DRAFT

CONTROL CORRELATION IDENTIFIER (CCI) SPECIFICATION

VERSION 2 RELEASE 0.1

28 February 2011

DEVELOPED BY

Defense Information Systems Agency
Field Security Operations

Table of Contents

1 INTRODUCTION 3

1.1 SCOPE 3
1.2 CHANGES FROM PREVIOUS VERSIONS 3

2 WHAT IS A CCI? 4

2.1 CCI CRITERIA 5
2.2 CCI DEVELOPMENT 5
2.2.1 Comparison of Source Policy Documents 5
2.2.2 Decomposition of Source Policy Documents 7
2.3 CCI APPLICABILITY 9

3 CCI USE CASES 10

3.1 SECURE PRODUCT DEVELOPMENT 10
3.2 IA COMPLIANCE REPORTING 10
3.2.1 Rollup of Results to CCI 11
3.2.2 Rollup of Results to Source Document 11
3.3 SECURITY GUIDE DEVELOPMENT 12
3.3.1 Sourcing Requirements 12
3.3.2 Scoping Requirements 12
3.3.3 Referencing Requirements 12
3.4 SUMMARY 13

4 SAMPLES 14

4.1 GOOD CCI SAMPLE 14
4.2 BAD CCI SAMPLE 14
4.3 ROLLUP REPORTING SAMPLE 15
4.4 SECURITY GUIDE SAMPLE 16

5 REFERENCING CCI WITHIN SCAP DOCUMENTS 17

5.1 XCCDF 17
5.2 OVAL 17
5.3 OCIL 18

1 Introduction

Organizations today are faced with the daunting task of ensuring that Information Technology (IT) systems deployed within their infrastructure are securely configured and that these systems comply with the applicable security policies under which they must operate. Given the increasing number of systems, vulnerabilities and configuration settings, this task is becoming more challenging. Additionally, the integration of systems, networks and operations from different organizations may levy additional or perhaps different security compliance requirements that are based on factors such as the system's organizational affiliation, mission, function, and industry sector.

The *Control Correlation Identifier* (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks. CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies.

1.1 Scope

The CCI Specification addresses the description and identification of high-level security requirements. The specification discusses:

- Source Policy Documents (Section 2.2.1)
- Decomposition of Source Policy Documents (Section 2.2.2)
- Use Cases (Section 3)
- Referencing CCIs within SCAP Documents (Section 5)

This document does not include the CCI List XML schema, which is distributed as a separate file.

1.2 Changes from Previous Versions

In previous versions of this document, CCI was defined as "Common Control Identifier."

2 What is a CCI?

A CCI is a decomposition of an IA Control or an IA industry best practice into single, actionable statements. The CCI List is a collection of CCI Items, which express common IA practices or controls. A CCI Item is a foundational element of an IA policy or standard, written with a neutral position on an IA practice so as not to imply the specifics of the requirement. CCI can also be derived from other policy documents and the guidance expressed in a CCI is not specific to a product or explicitly associated with a Common Platform Enumeration (CPE).

The meaning of the term "CCI" varies depending on the context in which it is used, and may refer to the CCI specification, a specific CCI identifier, or the contents of a particular CCI Item.

The CCI specification is proposed to work in conjunction with the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP), as shown in Figure 1. CCI, when used in concert with the SCAP component specifications, provides additional benefits to information technology (IT) product vendors, security managers, and executive leadership.

