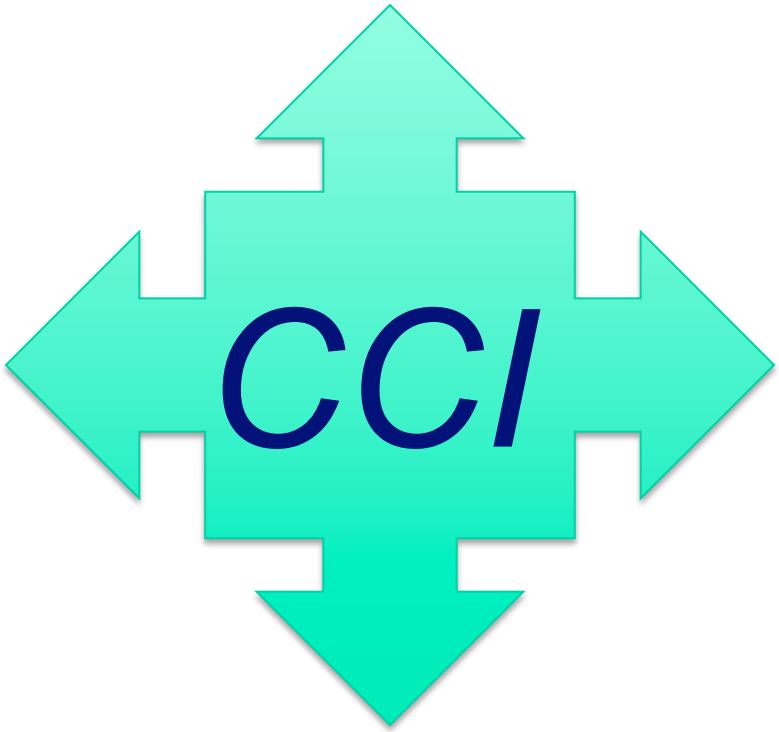
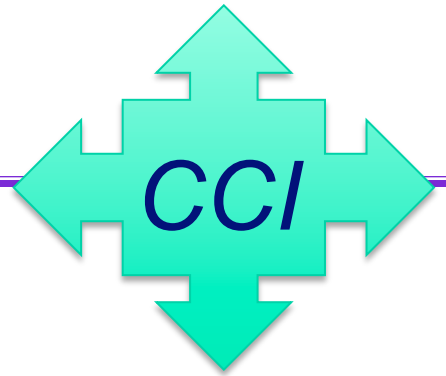
Defense Information Systems Agency
Department of Defense

# Common Control Identifier




DISA Field Security Operations
11 June 2009

# Who is DISA FSO




## Defense Information Systems Agency
## Field Security Operations

**Mission:**

Responsible for enhancing availability and security of the Global Information Grid by ensuring adherence to Information Assurance and NETOPS Policies including **development of guides and procedures**; training of Combatant Commands, subordinate and service components; **implementation of standard IA solutions; formal certification reviews and tracking compliance metrics**.

**Functions:**

**Develop, Implement and Maintain IA Security Guidance and Processes**. **Conduct Full Scope Security Reviews** and Provide Assistance. Provide **Certification and Accreditation Support** and Perform as The **Single Certifying Authority for DISA**. Develop and Implement a NETOPS Evaluation and Certification Program. Perform **Computer Network Defense Service Provider assessments** and **make Certification recommendations. Implement Security Architecture and Information Assurance Tools**. Develop and distribute IA Training Products and Provide IA Training. Develop, Implement and Maintain Vulnerability Management Systems.

# Our perspective?

CCI

Facts (Currently)

> DoD 8500 Series
> IAVMs
> CTO's
> SP 800-53 & CNSS 1253
> CJCSM & more…

DoD Policies

***Analyze Policies***

**Security Requirements**

and

**STIGs**

Facts (Currently)

> 39 STIGs
> 125+ Checklists
> 45,000+ vulnerabilities and requirements in VMS

***Publish Guidance***

***SA***

Secure Systems

***Report Compliance***

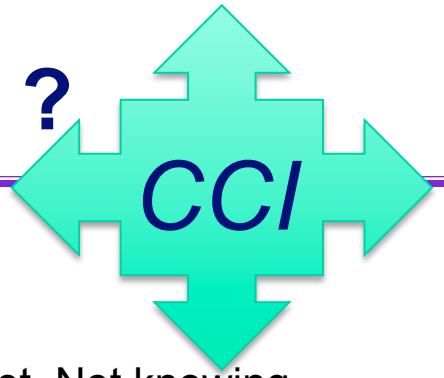
**Compliance Report Card**

Compliance Statistics

Facts (Currently)

> 10,000+ Reviews Annually
> Certification & Accreditations (C&A)
> Security Test & Evaluations (ST&E)
> Enhanced Compliance Visits (ECV)

# What Problems do we see ?




**Secure Product Development**

- Vendors do not know, in detail, what requirements they have to meet. Not knowing "when they are done"
- No master list of all requirements for products

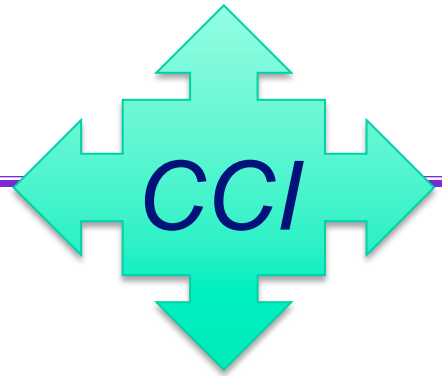
**IA Compliance Reporting**

- Determining compliance statistics
- Inability to be able to validate that all requirements are addressed in current checklists
- Inconsistent reporting of findings and compliance status

**Security Guide Development**

- High Demand for New & Updated Security Guidance
- Duplication of requirements
- Vague / General guidance in DoD IA Controls
- Various interpretations of the requirements
- Requirements not written in a measurable format
- Inconsistency in documents from different sources

# What is a CCI?




**A Common Control Identifier (CCI) is:**

- A decomposition of an IA Control or an IA industry best practice into single, actionable statements
- 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
- Not specific to a product or a Common Platform Enumeration (CPE).

