



**Centers for Medicare & Medicaid Services
Information Security and Privacy Group**

CMS InSpec Profile Lifecycle Standard Operating Procedure

Version 1.0

July 2, 2019

This document was prepared for authorized distribution only.
It has not been approved for public release.

Record of Changes

Version	Date	Author / Owner	Description of Change	CR #
1.0	7/2/2019	MITRE	Initial Full Version	

CR: Change Request

Executive Summary

CMS Programs have adopted Agile and DevOps software development methodologies to enable the continuous integration and continuous delivery of their business solutions.

An underlying goal of DevSecOps (i.e., building security into DevOps) is preventing vulnerable applications from reaching production, Sprint to Sprint. Faster deployments that are also part of DevOps, while appealing, can also lead to the deployments of vulnerable applications, leading to higher risk of unauthorized access to CMS data. For the ISSO, it is a tremendous challenge to track changes and weigh security at the end of each Sprint. For the developer, it is also a challenge to receive timely, concise security defect information each time they commit and build during a Sprint. The ISSO and developer need to be able to make an informed decision at the end of each Sprint to recommend a “security go-live,” having the confidence to know that the application about to be deployed is secure. To do this, they need timely security data.

To perform least functionality, patching, and configuration setting checks against the underlying infrastructure of cloud, network, operating system, container, database, application, and web server technologies supporting an application, CMS has adopted InSpec¹, an open-source testing framework that can be used by a developer on their laptop in a sandbox environment, from a system administrator’s management server, or incorporated into the existing testing harness of a DevOps pipeline’s orchestration server.

InSpec relies on testing content in the form of InSpec “profiles” to perform validation. An initial library of CMS-approved profiles is currently available on <https://github.cms.gov> and <https://github.com/mitre>. The current library (Appendix A) is expected to grow as CMS adopts different technologies to support CMS applications.

This document provides standard operating procedures for the lifecycle of InSpec profiles for CMS use. The scope is from proposal, to approval to develop, through development, to publishing for use, maintenance during use, and finally archiving of older profiles.

¹ <https://www.inspec.io/>

Table of Contents

1. Introduction	1
1.1 Background	1
1.2 Purpose	1
1.3 Audience.....	2
1.4 Document Organization	2
2. Roles and Responsibilities	3
3. New InSpec Profile Development	4
4. Maintenance of InSpec Profiles during Official Use	7
5. Archiving of old InSpec Profiles	9
Appendix A. Current CMS InSpec Profiles (June 2019)	10
Appendix B. CMS ARS 3.1 Overlay Spreadsheet Development Steps.....	14
Acronyms.....	26

List of Figures

Figure 3-1 New InSpec Profile Development Process Flow	4
Figure 4-1 Maintenance of InSpec Profiles during Official Use Process Flow	7
Figure 5-1 Archiving of old InSpec Profiles Process Flow	9
Figure A-1 Current CMS InSpec Profile Library	13

This page is intentionally blank.

1. Introduction

1.1 Background

CMS Programs have adopted Agile and DevOps software development methodologies to enable the continuous integration and continuous delivery of their business solutions.

An underlying goal of DevSecOps (i.e., building security into DevOps) is preventing vulnerable applications from reaching production, Sprint to Sprint. Faster deployments that are also part of DevOps, while appealing, can also lead to the deployments of vulnerable applications, leading to higher risk of unauthorized access to CMS data. For the ISSO, it is a tremendous challenge to track changes and weigh security at the end of each Sprint. For the developer, it is also a challenge to receive timely, concise security defect information each time they commit and build during a Sprint. The ISSO and developer need to be able to make an informed decision at the end of each Sprint to recommend a “security go-live,” having the confidence to know that the application about to be deployed is secure. To do this, they need timely security data.

To perform least functionality, patching, and configuration setting checks against the underlying infrastructure of cloud, network, operating system, container, database, application, and web server technologies supporting an application, CMS has adopted InSpec², an open-source testing framework that can be used by a developer on their laptop in a sandbox environment, from a system administrator’s management server, or incorporated into the existing testing harness of a DevOps pipeline’s orchestration server.

InSpec relies on testing content in the form of InSpec “profiles” to perform validation. An initial library of CMS-approved profiles is currently available on <https://github.cms.gov> and <https://github.com/mitre>. The current library (Appendix A) is expected to grow as CMS adopts different technologies to support CMS applications.

Note: **Baseline** vs. **overlay** profiles – to clarify, the library of CMS-approved profiles uses open-source public-community baselines maintained <https://github.com/mitre>, combined with overlays maintained at <https://github.cms.gov>. Baseline profiles contains tests aligned exactly to the original guidance provided by the supporting guidance document (e.g., DISA STIG, CIS benchmark, or product vendor guidance, etc.). Overlay profiles use the testing logic from the baseline profiles, but tailor the tests to specific requirements. The initial set of CMS overlays tailor to CMS ARS 3.1 policy. Examples include the specific password complexity settings and warning banner statements required for CMS systems.

1.2 Purpose

This document provides standard operating procedures for the lifecycle of InSpec profiles for CMS use. The scope is from proposal, to approval to develop, through development, to publishing for use, maintenance during use, and finally archiving of older profiles.