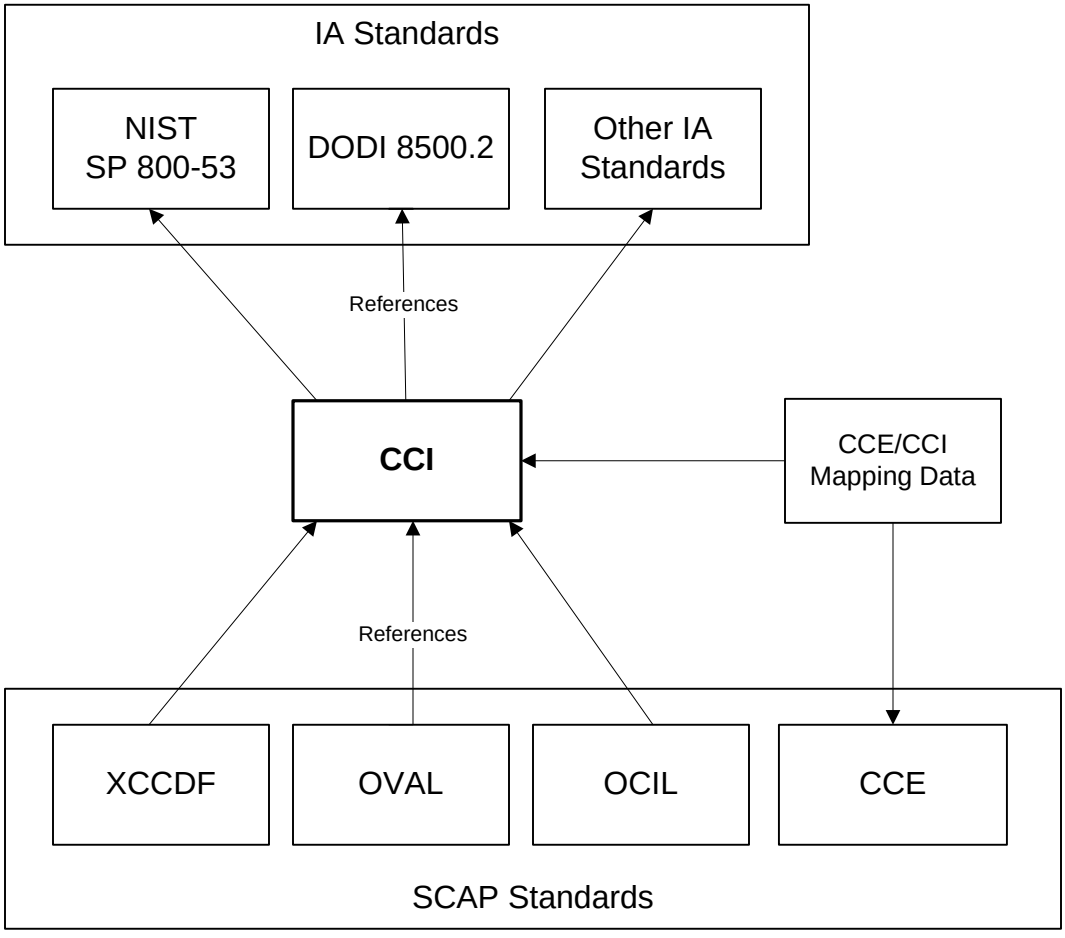

Figure 1. CCI Relationship to other SCAP Data Standards

CCIs can be used to relate items within various SCAP standards, including eXtensible Configuration Checklist Description Format (XCCDF) rules, CCEs, CVEs, Open Vulnerability Assessment Language (OVAL) definitions and Open Checklist Interactive Language (OCIL) questionnaires. CCI references in these items provide linkage to the originating policy, which

helps with reporting and consistency across technologies. Syntax and examples of including CCI references in SCAP documents are discussed in "Referencing CCI within SCAP Documents" (cf. Section 5).

2.1 CCI Criteria

A CCI must meet certain criteria to be considered a valid CCI. The following items describe the CCI criteria to be met:

- Discrete – The CCI will represent a single requirement that was decomposed from the source policy document. For example, if an IA Control for password policy were to include multiple requirements, addressing password minimum and maximum length, reuse, and minimum lifetime, five CCIs would originate from that single IA control. The five CCIs would address; a) minimum password length, b) maximum password length, c) password reuse, d) password minimum lifetime, and e) Establish admin procedures for lost/compromised passwords.
- Actionable – The CCI will represent an action that can be taken on a system or information that can be acquired by reviewing or querying organizational policy. In the previous example for minimum password length, there is a means of determining what the minimum password length setting is on the system.
- Measurable – The action that the CCI is describing must be determinate and measurable. Using the same example as above, the minimum password length can be a value that can be measured against the organization's policies or a system's configuration.

2.2 CCI Development

2.2.1 Comparison of Source Policy Documents

IA standards and policy documents are often written at varying levels of granularity, making the compliance reporting task difficult when an IA Control is comprised of multiple requirements. The technical IA requirements need to be specific and clear as to what needs to be validated to meet compliance. One objective of the CCI is to provide this level of granularity for the individual requirements of a particular security control.

If the security control is decomposed into a single, actionable statement, the process of comparing security controls from one IA policy documents to another is simplified. This process may also identify specific differences between related controls in different source policies. Understanding the differences in source policies enables more complete and accurate compliance reporting to multiple standards and policies for organizations tasked with securing IT systems.

NOTE: The following example is used to point out potential differences in specific IA controls from separate policy documents. It is not intended to make any judgment of the completeness or correctness of one versus the other.