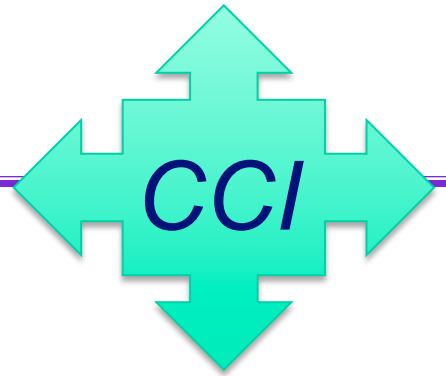
**The CCI List is:**

- A collection of CCI Items, which express common IA practices or controls

**The CCI data specification is:**

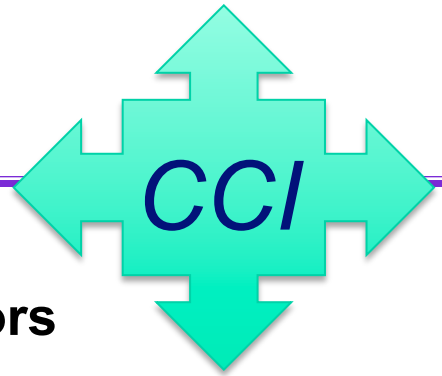
- Proposed to work in conjunction with the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP)

# CCI Use Cases




- **Secure Product Development**
  - Vendors can use CCI to incorporate security requirements into their products as part of the development cycle
  - They *'will know when they are done'*
- **IA Compliance Reporting**
  - CCI allows detailed reporting of compliance to IA Controls. Includes the ability to report partial compliance
- **Security Guide Development**
  - CCI data model in VMS will supports dynamic STIG generation based on asset characteristics
  - Supports Consistent Guide Development from External Sources

# Why is this needed?




- **Without Standards - Checklists are based on Authors Interpretations**
  - How many different answers for number of IA-5 requirements
  - Choice of the checklist you use may impact the security of your IT asset
- **Compliance Reporting to IA Controls**
  - Without a mechanism to identify actions at the lowest actionable level you can't:
    - Accurately report compliance
    - Report partial compliance
    - Identify the specifics of what is not compliant
    - Consistently Report to multiple Source Policy Documents
    - Accurately report compliance across multiple products and technologies

# SAMPLE - IA Control

CCI

IA-5 Authenticator Management (CNSS v4)

CONTROL: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/ refreshing authenticators periodically.

CONTROL Enhancements:

(1) Information Systems utilizing a logon ID and password for user identification and authentication enforce the following:

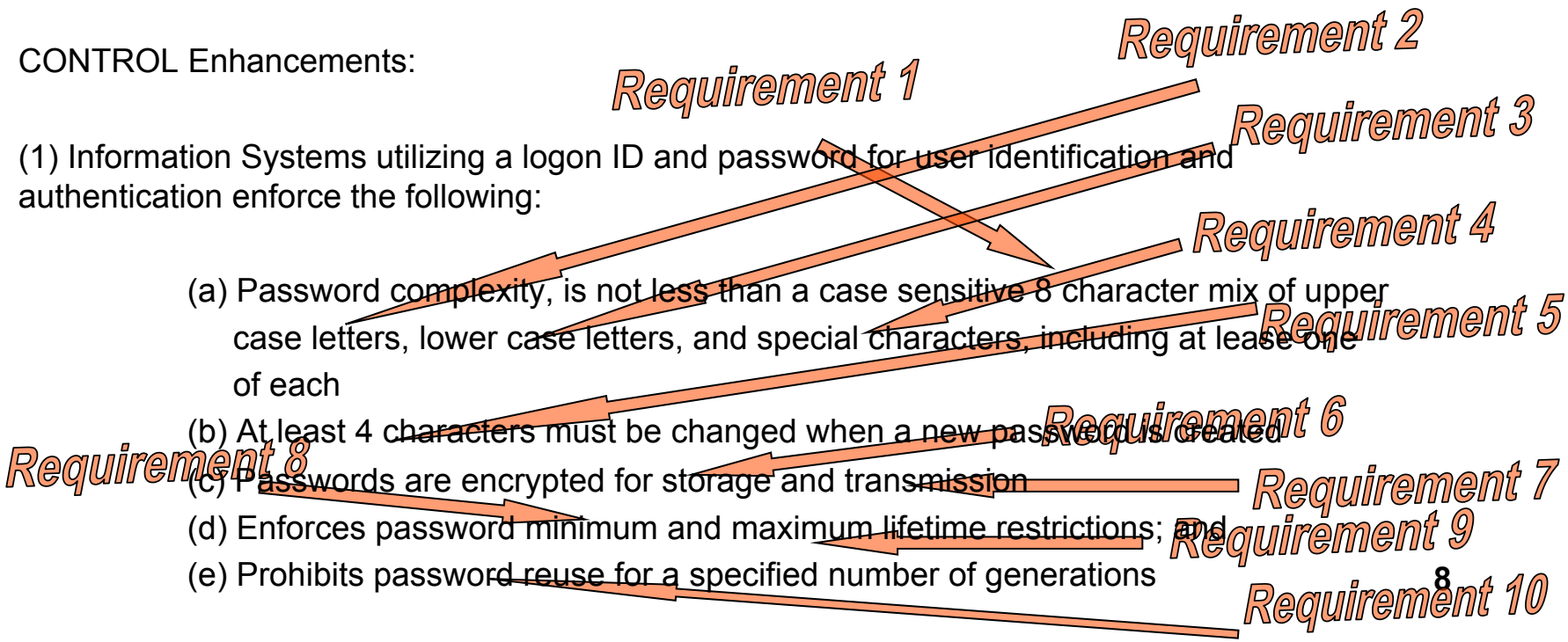
(a) Password complexity, is not less than a case sensitive 8 character mix of upper case letters, lower case letters, and special characters, including at lease one of each

