*
>
> *If any of these assumptions is incorrect, we should probably/possibly re-add the requirement that manual review can only occur for online systems.*
>
> *Alternatively, if I'm misinterpreted the intent of the wording in 3.e, and how it uses "and the system is online", that would also be good to identify.*
>
> 👂

f. Monitor the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation. <<3.1.2.1>>

> *This requirement was moved up into the logging and monitoring part of Section 3, in 3.1.2.1. The requirement was reformatted and a SHOULD statement was added to provide additional clarity/context (though I think it could/should be made a MUST).*
>
> *There's a bit of somewhat subtle, potentially unnecessary, specificity in the current 3.f in that CAs must currently monitor archival/retention of logs in order to ensure they're retained correctly, but it's not necessarily true (in my opinion) that monitoring is an absolute necessity for the outcome of having audit logs archived/retained for the appropriate amount of time.*
>
> *The phrasing "the disclosed business practices" is unclear with regard to what it's referencing (seemingly "the CA's disclosed business practices"?), but I think reusing the similar language from 3.1.1.1 and 3.1.1.2 works here as well to keep this concept consistently referenced.*
>
> *There are also several very closely adjacent requirements not specified here, such as secure storage and access control. These could be inferred by the requirement that they be retained (which would imply they not be lost, damaged, or otherwise made unavailable in any form other than the form in which they were originally archived/retained), but perhaps highlighting these aspects would help lead to better outcomes.*

> 👂

g. If continuous automated monitoring and alerting is utilized to satisfy sections 1.h. or 3.e. of these Requirements, respond to the alert and initiate a plan of action within at most twenty-four (24) hours. <<3.2.3 and 3.2.3.1>>

> *This requirement retains its position at the end of Section 3, but has been broken down to provide increased precision describing the current requirement and adds a SHOULD statement to provide additional clarity as to the purpose of the requirement.*
> *When first working through incorporating this requirement, I encountered several questions/issues:*
> *1. it's not clear how continuous monitoring/alerting satisfy 1.h (a part of 1.h, sure, but the entirety of the change management process certainly doesn't fit into monitoring/alerting)*
> *2. the requirements for responding and initiating a plan of action are weak/vague*
> *3. the presence of a timeline for automated monitoring/alerting highlights the stark lack of a timeline for non-automated monitoring/alerting*
> *4. 3.g requires responding to an alert within 24 hours, but only for 3.e and 1.h, somehow missing the "main" automated alerting requirement which is 3.c*
> *Ultimately, I tried to keep the requirement the same in its essence. I do think it would be an improvement to also define a requirement for when the initial response must **conclude**, e.g. "The CA MUST ensure the initial response is completed within seven (7) days of commencing."*
> ✏️