NIST SP 800-53 v3: IA-5(1)

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created;

(c) Encrypts passwords in storage and in transmission;

(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and

(e) Prohibits password reuse for [Assignment: organization-defined number] generations.

DoDI 8500.2: IAIA-1

DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.

Table 1 summarizes the password requirements from both source document IA controls.

Control Requirement	NIST SP 800-53 v3 IA-5 (1)	DoDI 8500.2 IAIA-1
Enforce Password Complexity.	X	X
Enforce number of changed characters during password changes.	X	X
Enforce encryption of passwords in storage and transmission.	X	X
Enforce password minimum and maximum lifetime restrictions.	X	X
Enforce restriction on password reuse.	X	X
Protects authenticators commensurate with the classification or sensitivity of the information accessed.		X
Require in-person registration to receive user ID and password assignment.		X
Remove or change all factory set, default, or standard user IDs and passwords.		X
Require passwords not be shared, embedded in access scripts, or stored on function keys.		X

Table 1. Password Requirements

In the preceding example, both IA Controls are providing guidance to cover information systems that are utilizing logon IDs and passwords, but the lists are not the same. There is substantial overlap, but there are items from the DoDI 8500.2 IAIA-1 that are not included in NIST SP 800-53 IA-5 (1). The NIST SP 800-53 control is divided into 5 requirement items, while the DoDI 8500.2 has a single combined requirement paragraph. This difference in scope and granularity of the controls makes meeting the requirements difficult for the security staff tasked with their implementation.

2.2.2 Decomposition of Source Policy Documents

The CCI List provides a common name and definition that refers to an IA practice. Table 2 shows how the two controls from the previous section are made easier to understand utilizing CCIs, which decompose the source requirements into discrete, actionable, and measurable statements.

CCI	Definition	Reference
CCI-000205	The organization enforces minimum password length.	800-53: IA-5 (1) (a) 8500.2: IAIA-1
CCI-000191	The organization enforces password complexity by the number of special characters used.	800-53: IA-5 (1) (a) 8500.2: IAIA-1
CCI-000192	The organization enforces password complexity by the number of upper case characters used.	800-53: IA-5 (1) (a) 8500.2: IAIA-1
CCI-000193	The organization enforces password complexity by the number of lower case characters used.	800-53: IA-5 (1) (a) 8500.2: IAIA-1
CCI-000194	The organization enforces password complexity by the number of numeric characters used.	800-53: IA-5 (1) (a) 8500.2: IAIA-1
CCI-000195	The organization enforces the number of characters that are changed when passwords are changed.	800-53: IA-5 (1) (b) 8500.2: IAIA-1
CCI-000196	The organization enforces password encryption for storage.	800-53: IA-5 (1) (c) 8500.2: IAIA-1
CCI-000197	The organization enforces password encryption for transmission.	800-53: IA-5 (1) (c) 8500.2: IAIA-1
CCI-000198	The organization enforces minimum lifetime restrictions.	800-53: IA-5 (1) (d) 8500.2: IAIA-1
CCI-000199	The organization enforces maximum lifetime restrictions.	800-53: IA-5 (1) (d) 8500.2: IAIA-1
CCI-000200	The organization prohibits password reuse for the organization-defined number of generations.	800-53: IA-5 (1) (e) 8500.2: IAIA-1
CCI-000201	The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.	800-53: IA-5 (6) 8500.2: IAIA-1
CCI-000188	The organization requires that the registration process to receive an organizationally defined type of authenticator, to be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	800-53: IA-5 (3) 8500.2: IAIA-1
CCI-000178	The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation.	800-53: IA-5 e 8500.2: IAIA-1
CCI-000202	The organization ensures unencrypted passwords are not embedded in access scripts.	800-53: IA-5 (7) 8500.2: IAIA-1
CCI-000203	The organization ensures unencrypted passwords are not embedded in function keys.	800-53: IA-5 (7) 8500.2: IAIA-1

Table 2. CCIs Covering 800-53: IA-5 (1) and DoDI 8500.2: IAIA-1

The example in Table 2 shows that a CCI is created to capture the specific requirement from an IA Control from the source documents, in this case the NIST SP 800-53 and the DoDI 8500.2. When the two IA Controls from the source documents have requirements that appear to be the same, one CCI will be created and reference both source policy documents. In the case where

requirements are unique to a particular source, then a CCI would be created for each, and each would reference the applicable source.