(b) At least 4 characters must be changed when a new password is created

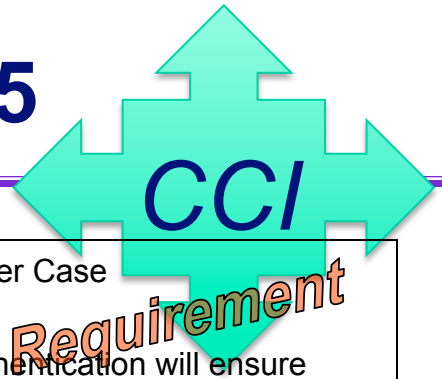
(c) Passwords are encrypted for storage and transmission

(d) Enforces password minimum and maximum lifetime restrictions; and

(e) Prohibits password reuse for a specified number of generations



# CCI Sample – CCIs for IA-5




**CCI-2980:** Authenticator Management - System Enforcement of I&A: Password Complexity Upper Case

**Identification & Authentication : Technical**

**Definition:** Information systems utilizing a logon ID and password for user identification and authentication will ensure password complexity contains at least [Organizationally Defined] number of upper case letters.

**Reference:** CNSS 1253 : IA-5 ; DoD 8500.2 : IAIA-1

**CCI-2990:** Authenticator Management - System Enforcement of I&A: Changing Password

**Identification & Authentication : Technical**

**Definition:** Information systems utilizing a logon ID and password for user identification and authentication will ensure at least [Organizationally Defined] number of characters must be changed when a new password is created.

**Reference:** CNSS 1253 : IA-5 ; DoD 8500.2 : IAIA-1

**CCI-3000:** Authenticator Management - System Enforcement of I&A: Password Encryption Storage

**Identification & Authentication : Technical**

**Definition:** Information systems utilizing a logon ID and password for user identification and authentication will ensure passwords are encrypted for storage.

**Reference:** CNSS 1253 : IA-5 ; DoD 8500.2 : IAIA-1

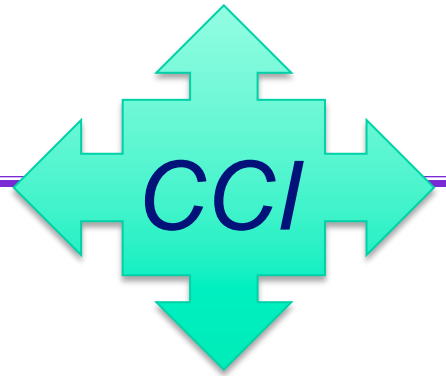
**CCI-3010:** Authenticator Management - System Enforcement of I&A: Password Maximum Lifetime

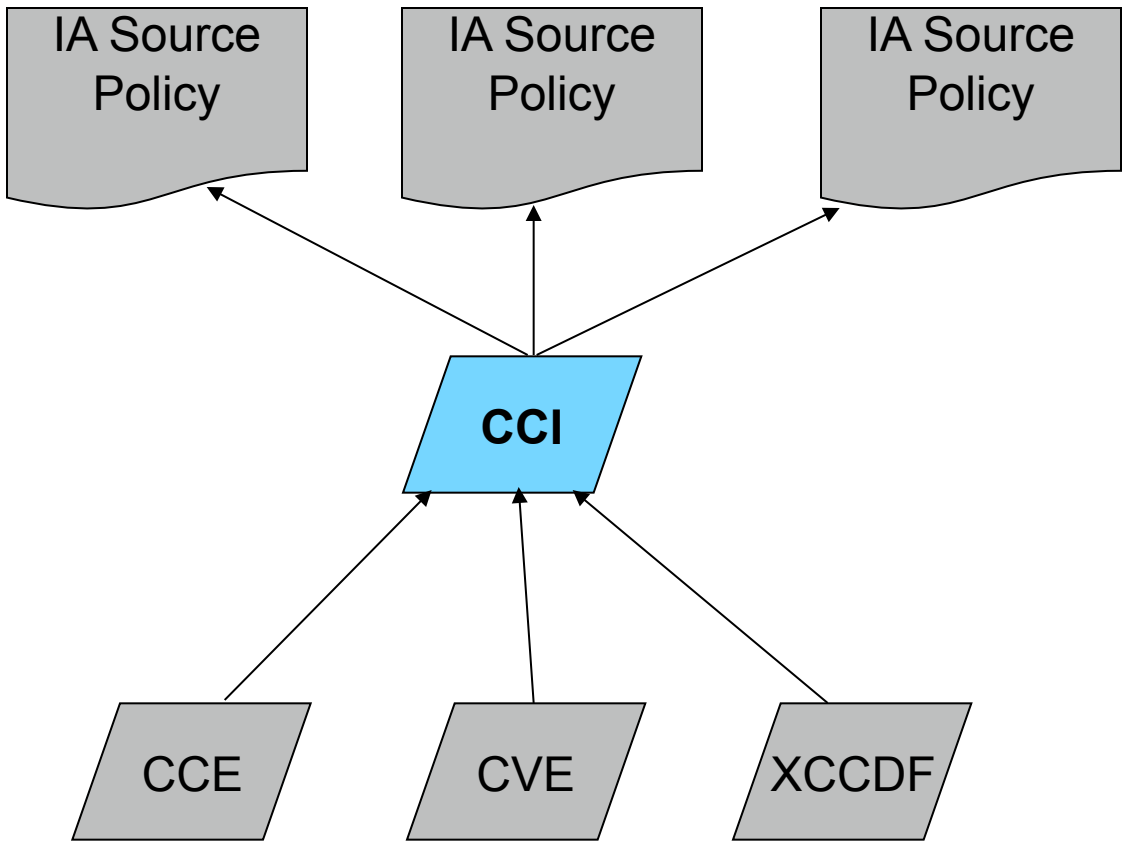
**Identification & Authentication : Technical**

