CCE List Submission and Style Guidelines

Date: March 4, 2011 **Document version:** 0.1

Table of Contents

Introduction

The purpose of this document is to describe the basic process by which members of the information security community can submit properly formatted CCE entries (also called "CCEs") to the CCE Content Team so they can be reviewed, have CCE Identifiers (CCE-IDs) assigned, and be published on the CCE List for use by the community.

This document is divided into two main sections:

- **CCE Submission Guidelines –** describes how to submit content for the CCE List, including acceptable file formats, how to organize the content for submission, and how to contact and coordinate with the CCE Content Team.

- **CCE Style Guide –** provides detailed guidance on how to create well-formatted CCE entries, on a field-by-field basis.

CCE Submission Guidelines

Submitting new or updated content to the CCE List consists of five primary steps:

1. **Select preferred submission format -** Content can be submitted using an approved spreadsheet format (Microsoft .xls or .xlsx).

2. **Organize submissions by platform group –** In general, a platform group corresponds to a major release of an operating system or software product.
3. **Organize submissions in terms of new entries and updates to existing entries -** New entries involve a more complex set of considerations than updates to existing entries, particularly in how new entries are discriminated between or counted.
4. **Follow CCE Style Guide for content creation -** CCE has established guidelines for how to discriminate between CCE entries (i.e., "counting" CCEs) and for authoring the content associated with each CCE entry. Consult the CCE Style Guide for general guidance and the CCE Content Decisions for more detailed guidance.
5. **Submit content for review -** To ensure consistency and utility, newly proposed CCE content is reviewed by the CCE Content Team and then distributed to the CCE Working Group for comment prior to being accepted as official CCE content. Submissions should be sent directly to the CCE Content Team at cce@mitre.org to begin this review and comment process.

More details on each of these steps are provided below.

Submission Formats

The approved format for submitted CCE content is in the form of Microsoft Excel spreadsheets (.xls or .xlsx). CCE publishes a set of preformatted spreadsheets that can be used to describe CCE content. Please contact the CCE Content Team at cce@mitre.org to request the CCE Submission Spreadsheets.

By prior agreement only and as situations merit, the CCE Content Team may accept content submitted in other machine readable formats. Please contact the CCE Content Team at cce@mitre.org to determine if there are any mutually agreeable formats prior to submitting content.

Separate Submissions by Platform Group

CCE-IDs are assigned based on platform groups. In general, a CCE platform group corresponds to a major version release of an operating system or application. Because configuration guidance documents are typically authored and configuration audit/management capabilities are often licensed or deployed according to such major releases, CCE-IDs are similarly divided. To ensure that CCE platform groups correspond to industry recognized major releases, the creation of new platform groups is done in close coordination with and input from the CCE Working Group, whose membership includes representatives from industry, government and academia.

Before authoring CCE content, determine whether or not CCE already has any existing platform groups that are applicable. The current list of recognized platform groups can be found on the CCE List page. If an applicable platform group does not exist, contact the CCE Content Team at cce@mitre.org to discuss the possibility of creating a new platform group.

When submitting new or revised content for multiple platform groups, please clearly separate the submissions according to platform groups. Using separate files (XML or spreadsheets) for separate platform groups is strongly preferred.

Note:

Content submitters are *strongly advised* to verify and coordinate their choice of platform groups with the CCE Content Team before spending time and resources on creating new CCE content.

Separate New and Updated Submissions

Newly proposed CCE entries and updates to existing CCEs are reviewed differently. The primary difference is that for newly proposed CCE entries, close consideration is given to how the newly proposed entries are discriminated or counted. Ideally, CCE-IDs correspond to discrete configuration controls as defined by the security model of the system. In practice, it can prove difficult to create new CCE entries that are consistent with established CCE practices and existing CCE entries.

When submitting both new and revised content for any given platform group, please clearly separate newly proposed CCE entries from proposed edits to existing CCEs. Using separate files (XML or spreadsheets) for new and updated entries is strongly preferred.

Apply Documented Style Guide and Content Decisions

For the sake of consistency, new or updated CCE new entries should be as similar to existing CCEs as is practically possible. The CCE Content Team strongly suggests reviewing the following resources prior to creating or modifying CCE entries:

- Review the CCE List to find similar entries, paying special attention to entries from closely related platform groups that correspond to similar areas of functionality. For example, when creating new CCE entries for a new major release of an operating system or application and if there is a CCE platform group for a prior major release, then review the entries in that platform group closely. In particular, ensure that issues are counted (separated out as individual entries) in the same manner, unless there is a compelling reason to do otherwise. Likewise, reuse elements (description, parameters, and technical mechanisms) from existing CCE entries, whenever possible.

- Review the CCE Style Guide, which provides basic guidance for populating each element or field.