The correctness of the CCI to the source policy will need to be validated by the source policy owners to ensure the intent of the original control is being met. It is not the intent of the CCI to change the requirement in any way; but, rather to state it in a more measurable and actionable format.

2.3 CCI Applicability

Many IA controls may be categorized as technical or policy, depending on whether a control specifies that a technical mechanism be configured to comply with a requirement, or that an organization must define a policy that addresses a particular control statement. The CCI Item includes an optional field that distinguishes between these two categories of controls, where such a distinction can be asserted.

IA controls may also be scoped to specific technology areas, such as operating systems, applications, or network infrastructure devices. Currently, CCI does not attempt to address these distinctions. Source policy documents do not consistently define applicability information. The assignment of CCIs to particular technology areas may be accomplished by organizations consuming the CCI List, consistent with their requirements and definitions of technology areas.

3 CCI Use Cases

Three use cases for CCI are described in this section: secure product development, IA compliance reporting, and security guide development.

3.1 Secure Product Development

IT product vendors have an extremely challenging task of designing products that not only perform their intended functions, but are also able to conform to IA security controls. In many cases, the vendor's largest customer bases drive their research and development efforts. If a vendor deals primarily with commercial customers, that vendor would develop solutions for their commercial customer base and support the IA configurations that their commercial customer needs. Although this practice is sound from a business support perspective, it presents a challenge when that vendor attempts to expand into other customer bases, such as with the DoD.

The CCI List can be used to assist the vendor in the research and development of their products. Since the CCI List is a consolidated list of IA Controls, product vendors could use that list to develop capabilities into their products that satisfy all applicable CCI items for their products. This allows the vendor to have a primary source that represents both commercial and DoD requirements from the beginning.

This decomposition of the IA Control, or other IA requirements, will aide in the removal of the ambiguity that exists in the native IA Control or IA requirements. This process will require the authoritative sources for the policy documents, along with the DoD and the rest of the community, to define what CCIs are needed to meet the intent of the IA Control or reference. When this is accomplished, it reduces the amount of interpretation required by vendors currently utilizing the IA Controls or requirements, which leads to consistency across the vendor community. This effort will also give the vendors the ability to answer the question, "When am I done?"

3.2 IA Compliance Reporting

The ability to compile or rollup results for a particular configurations setting, software update, or other security requirement is not possible with the existing SCAP specifications. The CCE is a source of platform specific configuration checks and the CVE are software flaws also specific to a software platform. Consolidating results regarding specific issues is a formidable challenge that will often result in redundant and inconsistent correlations performed by each organization.

The missing piece of the puzzle is the standardized mechanism that will provide organizations with the ability to select a specific requirement and to collect results from the various assessment tools that are utilized within their organizations for compliance assessment and remediation. CCI will serve as the rollup mechanism for CCEs and CVEs, as well as other types of requirements.

For example, if a mapping is created between CCE and CCI, the data necessary to tie high-level requirements to individual configuration checks will exist.

3.2.1 Rollup of Results to CCI

Organizational leadership is concerned in many cases with the big picture. Leadership wants to know if there are issues with requirements in their span of control. A mechanism is needed to compile compliance information at the requirement level. CCI is the focal point for this type of rollup. CCI results rollups can provide the high level of focus on a requirement, while not impacting the ability to drill down to product-specific levels of compliance statistics.

CCI provides the identifier and actionable requirement that, when used in conjunction with SCAP component specifications, provides the capability to simultaneously measure and score compliance with multiple IA or regulatory source policies using a single collection of SCAP compliant IA assessment results. CCIs can provide the ability to consolidate or rollup like requirements for reporting. In the case of CCE, multiple CCEs can be mapped to a single CCI which would provide the ability of reporting compliance for a requirement across multiple CCE platform groups.

The following is an example of the rollup of CCEs to a CCI:

CCI-000205 – Enforces password minimum length requirements.

CCE-2981-9: Windows XP: Password Minimum Length Check

CCE-2240-0: Windows Server 2008: Password Minimum Length Check

CCE-4625-0: Solaris 10: Password Minimum Length Check

For the previous listed CCEs which all address the minimum password length, CCI provides the ability to consolidate statistics for the minimum password length requirement above the level of the CCE platform group. In the case of CCE, by creating a mapping between CCE and CCI, the information needed for this rollup will exist and additional work will not be required.

The inclusion of CCI references within OVAL and OCIL, or mappings between CCI and CCE, or other source information for checking requirements, allows for guidance from multiple sources to mesh to provide the rollup capabilities to the consumers of the guidance.