**Definition:** Information systems utilizing a logon ID and password for user identification and authentication will ensure password maximum lifetime restrictions are enforced.

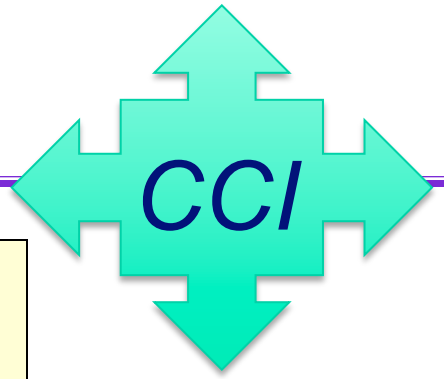
**Reference:** CNSS 1253 : IA-5 ; DoD 8500.2 : IAIA-1

# CCI – SCAP Relationship



# CCI – Data Model




**CCI List**

**CCIItems**

CCIItem
- CCIName
- **CCIItemID**
- CCIPublishedDate
- CCIItemStatus
- CCIContributor
- CCIDescription
- CCINote
- CCIParameter
- CCIDepricatedBy
- CCIApplicability

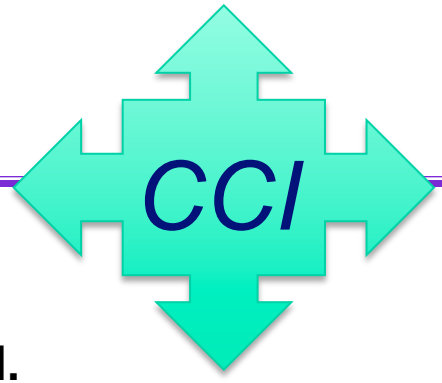
**CCIRefMaps**

CCIRefMap
- **CCIRefMapID**
- **CCIRefMapCCIItemID**
- CCIRefMapRecordIndex
- CCIRefMapGuideline
- CCIRefMapValidatedBy
- CCIRefMapValidatedByDate

**CCIRefs**

CCIRef:
- **CCIRefID**
- CCIRefName
- CCIRefVersion
- CCIRefDate
- CCIRefCreator
- CCIRefContributor
- CCIRefApplicability
- CCIRefLocation
- CCIRefCoverageValidated
- CCIRefCoverageValidatedNote
- CCIRefCoverageValidatedDate

# CCI Business Rules



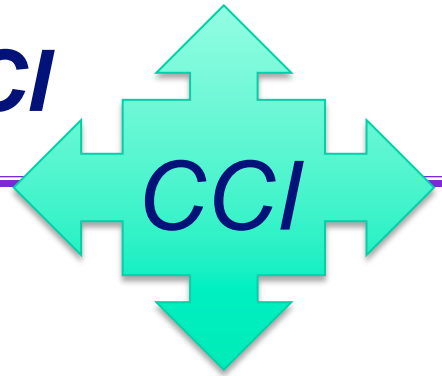

**A CCI must meet certain criteria to be considered a valid CCI.**

- **Single requirement** – The CCI represents a single capability that was decomposed from the source policy document.
- **Actionable** – The CCI represents an action that can be taken against the system or an organizational policy.
- **Measurable** – The action that the CCI is describing will be something that can be determined or measured.

***Example:***

***The organization manages information system authenticators for users and devices by establishing minimum password length requirements.***