- Become familiarized with the CCE Content Decisions document, especially when creating new CCE entries. The primary focus of the content decisions document is to provide more detailed guidance on how to delineate (i.e., count) CCE entries.

Submit Content for Consideration

Please send proposed content to the CCE Content Team at cce@mitre.org, as follows:

- **Email subject line:**
  - Include the name of the content on the subject line. For example, "Subject: CCE Content Team, Windows XP".

- **Email body:**
  - Your name, organizational affiliation, and job title.
  - Description of the content, including a list of existing or pre-approved new platform groups and whether the proposed content contains new CCE entries, updates to existing CCEs, or both.

- **Attachments:**
  - Include a copy of each reference document referred to in your content.

- For each platform group, include a separate submission file for proposed new entries and for proposed updates to existing entries.

CCE Style Guide

CCE entries must provide enough information to allow security analysts to recognize individual entries, and to distinguish between a set of entries. To this end, there are two primary issues when creating CCE content. The first is to correctly delineate (i.e., count) the entries. In CCE vernacular, this is often called the "level of abstraction" problem. The second is to create correct and well formatted information for the five fields that define a single CCE entry: ID, Description, Parameters, Technical Mechanisms, and References. We discuss each of these in more detail in the sections that follow.

Note that acceptable style for both counting and authoring have evolved over the course of CCE's history and it is expected that style will continue to evolve based on feedback from the CCE Working Group. This document will be updated as new decisions are made. Please verify that all submissions to the CCE Content Team align with these guidelines prior to sending a submission.

For more information on submitting new and modified CCE content to the CCE Content Team, please review the CCE Submission Guidelines.

Counting: The Delineation of Entries

Experience has shown that the process of delineating or "counting" entries is among the most controversial topics within CCE, and the most difficult to master for analysts creating CCE content for the first time. Typically, the following principle applies:

> *CCE-IDs are associated with the lowest level controls (most granular) of the human comprehensible abstract security model of the system.*

This statement attempts to capture the tension involved with creating CCEs at the correct level of abstraction. On the one hand, it is common for analysts to talk and write in a way that naturally groups individual configuration controls together. Examples include, "strong passwords" or "install and configure FTP". For CCE, these statements are at too high of a level of abstraction and they should be decomposed into more granular individual statements. This is what is meant in saying that CCE-IDs are associated with "the lowest level controls (most granular)."

On the other hand, a system will typically provide multiple technical mechanisms by which the same conceptual configuration control can be applied. For example, the same configuration control might be applied via: (a) a selection in a graphical user interface, (b) a variable defined in a configuration file, or (c) a function call in the system's application programming interface (API).

Because all three of these technical mechanisms achieve the same conceptual effect, CCE considers them to be comparable at the level of the "human comprehensible abstract security model". For this reason, different CCE-IDs are not associated with these individual technical mechanisms and, instead, a single CCE-ID is associated with the conceptual security control that unites them (relative to the conceptual security model for the system).

In practice, determining this level of abstraction can be difficult. We offer the following general guidelines. For a more detailed discussion on counting issues, please refer to the CCE Content Decisions. When in doubt, please seek guidance and input from the CCE Working Group mailing list (first) and the CCE Content Team (secondly).

CCE Counting Guidelines:

- CCE-IDs tend to be associated with selection controls in commonly used graphical user interfaces (GUIs). This is because GUIs tend to be designed to present the conceptual security model to the user.
- Create CCEs in a manner consistent with prior, related CCEs. When creating CCEs for a new major release of a system, review all CCEs for prior major versions of the system. It is common for security models (or portions of security models) to be reused across major releases. CCE-IDs must be consistently created across these major releases. CCEs should only be assigned differently when there has been a significant change in the security model between major releases.
- CCEs for applications tend to be similar for CCEs for the operating systems they are designed to run on. It is common, but not universal, for applications to use security models that are native to the underlying operating system that the application is expected to be installed on. For example, an application may manage user accounts and rights by utilizing native operating system account constructs. In these cases, CCEs for the application should be assigned in a manner that is consistent with those assigned to the base OS. For this reason, when creating CCEs for an application, review associated OS CCEs carefully. Some applications have security models that are truly cross-platform, and in those cases OS level CCEs may not provide helpful guidance.
- Consult the CCE Content Decisions. Over the years, many difficult and recurring counting issues have been encountered and discussed by the CCE Working Group. The lessons learned from these discussions are reflected in these CCE editorial policies.
- Consult the CCE Working Group. CCEs must be recognizable for constituents across the range of the configuration management life-cycle. The CCE Working Group is populated by security professionals who represent the cutting edge of the field. It is always appropriate and we actively encourage CCE content authors to discuss CCE creation questions on the CCE mailing list and to seek the input and guidance from industry peers.
- Consult the CCE Content Team. In those cases in which neither the Content Decisions document nor the CCE Working Group provide sufficient guidance, please contact the CCE Content Team at cce@mitre.org. For difficult counting issues, we actively encourage CCE content authors to seek guidance from the CCE Content Team prior to investing large amounts of labor. Experience has repeatedly shown that pre-coordination on counting issues makes both the CCE authoring and final review to go more smoothly and efficiently.