² <https://www.inspec.io/>

1.3 Audience

All system developers and maintainers (SDMs), CMS Business Owners, CMS ISSOs operating under an Agile/DevOps methodology; and supporting Information Security and Privacy Group (ISPG) Cyber Risk Advisors, Privacy Advisors, CCIC security monitoring team, ACT team, and ISPG front office.

1.4 Document Organization

This document is organized as follows:

Section	Purpose
Section 2: Roles and Responsibilities	Identifies who is assigned to each role identified in this procedure document.
Section 3: New InSpec Profile Development	Details the roles and steps for introduction of new profiles.
Section 4: Maintenance of InSpec Profiles during Official Use	Details the roles and steps for maintenance of existing profiles.
Section 5: Archiving of Old InSpec Profiles	Reviews the roles and steps for archiving of old profiles.
Appendix A	Current CMS InSpec Profile List
Appendix B	CMS ARS 3.1 overlay spreadsheet development steps
Acronym List	Defines the acronyms used in this document

2. Roles and Responsibilities

- **Requestor**
 - Any CMS Business Owner, Developer, Operator, ISSO, CRA, ISPG staff
- **Planning SME**
 - MITRE DevSecOps SME (experienced InSpec profile author)
- **Baseline Author**
 - Digital Infuzion
 - or other CMS developer trained under the MITRE InSpec Developer Training class³
- **Overlay Author**
 - Digital Infuzion
 - or other CMS developer trained under the MITRE InSpec Developer Training class
- **Peer Reviewer(s)**
 - MITRE or Digital Infuzion staff
(different than the authors developing or updating a profile)
- **SME Approver**
 - MITRE DevSecOps SME (experienced InSpec profile author)
- **ISPG Approver**
 - Gregory Jones or alternate ISPG staff

³ https://github.com/mitre/inspec_training_courses/tree/master/InSpec-Developer-Course

3. New InSpec Profile Development

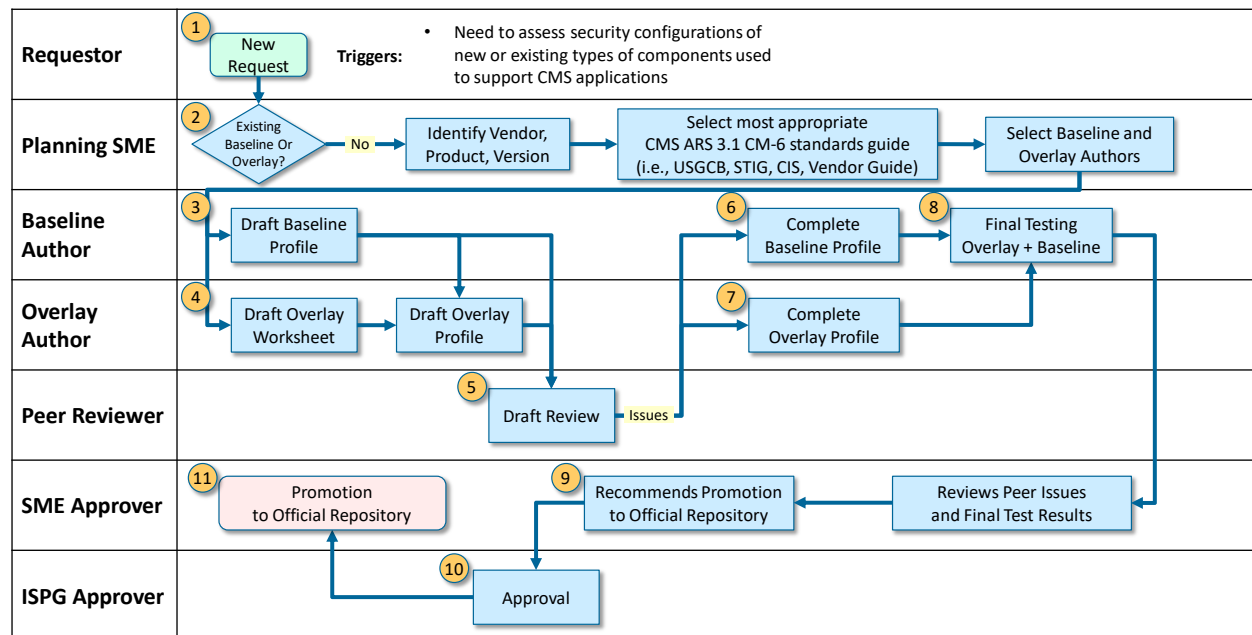


Figure 3-1 New InSpec Profile Development Process Flow

1. A new profile request is submitted to the Planning SME. New profile requests are triggered by the need to assess security configurations of new or existing types of components used to support CMS applications.
2. The **Planning SME**:
 - verifies that no profile currently exists for the requested component type. If a profile or similar profile exists, the process shifts maintenance of current profiles (see section 4)
 - confirms the specific vendor, product, and version of the component type
 - consults CMS ARS 3.1 CM-6 to identify the appropriate applicable security configuration setting standard on which to base the new InSpec profile. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is:

1. USGCB;
2. NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order;
3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
4. National Security Agency (NSA) STIGs;
5. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists.