# Requirements Guides & CCI



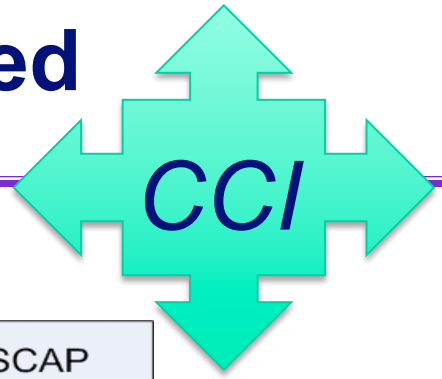

DoD Policy Document
NIST SP 800-53v3

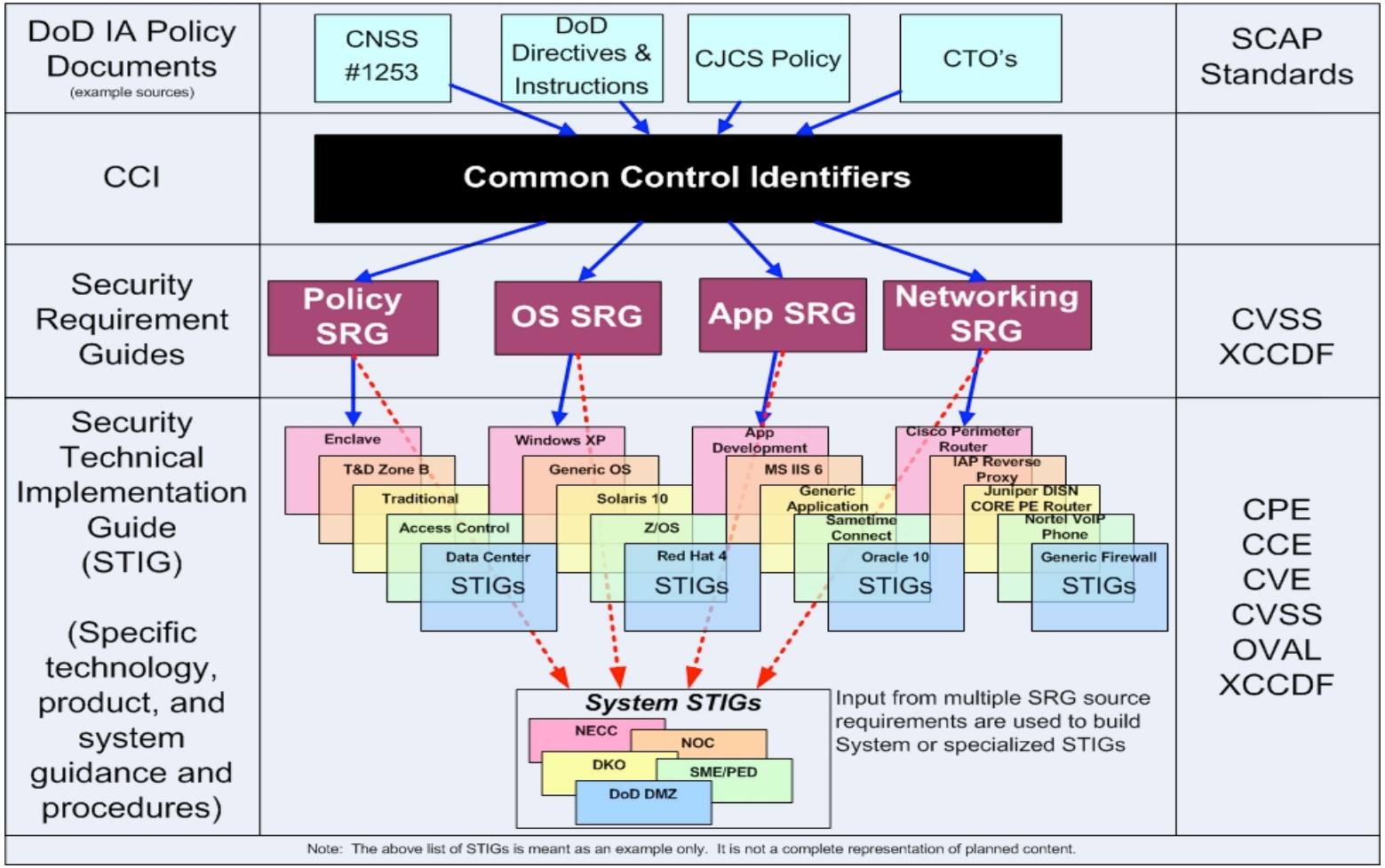
**Common Control Identifier (CCI)**

Security Requirements Guide

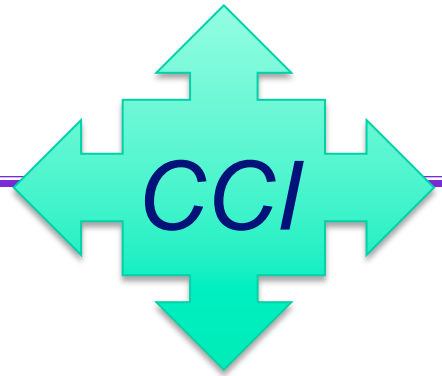
- Applications
- Operating Systems
- Network Infrastructure Devices
- Organizational Policy

# DISA STIG Content / SCAP Enabled



# CCI Way Ahead



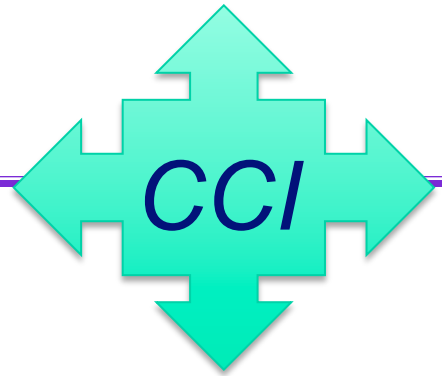

## Current

- DISA FSO will establish the initial CCI List based on NIST SP 800-53 v3.
- The list will then be distributed to the Consensus Group for review and comment.
- Utilize a comment tracking matrix to capture all reported actions to the consensus group that will track the status of the actions through completion.
- An updated matrix will be distributed on a monthly basis in an effort to provide a status of outstanding issues.
- Additions to the CCI List can be submitted to DISA FSO for inclusion to the CCI List. Submissions should be sent to cci@disa.mil.
- It is anticipated that the CCI List will initially be published on a semi-annual basis.
- DISA FSO will work with source policy owners and authoritative sources to validate CCI item and reference mappings. When CCI reference mappings are validated, DISA FSO will update the CCI list with the *CCIRefMapValidatedBy* and *CCIRefMapValidatedByDate* data elements.

## Future

- As the CCI process and specification matures, DISA FSO will consider alternative options for the management and moderation of the CCI List.