3.2.2 Rollup of Results to Source Document

Organizations may also be obligated to provide reporting at the level of source documents or source IA controls based on policy or regulatory requirements. Rollup of results in the context of source documents is another use case of CCI.

The CCI List is composed of multiple CCI Items, which are the individual IA practices and references to applicable IA source policy. Each CCI Item can be mapped to many IA source policy references, thereby providing the inherent ability to assist in the correlation of IA practices between multiple IA source policy references.

Since CCI Items are mapped to applicable IA source policy references, IA compliance results are easily correlated between multiple standards when IA requirements are mapped to the CCI Items.

It should be noted that the reporting of compliance against the standard will be dependent on how well the existing CCIs cover the items identified in the source policy document. The CCI will contain a reference to the source policy document and this reference information will

provide data to indicate if the authoritative source has validated that coverage for their document is met with existing CCIs.

It is envisioned that a mapping could be created between CCE and CCI, such that each CCE would map to one or more CCIs. The CCE to CCI mapping provides two beneficial reporting capabilities: compliance result correlation between multiple IA standards and compliance summarization using results from multiple product assessments. This mapping data is not expected to be maintained within either CCE or CCI, but as a separate XML resource.

3.3 Security Guide Development

3.3.1 Sourcing Requirements

CCI provides security guide authors with a consolidated collection of IA requirements to drive the development of IA configuration guides for IT products. The granular nature of CCIs provides high assurance of complete coverage of applicable requirements in the guide development process. Compared with other approaches, such as developing from the source documents directly, or performing a reverse mapping of existing product IA capabilities back to requirements, a CCI-driven approach promises to result in more complete and consistent guidance.

3.3.2 Scoping Requirements

CCI provides the ability to filter requirements asserted to be applicable to organizational policy or technical configuration. This allows for the generation of requirements documents based on the desired scope of the document. Additional levels of filtering can be applied at the organizational level, which can be unique for each organization.

The organizational level of filter granularity could be accomplished by a separate specification that is specific to an organization. Such filtering could be defined for various criteria, including the type of product or its role in the organization. The discussion of this specification and capabilities are beyond the scope of this document, although it is important to note that this additional capability can provide the level of granularity that may be seen as missing from the CCI.

3.3.3 Referencing Requirements

In addition to driving the development of security guidance from source policy down to product specifics, CCI can be used to maintain references back to source policy from security guides.

An example of this concept is the Federal Desktop Core Configuration (FDCC), which is an OMB-mandated security configuration that is expressed using XCCDF checklists that contain the FDCC settings. Currently, there is a “nist_sp80053_controls” Group and a Requires field within each rule that references numerous items. This could be simplified by using a CCE reference (which would provide a transitive link to a CCI via a CCE to CCI mapping), and if a CCE is not available, then the CCI could be used. CCE could then be used as a key to lookup the numerous references back to the policy document, which would be contained in the CCI.

The “Referencing CCI within SCAP documents” section of this document covers implementation details for referencing CCI from within SCAP documents.

3.4 Summary

CCI supports several IA functions performed by IT managers, IT vendors, and IA policy and guidance developers. CCI's uses in SCAP are multi-functional: first as a way to roll-up CCEs for reporting and metrics and as a way to catalog vulnerabilities that are not specific to a product group. When CCEs are mapped to CCIs and CCIs are mapped to IA Controls, CCIs can help determine policy compliance. CCIs can also be used as references in SCAP documents in a manner similar to CVE and CCE. For instance, in the absence of unique IDs for XCCDF rules, CCI is one way to link benchmark rules that do not have CVE or CCE references.

4 Samples

4.1 Good CCI Sample

The following is a good sample of a CCI.

Definition: The organization enforces minimum password length.
Parameter: Number of characters
Type: technical

This CCI fulfills the three CCI criteria: it is discrete, actionable, and measurable. The requirement is clear and does not leave room for interpretation. The parameter represents a number that can be compared in a meaningful, quantitative manner.

4.2 Bad CCI Sample

The following is not a good sample of a CCI.

Definition: Enforce strong passwords.
Parameter: Strength of password
Type: technical

The requirement is not discrete, as enforcing strong passwords typically involves multiple configuration settings. The requirement is not actionable, since it is not clear what constitutes a strong password. The parameter is not measurable, as password strength is not readily quantifiable without further definition.