- selects authors for the baseline InSpec profile and associated CMS ARS 3.1 overlay InSpec profile. (Note: based on resource availability, the overlay author may be the same as the baseline author)
3. The **Baseline profile Author** begins to draft the baseline InSpec profile:
 - creates a repository on <https://github.com/mitre> using the naming convention:
“vendor-product-version-edition[-stig|cis]-baseline”
 - for STIG and CIS guidelines, the author uses https://github.com/mitre/inspec_tools to convert the guideline language into an initial profile to populate the repo, under a branch named development.
 - constructs the /README.md file based on the following template:
https://github.com/mitre/docs-mitre-inspec/blob/master/templates/baseline_readme.md
 - adds the following notice at the top of the /README.md file:

This is a ***Work in Progress***. We will release the final version in the ***MASTER*** Branch
This profile will continue to change until we do a final release
 - populates or updates InSpec describe blocks for all tests within the “controls” directory.
 4. The **Overlay profile Author** begins to draft the CMS ARS 3.1 overlay profile(s):
 - creates 3 planning spreadsheets using the method discussed in Appendix B.
 - creates three repositories on <https://github.cms.gov/ispq> using the naming convention:
“cms-ars3.1-high-vendor-product-version-edition[-stig|cis]-overlay”
“cms-ars3.1-moderate-vendor-product-version-edition[-stig|cis]-overlay”
“cms-ars3.1-low-vendor-product-version-edition[-stig|cis]-overlay”
 - for each repo, populates a controls directory, controls/overlay.rb, inspec.yml, and planning spreadsheet file under a branch named development.
 - constructs the /README.md file based on the following template:
https://github.com/mitre/docs-mitre-inspec/blob/master/templates/overlay_readme.md
 - adds the following notice at the top of the /README.md file:

This is a ***Work in Progress***. We will release the final version in the ***MASTER*** Branch
This profile will continue to change until we do a final release
 - populates the controls/overlay.rb with tailored changes (relative to the baseline profile) based on each overlay’s respective planning spreadsheet.
 5. After initial full draft by the Authors, the **Peer Reviewer**:
 - places a Review.md sheet in each repository based on the following template:
<https://github.com/mitre/docs-mitre-inspec/blob/master/templates/Review.md>
 - reviews both the baseline and overlay profiles covering the categories listed in the Review.md template (peer reviewers may review during draft development)

- enters issues in each repo as needed to note items to be corrected and notes the issue number on the Review.md sheet for the related review category (e.g., syntax check, documentation quality, error handling, etc.)
 - notifies the Authors when they have completed their review
6. The **Baseline Author**:
- resolves the issues noted by the Peer Reviewer
 - updates the completion date column in the Review.md sheet as all issues for a related review category are completed
7. The **Overlay Author**:
- resolves the issues noted by the Peer Reviewer
 - updates the completion date column in the Review.md sheet as all issues for a related review category are completed
 - informs the Baseline Author when they have resolved all issues
8. The **Baseline Author**:
- performs final testing on the overlay used in conjunction with the baseline profile.
 - works with Overlay Author to post and resolve any additional issues found
 - places sample InSpec output in the json format in a samples folder
 - notifies the SME approver for final review
9. The **SME Approver**:
- reviews the Peer review issues and final tests results provided by the Authors
 - recommends to the ISPG Approver promotion of the baseline and overlay profiles to the official repositories
10. The **ISPG Approver**:
- reviews the scope of the original request and recommendations from the SME Approver
 - if all looks in order, provides approval to the SME Approver
11. The **SME Approver** works with the Authors to:
- remove the following notice at the top of the /README.md file:
This is a *Work in Progress***. We will release the final version in the ***MASTER*** Branch
This profile will continue to change until we do a final release**
 - promote from the development branch to the master branch of the repositories