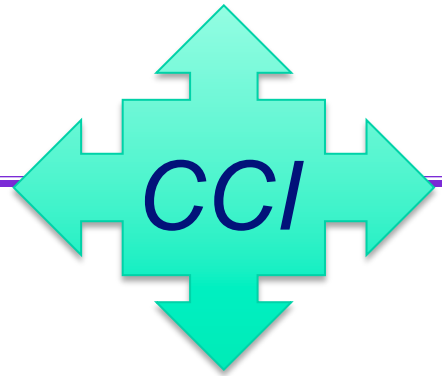
# Windows XP FDCC CCI Analysis




The Windows XP FDCC Content was analyzed:

- To document the mappings of the Checks to the Source Policy Document, NIST SP 800-53
- To provide a sample compliance report for compliance to the following IA Controls:
  - AC-1 thru AC-21
  - AT-1 thru AT-5
  - AU-1 thru AU-12
  - **IA-5** thru IA-6
- To document the mapping of the checks to sample CCIs developed from the same controls mentioned above
- To provide a sample compliance report for compliance to the draft CCIs
- Compare the compliance results with and without CCI

# Windows XP FDCC CCI Analysis




| IA Control | XP CCE's | OS CCI's | Total CCI's | OS Coverage Percentage |
|---|---|---|---|---|
| AC-2 | 0 | 2 | 15 | 0% |
| AC-3 | 145 | 2 | 4 | 100% |
| AC-4 | 0 | 10 | 11 | 0% |
| AC-7 | 3 | 3 | 6 | 100% |
| AC-8 | 0 | 2 | 4 | 0% |
| AC-9 | 0 | 2 | 2 | 0% |
| AC-10 | 0 | 1 | 2 | 0% |
| AC-16 | 0 | 4 | 4 | 0% |
| AC-17 | 0 | 5 | 19 | 0% |
| AU-2 | 9 | 2 | 7 | TBD |
| AU-3 | 0 | 7 | 7 | 0% |
| AU-4 | 9 | 2 | 2 | 100% |
| AU-5 | 0 | 5 | 9 | 0% |
| AU-6 | 0 | 2 | 8 | 0% |
| AU-7 | 0 | 3 | 3 | 0% |
| AU-8 | 0 | 2 | 3 | 0% |
| AU-9 | 0 | 4 | 4 | 0% |
| AU-10 | 0 | 1 | 1 | 0% |
| AU-12 | 0 | 4 | 6 | 0% |
| IA-5 | 6 | 14 | 33 | 43% |
| IA-6 | 0 | 1 | 1 | 0% |

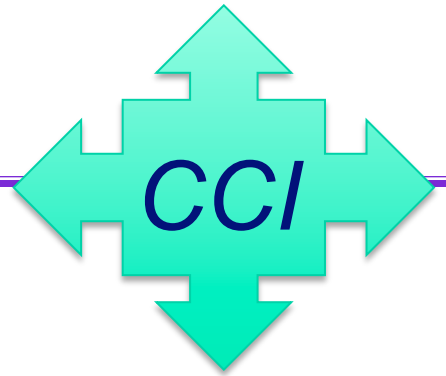
**Count of:**

- XP CCE's
- OS CCIs
- Total CCIs

**That are contained in the XP FDCC**

**(These are estimated numbers at this point, analysis still ongoing)**

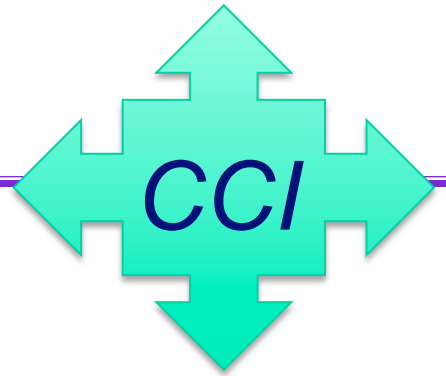
# Windows XP FDCC CCI Analysis




## Details of XP FDCC and SP 800-53v3 Proposed CCIs

| XP FDCC OS Rules for IA-5 | OS CCIs from SP 800-53v3 (June 2009) IA-5 (Proposed) |
|---|---|
| CCE-2994-2 Password History | The organization enforces password reuse conditions. |
| CCE-2920-7 Maximum Password Age | The organization enforces maximum lifetime restrictions. |
| CCE-2439-8 Minimum Password Age | The organization enforces minimum lifetime restrictions. |
| CCE-2981-9 Minimum Password Length | The organization enforces minimum password length. |
| CCE-2889-4 Password Storage Reversable Encryption | The organization enforces password encryption for storage. |
| CCE-2735-9 Password Complexity | The organization enforces password complexity by the number of special characters used. |
| | The organization enforces password complexity by the number of upper case characters used. |
| | The organization enforces password complexity by the number of lower case characters used. |
| | The organization enforces password complexity by the number of numeric characters used. |
| | The information system, for PKI-based authentication validates certificates by constructing a certification path with status information to an accepted trust anchor. |
| | The organization enforces the number of characters that are changed when passwords are changed. |
| | The information system, for PKI-based authentication enforces authorized access to the corresponding private key. |
| | The information system, for PKI-based authentication maps the authenticated identity to the user account. |
| | The organization enforces password encryption for transmission. |