Elements of a CCE Entry

CCE-Identifier Number (CCE-ID)

Like the Common Vulnerabilities and Exposures (CVE®) project, CCE assigns identifier tags to each commonly recognized configuration issue. These identifiers are intended to be unique tags or keys, not descriptive names. By way of a loose analogy, CCE-IDs are like license plates on cars. They act as a unique identifier but are not descriptive. Like license plates whose issuance is overseen and coordinated by a state's registry of motor vehicles, the issuance of official CCE-IDs is centrally managed.

CCE's stated goal for identifier assignment is to evolve towards a "federated" ID assignment model similar to that used by the International Standardized Book Number (ISBN) system. In this system, authorized organizations can issue new IDs while final oversight and management of the system is maintained by a central management authority. The ability for an organization to assign CCE-IDs is dependent on that organization demonstrating a mastery of the basics of CCE content creation, particularly with respect to counting (i.e., level of abstraction) issues. CCE maintains a centralized ID generation capability that guarantees the generation of unique IDs with correct check digits. No other organization is authorized to generate CCE-IDs, as doing so will destroy the uniqueness of IDs, and with it, the integrity of the CCE system. Organizations that have demonstrated mastery of CCE content authoring and who wish to assign CCE-IDs as a part of their CCE content creation process can obtain blocks of pre-generated CCE-IDs from the CCE Content Team.

Summarizing, there are three options available for populating the "CCE-ID" column in a CCE spreadsheet when submitting new content.

- **Leave the "CCE-ID" column blank** - It is acceptable for this column to be left blank entirely. This is the most common approach used for initial submissions.

- **Use a proprietary ID** - If the authoring organization has a preferred proprietary identifier system or internal key for individual proposed CCE entries and if it would be helpful to have those identifiers associated with the proposed entries during the authoring or review process, it is acceptable to populate this column with those IDs.

  However, please note the following:
    - The proprietary IDs must be unique.
    - These IDs will be removed entirely if/when CCE-IDs are assigned by the CCE Content Team. (If it is desirable to have the proprietary IDs to be permanently associated with the CCE entries, please also add them in the "References" field as well.)

- **Assign pre-generated CCE-IDs -** If your organization has been approved by CCE to assign CCE-IDs, the CCE Content Team will provide your organization with a block of official CCE-IDs that can be used to populate this column at your discretion. Your organization is also free to begin utilizing these CCE-IDs in products and publications on a provisional basis. It must be emphasized that review of proposed CCE-IDs by the CCE Working Group and the CCE Content Team may reveal deficiencies in the proposed content that may require entries to be modified and for proposed CCE-ID assignments to be deprecated. Managing such deprecations is costly for both CCE authors and CCE users, and for this reason, we urge CCE authors to exercise due care when assigning CCE-IDs. In particular, if the entries involved are at all potentially controversial in terms of counting (i.e., level of abstraction issues), we strongly advise authors to seek guidance and input from both the CCE Working Group and CCE Content Team prior to assigning IDs.

Description

CCE entries contain a humanly understandable description of the configuration control. This description is intended to describe the control in terms of the conceptual security model. Arguably, the description is the most important field in allowing analysts to quickly and accurately recognize an entry and to distinguish it from other entries.

Because selection controls in GUIs tend to reflect the security model of the system and are so formative in terms of CCE counting, it is considered best practice for the description to reflect the language associated with the names or strings from most common GUI associated with the control. With the advent of configuration management capabilities that are not locally installed on end systems (e.g., Microsoft Active Directory Group Policy Objects or XCCDF benchmarks), it is not uncommon for different GUI controls to be associated with different names or strings, despite the fact that they both are associated with the same conceptual control or CCE-ID. In such cases, the author must use discretion and choose wording that is most likely to be recognizable to users of all associated GUIs. In this light, CCE descriptions functionally operate as the "name" of a CCE entry.

CCE-IDs are used to identify a control that can be configured. But, CCE entries never make an assertion as to what particular configuration should or should not be made. Traditionally, it has been common for new users of CCE-IDs, to look to CCE content for guidance on what is considered best practice for a given particular setting. For this reason, CCE has adopted the convention of authoring descriptions in a way that emphasizes and makes clear that CCE remains agnostic on how a particular control should be configured.