4. Maintenance of InSpec Profiles during Official Use

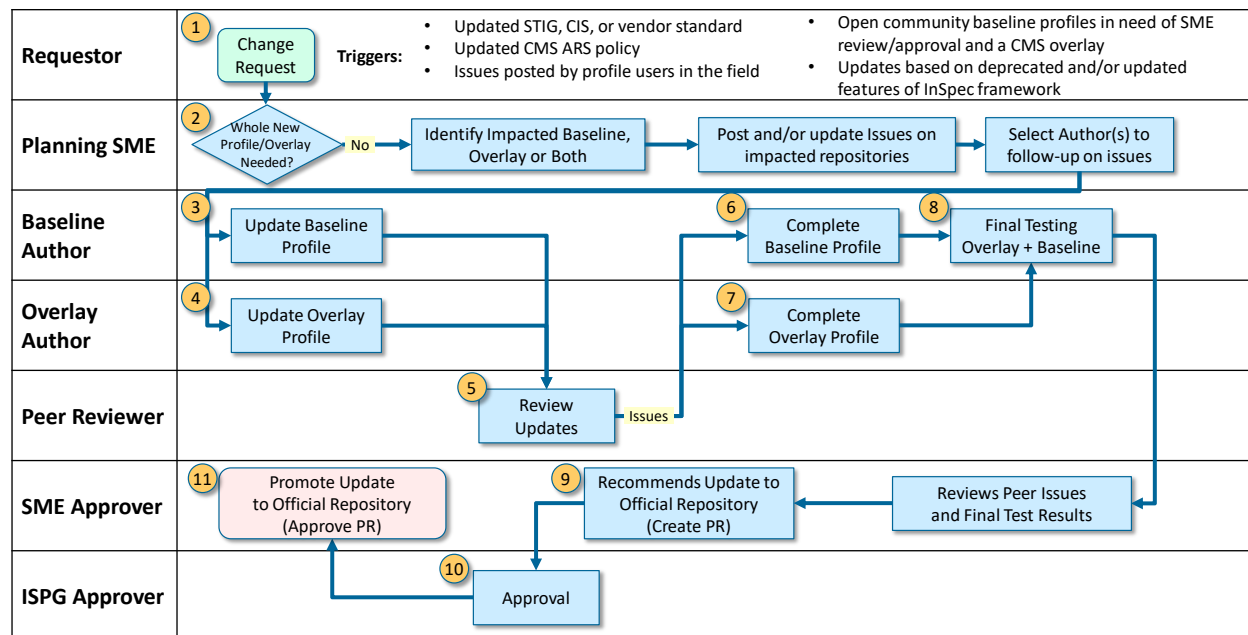


Figure 4-1 Maintenance of InSpec Profiles during Official Use Process Flow

1. A change request is submitted to the Planning SME. Changes requests are triggered by many factors:
 - Updated STIG, CIS, or vendor standard guidance
 - Updated CMS ARS policy
 - Issues posted by profile users in the field
 - Open-source community baseline profiles in need of SME review/approval and a CMS overlay
 - Updates based on deprecated and/or updated features of InSpec framework
2. The **Planning SME**:
 - determines whether a whole new profile or overlay is needed. If so, follows the new profile/overlay process (see section 4)
 - identifies/verifies impacted baseline and/or overlay profiles
 - posts and/or updates issues on impacted repositories
 - selects authors to address the issues on the baseline InSpec profile and/or associated CMS ARS 3.1 overlay InSpec profile.
3. The **Baseline profile Author**:
 - creates a separate issue-branch
 - drafts updates to address the issue(s) for this change request

4. The **Overlay profile Author**:
 - creates a separate issue-branch
 - drafts updates to address the issue(s) for this change request
5. After draft are completed by the Authors, the **Peer Reviewer**:
 - enters issues in each repo as needed to note items to be corrected
 - notifies the Authors when they have completed their review
6. The **Baseline Author**:
 - resolves the issues noted by the Peer Reviewer
7. The **Overlay Author**:
 - resolves the issues noted by the Peer Reviewer
8. The **Baseline Author**:
 - performs final testing on the overlay used in conjunction with the baseline profile.
 - works with Overlay Author to post and resolve any additional issues found
 - places sample InSpec output in the json format in a samples folder
 - notifies the SME approver for final review
9. The **SME Approver**:
 - reviews the Peer review issues and final tests results provided by the Authors
 - recommends to the ISPG Approver update of the baseline and/or overlay profiles to the official repositories (by creating a Pull Request)
10. The **ISPG Approver**:
 - reviews the scope of the original request and recommendations from the SME Approver
 - if all looks in order, provides approval to the SME Approver
11. The **SME Approver** works with the Authors to:
 - promote from the change request branch to the master branch of the repositories

5. Archiving of old InSpec Profiles

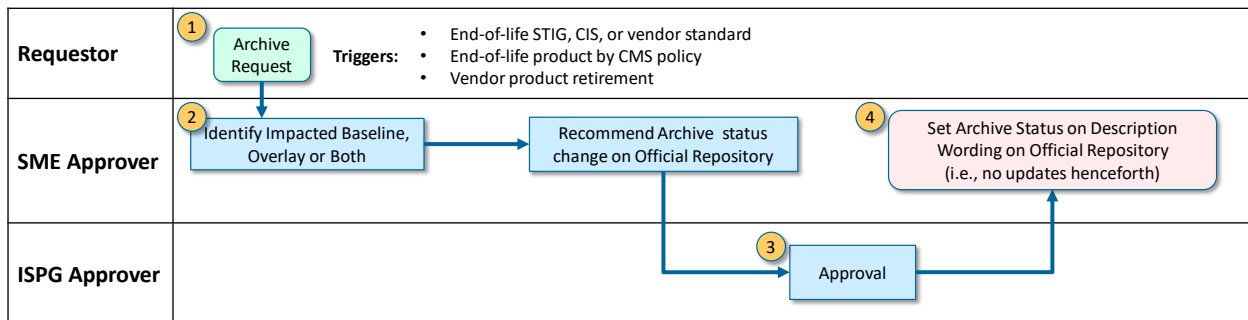


Figure 5-1 Archiving of old InSpec Profiles Process Flow

1. An archive request is submitted to the Planning SME. Archive requests are triggered by many factors:
 - End-of-life STIG, CIS, or vendor standard
 - End-of-life product by CMS policy
 - Vendor product retirement
2. The **SME Approver**:
 - identifies/verifies impacted baseline and/or overlay profiles
 - recommends to the ISPG Approver a change to archive status for the impacted baseline and/or overlay profiles
3. The **ISPG Approver**:
 - reviews the scope of the original request and recommendations from the SME Approver
 - if all looks in order, provides approval to the SME Approver
4. The **SME Approver** works with the Authors to:
 - add the following notice at the top of the /README.md file:

```
### This is an ***Archived***, for legacy component security testing.
### No additional changes will be made to this profile.
```