# Windows XP FDCC CCI Analysis

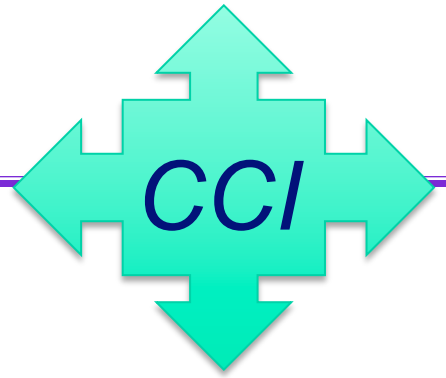



## Results of assessment for proposed 800-53v3 CCIs

| System A IA-5 | | | |
|---|---|---|---|
| **Status** | **CCE ID** | **CCI ID** | **Description** |
| Pass | CCE-2994-2 | CCI-000206 | The organization enforces password reuse conditions. |
| Pass | CCE-2920-7 | CCI-000205 | The organization enforces maximum lifetime restrictions. |
| Pass | CCE-2439-8 | CCI-000204 | The organization enforces minimum lifetime restrictions. |
| Pass | CCE-2981-9 | CCI-000213 | The organization enforces minimum password length. |
| Pass | CCE-2889-4 | CCI-000202 | The organization enforces password encryption for storage. |
| Pass | CCE-2735-9 | CCI-000197 | The organization enforces password complexity by the number of special characters used. |
| Pass | | CCI-000198 | The organization enforces password complexity by the number of upper case characters used. |
| Pass | | CCI-000199 | The organization enforces password complexity by the number of lower case characters used. |
| Pass | | CCI-000200 | The organization enforces password complexity by the number of numeric characters used. |
| Pass | | CCI-000201 | The organization enforces the number of characters that are changed when passwords are changed. |
| Pass | | CCI-000191 | The information system, for PKI-based authentication validates certificates by constructing a certification path with status information to an accepted trust anchor. |
| Pass | | CCI-000192 | The information system, for PKI-based authentication enforces authorized access to the corresponding private key. |
| Pass | | CCI-000193 | The information system, for PKI-based authentication maps the authenticated identity to the user account. |
| Pass | | CCI-000203 | The organization enforces password encryption for transmission. |

| Tests | Checks Passed | % Passed |
|---|---|---|
| CCEs | 6/6 | 100% |
| CCIs | 14/14 | 100% |
| | | |
| FDCC against CCI List | 6/14 | 43% |

# Windows XP FDCC CCI Analysis

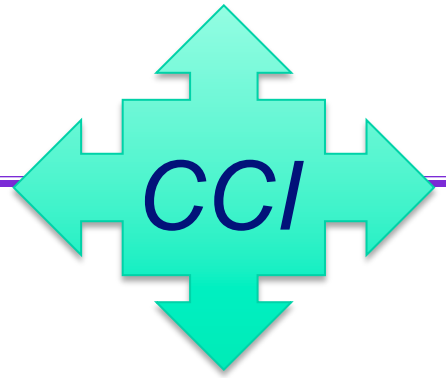



## Results of assessment for proposed 800-53v3 CCIs

| System B IA-5 | | | |
|---|---|---|---|
| **Status** | **CCE ID** | **CCI ID** | **Description** |
| Pass | CCE-2994-2 | CCI-000206 | The organization enforces password reuse conditions. |
| Pass | CCE-2920-7 | CCI-000205 | The organization enforces maximum lifetime restrictions. |
| Pass | CCE-2439-8 | CCI-000204 | The organization enforces minimum lifetime restrictions. |
| Pass | CCE-2981-9 | CCI-000202 | The organization enforces minimum password length. |
| Pass | CCE-2889-4 | CCI-000213 | The organization enforces password encryption for storage. |
| Pass | CCE-2735-9 | CCI-000197 | The organization enforces password complexity by the number of special characters used. |
| Pass | | CCI-000198 | The organization enforces password complexity by the number of upper case characters used. |
| Pass | | CCI-000199 | The organization enforces password complexity by the number of lower case characters used. |
| Pass | | CCI-000200 | The organization enforces password complexity by the number of numeric characters used. |
| Pass | | CCI-000201 | The organization enforces the number of characters that are changed when passwords are changed. |
| Pass | | CCI-000191 | The information system, for PKI-based authentication validates certificates by constructing a certification path with status information to an accepted trust anchor. |
| Pass | | CCI-000192 | The information system, for PKI-based authentication enforces authorized access to the corresponding private key. |
| Pass | | CCI-000193 | The information system, for PKI-based authentication maps the authenticated identity to the user account. |
| Fail | | CCI-000203 | The organization enforces password encryption for transmission. |

| Tests | Checks Passed | % Passed |
|---|---|---|
| CCEs | 6/6 | 100% |
| CCIs | 13/14 | 93% |
| | | |
| FDCC against CCI List | 6/14 | 43% |

# Windows XP FDCC CCI Analysis

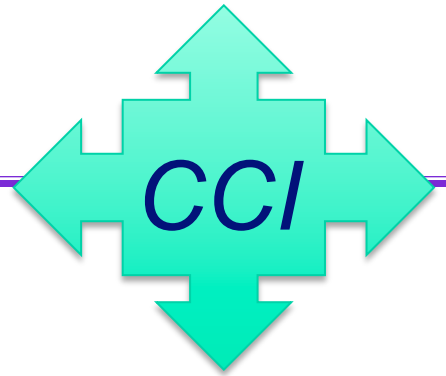



## Results of assessment for proposed 800-53v3 CCIs

| System C IA-5 | | | |
|---|---|---|---|
| **Status** | **CCE ID** | **CCI ID** | **Description** |
| Fail | CCE-2994-2 | CCI-000206 | The organization enforces password reuse conditions. |
| Pass | CCE-2920-7 | CCI-000205 | The organization enforces maximum lifetime restrictions. |
| Pass | CCE-2439-8 | CCI-000204 | The organization enforces minimum lifetime restrictions. |
| Pass | CCE-2981-9 | CCI-000213 | The organization enforces minimum password length. |
| Pass | CCE-2889-4 | CCI-000202 | The organization enforces password encryption for storage. |
| Pass | CCE-2735-9 | CCI-000197 | The organization enforces password complexity by the number of special characters used. |
| Fail | | CCI-000198 | The organization enforces password complexity by the number of upper case characters used. |
| Fail | | CCI-000199 | The organization enforces password complexity by the number of lower case characters used. |
| Fail | | CCI-000200 | The organization enforces password complexity by the number of numeric characters used. |
| Fail | | CCI-000201 | The organization enforces the number of characters that are changed when passwords are changed. |
| Fail | | CCI-000191 | The information system, for PKI-based authentication validates certificates by constructing a certification path with status information to an accepted trust anchor. |
| Fail | | CCI-000192 | The information system, for PKI-based authentication enforces authorized access to the corresponding private key. |
| Fail | | CCI-000193 | The information system, for PKI-based authentication maps the authenticated identity to the user account. |
| Fail | | CCI-000203 | The organization enforces password encryption for transmission. |

| Tests | Checks Passed | % Passed |
|---|---|---|
| CCEs | 5/6 | 83% |
| CCIs | 5/14 | 36% |
| | | |
| FDCC against CCI List | 5/14 | 36% |