For example, typical CCE descriptions include:

- "The minimum password length should be set appropriately."
- "The 'Turn off printing over HTTP' setting should be configured correctly."
- "File permissions should be set appropriately for all shell executables."

It is critical that CCE descriptions be recognizable by analysts and consistency is important to achieve this goal. When creating a CCE entry for a control in a new major release of a system for which there exists CCEs for prior versions of that system, it is expected that CCEs for "the same" control will use the same description. Please review CCE entries for prior major releases and reuse applicable descriptions when possible.

Parameters

CCE entries contain a list of conceptual parameters that would be needed to be specified in order to configure a CCE on a system. For example, for the CCE associated with "The start-up permissions on telnet should be set appropriately" (for Windows) there is a single conceptual parameter of "start up type" which has the possible values: Automatic, Manual, and Disabled. CCE entries distinguish between such humanly understandable conceptual parameters and machine understandable parameters such as the specific registry key values that might be associated with the conceptual notions of "Automatic", "Manual", and "Disabled". Established practice for CCE parameters is to list all possible conceptual values of the parameter.

While most controls are defined by a single parameter (which may have many possible values), some controls are defined by multiple parameters. In these cases, the accepted practice is to provide a list of possible values for each parameter and to delimit the lists in the spreadsheet cell with leading "(1)", "(2)", "(3), etc., as needed.

For example, in Windows 2000, there is the following CCE:

> CCE-3858-8
> Description: The required auditing for %SystemDrive% directory should be enabled.
> Parameters: (1) set of accounts (2) events to audit (3) applicability

As with descriptions, consistency across associated platform groups (i.e., major releases) is important. For this reason, it is expected that CCE content authors review associated platform groups and reuse parameter descriptions when possible.

Technical Mechanisms

For any given configuration issue there may be more than one way to implement the desired result. For example, in Windows the issue of "The Autoplay feature should be set correctly for all drives" can be set either with a direct registry key edit or by way of a Group Policy Object if the system participates in an Active Directory domain. And in most forms of Unix and Linux, the issue of "The FTP service should be enabled or disabled as appropriate" can be achieved in multiple ways.

The listing of technical mechanisms for a CCE entry serves two purposes. First, it augments and enriches the description of the CCE. While the "Description" field describes the issue at a conceptual (i.e., GUI) level, the associated technical mechanisms describe the issue at a more technical level. Second, they help clarify the relationship between comparable technical mechanisms that achieve the same configuration goals and the CCE-ID and description that unites them.

It is common for CCEs to have multiple technical mechanisms. Each should be listed in the associated cell and should be delimited with leading "(1)", "(2)", "(3)", etc., as needed.

In cases where a technical mechanism is described by a navigation path (e.g., Microsoft registry keys or GPO settings), the accepted practice is to provide the full path.

References

Each CCE entry has a set of references from published configuration guidance documents such as the NSA Security Guides, the Center for Internet Security Benchmarks, and DISA STIGS that point to the specific sections of the documents or tools in which the configuration issue is described in more detail. These references provide a logical linkage to more detailed information, validate the need for a CCE-ID for any given configuration issue, and validate that the CCE-ID is described at a level of abstraction that is used and accepted within the community.

The submission spreadsheet should contain a single column for each reference document. The top cell of each column should contain the name of the reference document and, if it exists, a URL where the document can be accessed.

For each proposed CCE entry, provide the most granular internal identifier that is associated with the proposed CCE. Ideally, the document has a set of proprietary identifiers that map 1-1 with the proposed CCE-IDs, but in practice this is often not the case. Often, the best possible index that can be used is a section heading or page number.

Security controls that are not documented in publicly accessible documents are problematic for the CCE Working Group, especially when CCE authors are from organizations other than producer of the platform. There is a real problem of who has the authority to definitively say that a configuration control exists. There have been numerous occasions where CCEs have been proposed by third parties that were disputed by the platform vendor and ultimately rejected. For this reason, it is essential that the necessity for proposed CCEs be established by the inclusion of at least one reference. As of this time, CCE cannot accept submissions for new CCEs unless there is at least one publically accessible reference document for each proposed entry.

Example of a Valid CCE Entry

The following table is an example of a valid CCE entry.

CCE Identifier	**CCE Description**	**CCE Parameters**	**CCE Technical Mechanisms**	**Reference 1** CIS WXP Pro Benchmark v1.3
CCE-3353-0	The startup type of the IIS Admin service should be correct.	disabled/manual/automatic	(1)HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ADMIN\Start (2) defined by the Services Administrative Tool (3) defined by Group Policy	4.1.8 IIS Admin Service

Conclusion

This is a living document that will be updated over time. Please send any comments or suggestions to cce@mitre.org.