Appendix A. Current CMS InSpec Profiles (June 2019)

Profile Type	Component Type	Profile Name	Github Repository URL
Baseline	Operating System	RedHat 6 STIG Baseline	https://github.com/mitre/red-hat-enterprise-linux-6-stig-baseline
CMS Overlay	Operating System	CMS ARS 3.1 Moderate Redhat 6 STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-red-hat-enterprise-linux-6-stig-overlay
Baseline	Operating System	Redhat 7 STIG Baseline	https://github.cms.gov/ISPG/inspec-profile-disa_stig-el7
CMS Overlay	Operating System	CMS ARS 3.1 Moderate Redhat 7 STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-red-hat-enterprise-linux-7-stig-overlay
Baseline	Operating System/CVE	RedHat CVE Vulnerability Scan Baseline	https://github.cms.gov/ISPG/rhel_cve_vulnerability_scan_baseline
Baseline	Operating System	Microsoft Windows 2012r2 Member Server STIG Baseline	https://github.com/mitre/microsoft-windows-2012r2-memberserver-stig-baseline
CMS Overlay	Operating System	CMS ARS 3.1 High Microsoft Windows 2012r2 Member Server STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-microsoft-windows-2012r2-member-server-stig-overlay
Baseline	Operating System	Docker CE CIS Baseline	https://github.com/mitre/docker-ce-cis-baseline
CMS Overlay	Operating System	CMS ARS 3.1 Moderate Docker CE CIS Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-docker-ce-cis-overlay
Baseline	Application Logic	RSA Archer 6 Security Configuration Guide Baseline	https://github.com/mitre/rsa-archer-6-security-configuration-guide-baseline
CMS Overlay	Application Logic	CMS ARS 3.1 RSA Archer 6 Security Configuration Guide Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-rsa-archer-6-security-configuration-guide-overlay
Baseline	Application Logic	Red Hat Jboss Enterprise Application Server 6.3 STIG Baseline	https://github.com/mitre/red-hat-jboss-eap-6.3-stig-baseline
CMS Overlay	Application Logic	CMS ARS 3.1 Moderate Red Hat Jboss Enterprise Application Server 6.3 STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay

Profile Type	Component Type	Profile Name	Github Repository URL
Baseline	Application Logic	Oracle Java Runtime Environment 7 Unix STIG Baseline	https://github.com/mitre/oracle-java-runtime-environment-7-unix-stig-baseline
CMS Overlay	Application Logic	CMS ARS 3.1 Moderate Oracle Java Runtime Environment 7 Unix STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-oracle-java-runtime-environment-7-unix-stig-overlay
Baseline	Application Logic	Oracle Java Runtime Environment 8 Unix STIG Baseline	https://github.com/mitre/oracle-java-runtime-environment-8-unix-stig-baseline
CMS Overlay	Application Logic	CMS ARS 3.1 Moderate Oracle Java Runtime Environment 8 Unix STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-oracle-java-runtime-environment-8-unix-stig-overlay
Baseline	Web Server	Microsoft IIS 8.5 Server STIG Baseline	https://github.com/mitre/microsoft-iis-8.5-server-stig-baseline
CMS Overlay	Web Server	CMS ARS 3.1 High Microsoft IIS 8.5 Server STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-microsoft-iis-8.5-server-stig-overlay
Baseline	Web Server	Microsoft IIS 8.5 Site STIG Baseline	https://github.com/mitre/microsoft-iis-8.5-site-stig-baseline
CMS Overlay	Web Server	CMS ARS 3.1 High Microsoft IIS 8.5 Site STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-microsoft-iis-8.5-site-stig-overlay
Baseline	Web Server	NGINX Baseline	https://github.com/mitre/nginx-baseline
CMS Overlay	Web Server	CMS ARS 3.1 Moderate NGINX Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-nginx-overlay
Baseline	Cloud Service Provider	AWS CIS Foundations Baseline	https://github.com/mitre/cis-aws-foundations-baseline
CMS Overlay	Cloud Service Provider	CMS ARS 3.1 AWS CIS Foundations Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-cis-aws-foundations-baseline
Baseline	Cloud Service Provider/S3	AWS S3 Baseline	https://github.cms.gov/ISPG/aws-s3-baseline
Baseline	Cloud Service Provider/RDS	AWS RDS Infrastructure CIS Baseline	https://github.com/mitre/aws-rds-infrastructure-cis-baseline