# Windows XP FDCC CCI Analysis

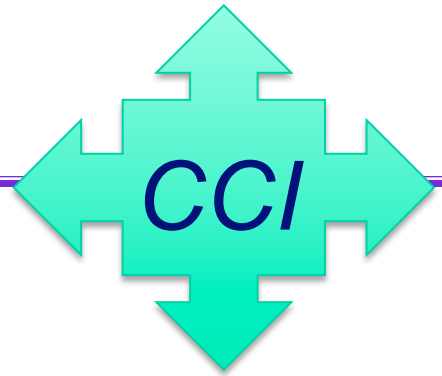



## Results of assessment for proposed 800-53v3 CCIs

| System D IA-5 | | | |
|---|---|---|---|
| **Status** | **CCE ID** | **CCI ID** | **Description** |
| Fail | CCE-2994-2 | CCI-000206 | The organization enforces password reuse conditions. |
| Fail | CCE-2920-7 | CCI-000205 | The organization enforces maximum lifetime restrictions. |
| Fail | CCE-2439-8 | CCI-000204 | The organization enforces minimum lifetime restrictions. |
| Fail | CCE-2981-9 | CCI-000202 | The organization enforces minimum password length. |
| Fail | CCE-2889-4 | CCI-000197 | The organization enforces password encryption for storage. |
| Fail | CCE-2735-9 | CCI-000213 | The organization enforces password complexity by the number of special characters used. |
| Pass | | CCI-000198 | The organization enforces password complexity by the number of upper case characters used. |
| Pass | | CCI-000199 | The organization enforces password complexity by the number of lower case characters used. |
| Pass | | CCI-000200 | The organization enforces password complexity by the number of numeric characters used. |
| Pass | | CCI-000201 | The organization enforces the number of characters that are changed when passwords are changed. |
| Pass | | CCI-000191 | The information system, for PKI-based authentication validates certificates by constructing a certification path with status information to an accepted trust anchor. |
| Pass | | CCI-000192 | The information system, for PKI-based authentication enforces authorized access to the corresponding private key. |
| Pass | | CCI-000193 | The information system, for PKI-based authentication maps the authenticated identity to the user account. |
| Pass | | CCI-000203 | The organization enforces password encryption for transmission. |

| Tests | Checks Passed | % Passed |
|---|---|---|
| CCEs | 0/6 | 0% |
| CCIs | 8/14 | 57% |
| | | |
| FDCC against CCI List | 0/14 | 0% |

# Windows XP FDCC CCI Analysis

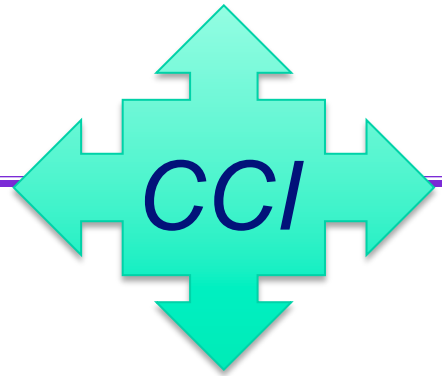



## Compliance status based utilizing CCIs

| Summary | XP FDCC Results | | | | | | |
|---|---|---|---|---|---|---|---|
| System | IA Control | Status | Checks Passed | Compliance Based on XP FDCC | Checks Passed | Status | Compliance Based on SP 800-53v3 |
| System A | IA-5 | Pass | 6 of 6 | 100% | 14 of 14 | Pass | 100% |
| System B | IA-5 | Pass | 6 of 6 | 100% | 13 of 14 | Fail | 93% |
| System C | IA-5 | Fail | 5 of 6 | 83% | 5 of 14 | Fail | 36% |
| System D | IA-5 | Fail | 0 of 6 | 0% | 8 of 14 | Fail | 57% |

- **System A – Passed**
- **System B – Passed/Failed - compliant based on CCE, non compliant based on CCIs**
- **System C – Failed - non compliant based on CCE or CCI, but CCI results indicate a larger degree of non-compliance**
- **System D – Failed - non compliant based on CCE or CCI, but CCI results indicate a higher degree of compliance than CCE.**

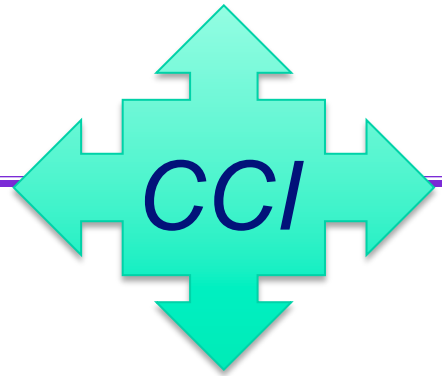
# Windows XP FDCC
# CCI Analysis




## Summary of Analysis

- CCI enables factual representation of compliance results
- CCI helps scope content development and completeness

# CCI Contact Info




http://iase.disa.mil/cci

CCI questions or support

cci@disa.mil