4.3 Rollup Reporting Sample

IT management is often concerned with understanding the "big picture" of IA requirements compliance. The ability to consolidate or rollup detailed statistics into broader categories is possible with CCI. The following is a sample rollup report that depicts an organization's compliance status for the IA-5 IA Control of NIST SP 800-53. The ability to obtain granular statistics at the actionable level will provide a mechanism for obtaining an accurate picture of the overall compliance with the IA control. The following example report only addresses a portion of the IA-5 requirements.

IA Policy Compliance Report

IA Control: NIST SP 800-53: IA-5					**90% Compliant**
CCI-000205	**Minimum Password Length**				**80% Compliant**
	CCE-2981-9	Win XP	8 pass	2 fail	80% Compliant
	CCE-2240-0	Win 2k8	5 pass	0 fail	100% Compliant
	CCE-4625-0	Sol 10	15 pass	5 fail	75% Compliant
CCI-000198	**Minimum Password Lifetime**				**100% Compliant**
	CCE-2439-8	Win XP	10 pass	0 fail	100% Compliant
	CCE-1861-4	Win 2k8	5 pass	0 fail	100% Compliant
	CCE-4367-9	Sol 10	20 pass	0 fail	100% Compliant

4.4 Security Guide Sample

Security Guides can be created at various levels of granularity from the general operating system perspective to the detailed Windows XP product-specific perspective. The following depicts the general operating systems view and provides a high level presentation of the requirements that are applicable to an operating system:

Operation System Security Requirements

CCI: CCI-000205

CCI Definition: The organization enforces minimum password length.

References: NIST SP 800-53 v3: IA-5 (1) (a)

Discussion: To ensure the protection of passwords, a minimum length needs to be established. Passwords that are too short can be easily compromised.

Check: Consult vendor documentation for the location of the minimum password length setting. Verify this setting has the value of the minimum password length defined by the organization.

Fix: Consult vendor documentation for the location of the minimum password length setting. Configure this setting to have the value of the minimum password length defined by the organization.

CCI: CCI-000198

CCI Definition: The organization enforces minimum password lifetime restrictions.

References: NIST SP 800-53 v3: IA-5 (1) (d)

Discussion: To ensure rapid password changes do not allow users to bypass password reuse requirements, passwords must be enforced to have a minimum lifetime.

Check: Consult vendor documentation for the location of the minimum password age setting. Verify this setting conforms to the minimum password lifetime defined by the organization.

Fix: Consult vendor documentation for the location of the minimum password age setting. Configure this setting to conform to the minimum password lifetime defined by the organization.

5 Referencing CCI within SCAP documents

5.1 XCCDF

When an XCCDF rule is associated with one or more CCIs, the association may be indicated by providing <xccdf:ident> elements within the <Rule> element.

When used for a CCI reference, the <xccdf:ident> element must adhere to the following syntax:

1. The system attribute for the <xccdf:ident> element must be defined using the CCI system identifier "http://iase.disa.mil/cci".
2. The CCI Identifier must be used for the <xccdf:ident> element content.

For example:

```
<Rule id="PasswordLength">
      <title>Minimum Password Length</title>
      …
      <ident system="http://iase.disa.mil/cci">CCI-000205</ident>
      …
</Rule>
```

5.2 OVAL

When an OVAL definition is associated with one or more CCIs, the association may be indicated by providing <oval-def:reference> elements within the definition's <oval-def:metadata> element.

When used for a CCI reference, the <oval-def:reference> element must adhere to the following syntax:

1. The source attribute for the <oval-def:reference> element must be defined using the CCI system identifier "http://iase.disa.mil/cci".
2. The ref_id attribute for the <oval-def:reference> element must contain the CCI Identifier.

For example:

```
<oval-def:definition id="oval:com.example.oval:def:1">
<metadata>
      <reference source="http://iase.disa.mil/cci" ref_id="CCI-000205"/>
      …
</metadata>
…
</oval-def:definition>
```

5.3 OCIL

When an OCIL questionnaire is associated with one or more CCIs, the association may be indicated by providing <ocil:reference> elements within the questionnaire's <ocil:references> element.

When used for a CCI reference, the <ocil:reference> element must adhere to the following syntax:

1. The href attribute for the <ocil:reference> element must be defined using the CCI system identifier "http://iase.disa.mil/cci".
2. The CCI Identifier must be used for the <ocil:reference> element content.

For example:

```
<ocil:questionnaire id="ocil:com.example.ocil:questionnaire:1">
…
<references>
      <reference href="http://iase.disa.mil/cci">CCI-000205</reference>
      …
</references>
…
</ocil:questionnaire>
```