Profile Type	Component Type	Profile Name	Github Repository URL
CMS Overlay	Cloud Service Provider/RDS	CMS ARS 3.1 Moderate AWS RDS Infrastructure CIS Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-aws-rds-infrastructure-cis-overlay
Baseline	Database	Oracle MySQL Enterprise Edition 5.7 CIS Baseline	https://github.com/mitre/oracle-mysql-ee-5.7-cis-baseline
CMS Overlay	Database	CMS ARS 3.1 Moderate Oracle MySQL Enterprise Edition 5.7 CIS Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-oracle-mysql-ee-5.7-cis-overlay
Baseline	Database/RDS	AWS RDS Oracle MySQL Enterprise Edition 5.7 CIS Baseline	https://github.com/mitre/aws-rds-oracle-mysql-ee-5.7-cis-baseline
CMS Overlay	Database/RDS	CMS ARS 3.1 Moderate AWS RDS Oracle MySQL Enterprise Edition 5.7 CIS Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-aws-rds-oracle-mysql-ee-5.7-cis-overlay
Baseline	Database	Crunchy Data PostgreSQL 9.x STIG Baseline	https://github.com/CrunchyData/pgstigcheck-inspec
CMS Overlay	Database	CMS ARS 3.1 Moderate Crunchy Data PostgreSQL 9.x STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-crunchy-data-postgresql-9-stig-overlay
Baseline	Database/RDS	AWS RDS Crunchy Data PostgreSQL 9 STIG Baseline	https://github.com/mitre/aws-rds-crunchy-data-postgresql-9-stig-baseline
CMS Overlay	Database/RDS	CMS ARS 3.1 Moderate AWS RDS Crunchy Data PostgreSQL 9 STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay
Baseline	Database	Microsoft SQL Server 2014 Database STIG Baseline	https://github.com/mitre/microsoft-sql-server-2014-database-stig-baseline
CMS Overlay	Database	CMS ARS 3.1 High Microsoft SQL Server 2014 Database STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-microsoft-sql-server-2014-database-stig-overlay
Baseline	Database	Microsoft SQL Server 2014 Instance STIG Baseline	https://github.com/mitre/microsoft-sql-server-2014-instance-stig-baseline
CMS Overlay	Database	CMS ARS 3.1 High Microsoft SQL Server 2014 Instance STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay
Baseline	Database/RDS	AWS RDS Microsoft SQL 2014 Server STIG Instance Baseline	https://github.com/mitre/aws-rds-microsoft-sql-server-2014-instance-stig-baseline
CMS Overlay	Database/RDS	CMS ARS 3.1 High AWS RDS Microsoft SQL 2014 Server STIG Instance Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-high-aws-rds-microsoft-sql-server-2014-instance-stig-overlay

Profile Type	Component Type	Profile Name	Github Repository URL
Baseline	Database	Oracle Database 12c STIG Baseline	https://github.com/mitre/oracle-database-12c-stig-baseline
CMS Overlay	Database	CMS ARS 3.1 Moderate Oracle Database 12c STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-oracle-database-12c-stig-overlay
Baseline	Database	MongoDB STIG Baseline	https://github.com/mitre/mongodb-enterprise-advanced-3-stig-baseline
CMS Overlay	Database	CMS ARS 3.1 Moderate MongoDB STIG Overlay	https://github.cms.gov/ISPG/cms-ars-3.1-moderate-mongodb-enterprise-advanced-3-stig-overlay

Figure A-2 Current CMS InSpec Profile Library

Appendix B. CMS ARS 3.1 Overlay Spreadsheet Development Steps

B.1 Background

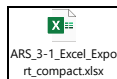
CMS ARS (Acceptable Risk Safeguards) version 3.1 is a selection of NIST SP 800-53 security controls appropriate for CMS applications categorized as High, Moderate, or Low. The control descriptions and implementation standards have been tailored to CMS policy requirements. CMS differs from DISA STIG and CIS benchmarks in key ways:

- CMS is not a DoD organization, therefore many settings differ, such as:
 - Password complexity
 - Authentication failure thresholds and block settings
 - Warning banners
 - Certificate authorities
 - Session timeouts
- DISA STIGs and other standards associate their checks to NIST SP 800-53 security controls. However, not all of these controls are selected within the ARS, or are included, but not mandatory.
- Some settings, such as certificate authorities, vary so widely across CMS that these InSpec tests should be set as manual.

This guide focuses on the highest level of overlay appropriate for CMS, which is based on tailoring to CMS ARS 3.1. The scope does not deal with daughter overlays, which may tailor further based on more specific approved implementations at CMS data centers or for specific CMS applications.

B.2 Resources

- ARS 3.1 Publication (full pdf)
<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html>
- ARS 3-1 Excel Export (full spreadsheet)
<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS-31-Excel-Export.zip>



- ARS 3-1 Excel Export Compact
(allows quick lookup - has only Control family, type, number, name, and associated baseline)

B.3 CMS ARS 3.1 Overlay Naming Convention

Example:

If baseline profile is named:

“microsoft-iis-8.5-server-stig-baseline”

Then a CMS ARS 3.1 overlay for systems categorized as “High” is named:

“**cms-ars-3.1-high-microsoft-iis-8.5-server-stig-overlay**”

B.4 Developing the CMS ARS 3.1 Overlay Planning Spreadsheet

1. Install inspec_tools (https://github.com/mitre/inspec_tools)
2. and InSpec (<http://inspec.io/>)
3. To convert a DISA STIG guideline to a spreadsheet:
 - Download the STIG zip file from <https://iase.disa.mil/stigs/Pages/a-z.aspx>
 - Isolate the xccdf xml file within the zip file
 - `inspec_tools xccdf2inspec -x <stig>-xccdf.xml`
 - `inspec json profile -o profile.json`
 - `inspec_tools inspec2csv -j profile.json -o profile.csv`
4. To convert a CIS (Center for Internet Security) guideline to a spreadsheet:
 - Download the CIS pdf file from <https://www.cisecurity.org/>
 - `inspec_tools pdf2inspec -p <cis>.pdf`
 - `inspec json profile -o profile.json`
 - `inspec_tools inspec2csv -j profile.json -o profile.csv`

5. Import the .csv file into Excel and hide all but these columns:

- Vuln/Test ID, Severity/Impact, Title, Discussion, Check Content/Text, Fix/Remediation Text, CCI/NIST.
- Add a NOTES column:

A	B	F	G	I	J	X	Y	Z
Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES	
V-76679	medium	The IIS 8.5 web server remote authors or content providers must only use secure encrypted logons and connections to upload web server content.	Logging onto a web server remotely using an unencrypted protocol or service when performing updates and maintenance is a major risk. Data, such as user account, is transmitted in plaintext and can easily be compromised. When performing remote administrative tasks, a protocol or service that encrypts the communication channel must be used. An alternative to remote administration of the web server is to perform web server administration locally at the console. Local administration at the console implies physical access to the server.	If web administration is performed at the console, this check is NA. If web administration is performed remotely the following checks will apply: If administration of the server is performed remotely, it will only be performed securely by system administrators. If website administration or web application administration has been delegated, those users will be documented and approved by the ISSO. Remote administration must be in compliance with any requirements contained within the Windows Server STIGs, and any applicable Network STIGs. Remote administration of any kind will be restricted to documented and authorized personnel. All users performing remote administration must be authenticated. All remote sessions will be encrypted and they will utilize FIPS 140-2-approved protocols. FIPS 140-2-approved TLS versions include TLS V1.1 or	Ensure the web server administration is only performed over a secure path.	CCI-001453 The information system implements cryptographic mechanisms to protect the integrity of remote access sessions. NIST SP 800-53 :: AC-17 (2) NIST SP 800-53A :: AC-17 (2).1 NIST SP 800-53 Revision 4 :: AC-17 (2)		

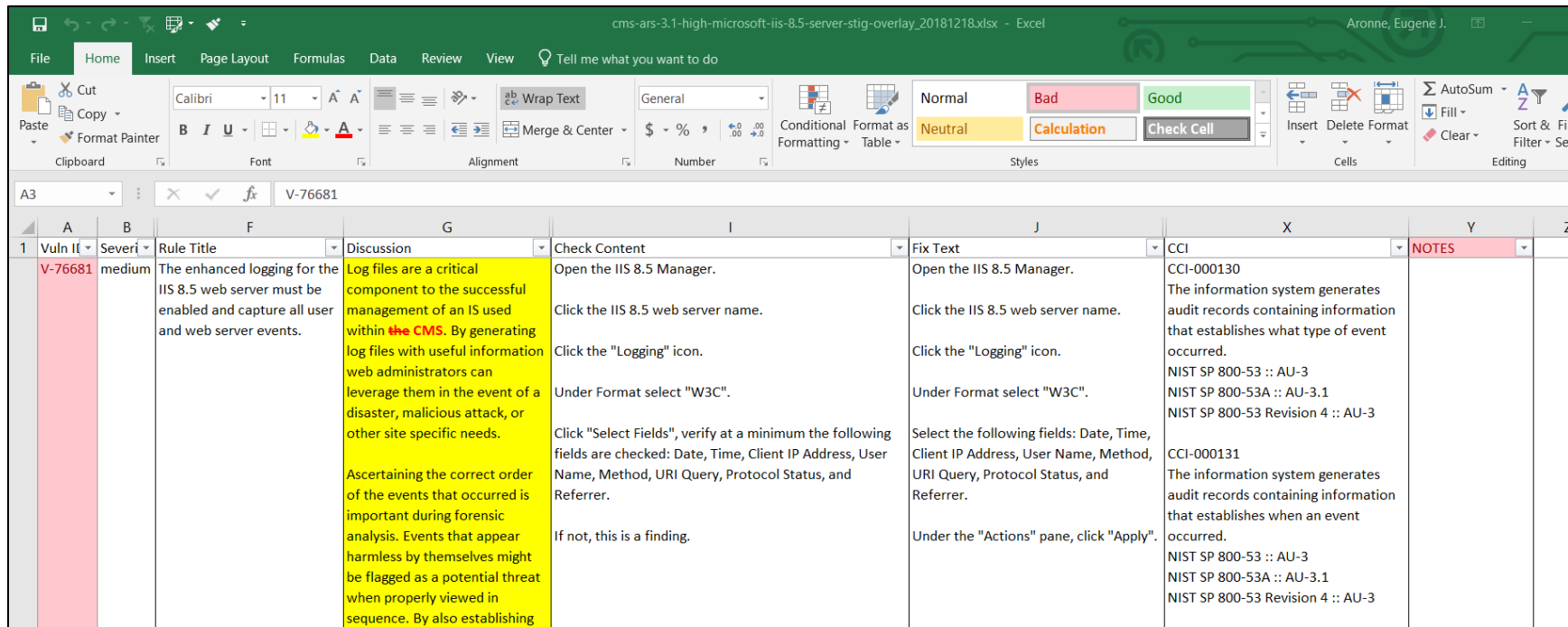
6. Planning spreadsheet conventions - Color first column using **Good (no change)** and **Bad (changed)**:

The image displays two overlapping screenshots of an Excel spreadsheet titled "cms-ars-3.1-high-microsoft-iis-8.5-server-stig-overlay_20181218.xlsx". The top screenshot shows a table with columns A through Z. Column A is highlighted in green, and the cell A23 contains the text "V-76727". The bottom screenshot shows a similar table, but with column A highlighted in pink. Red dashed arrows point from the green highlight in the top screenshot to the pink highlight in the bottom screenshot, indicating a change in the color of the first column. The table structure is as follows:

A	B	F	G	I	J	X	Y	Z
Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES	
V-76679	medium	The IIS 8.5 web server remote authentication providers must secure encrypted connections to server content.	Logging onto a web server	If web administration is performed at the console, this Ensure the web server administration is		CCI-001453		
V-76681	medium	The enhanced logging for the IIS 8.5 web server must be enabled and capture all user and web server events.	Log files are a critical component to the successful management of an IS used within the CMS. By generating log files with useful information web administrators can leverage them in the event of a disaster, malicious attack, or other site specific needs. Ascertain the correct order of the events that occurred is important during forensic analysis. Events that appear harmless by themselves might be flagged as a potential threat when properly viewed in sequence. By also establishing	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Click the "Logging" icon. Under Format select "W3C". Click "Select Fields", verify at a minimum the following fields are checked: Date, Time, Client IP Address, User Name, Method, URI Query, Protocol Status, and Referrer. If not, this is a finding.	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Click the "Logging" icon. Under Format select "W3C". Select the following fields: Date, Time, Client IP Address, User Name, Method, URI Query, Protocol Status, and Referrer. Under the "Actions" pane, click "Apply".	CCI-000130 The information system generates audit records containing information that establishes what type of event occurred. NIST SP 800-53 :: AU-3 NIST SP 800-53A :: AU-3.1 NIST SP 800-53 Revision 4 :: AU-3 CCI-000131 The information system generates audit records containing information that establishes when an event occurred. NIST SP 800-53 :: AU-3 NIST SP 800-53A :: AU-3.1 NIST SP 800-53 Revision 4 :: AU-3		

7. Highlight changes cells yellow, use **red bold text & strike-through** to note change

Use **Notes** column for any other types of changes:



	A	B	F	G	I	J	X	Y
1	Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES
	V-76681	medium	The enhanced logging for the IIS 8.5 web server must be enabled and capture all user and web server events.	Log files are a critical component to the successful management of an IS used within the CMS . By generating log files with useful information web administrators can leverage them in the event of a disaster, malicious attack, or other site specific needs. Ascertaining the correct order of the events that occurred is important during forensic analysis. Events that appear harmless by themselves might be flagged as a potential threat when properly viewed in sequence. By also establishing	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Click the "Logging" icon. Under Format select "W3C". Click "Select Fields", verify at a minimum the following fields are checked: Date, Time, Client IP Address, User Name, Method, URI Query, Protocol Status, and Referrer. If not, this is a finding.	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Click the "Logging" icon. Under Format select "W3C". Select the following fields: Date, Time, Client IP Address, User Name, Method, URI Query, Protocol Status, and Referrer. Under the "Actions" pane, click "Apply".	CCI-000130 The information system generates audit records containing information that establishes what type of event occurred. NIST SP 800-53 :: AU-3 NIST SP 800-53A :: AU-3.1 NIST SP 800-53 Revision 4 :: AU-3 CCI-000131 The information system generates audit records containing information that establishes when an event occurred. NIST SP 800-53 :: AU-3 NIST SP 800-53A :: AU-3.1 NIST SP 800-53 Revision 4 :: AU-3	

8. Non-ARS Security Controls

- If an associated NIST SP 800-53 security control is not listed in the “ARS 3-1 Excel Export Compact” spreadsheet:
- Color the first column to **Bad (changed)**
- Set Severity (Impact) to **“None”**
- Add to NOTES:

(not in ARS)

Add to Overlay:

desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not included in CMS ARS 3.1'

Add to NOTES:
(not in ARS)
Add to Overlay:
desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not included in CMS ARS 3.1'

Set Severity (Impact) to “None”

Color the first column to Bad (changed)

Control Family	Control Type	Control Number	Control Name
380 System and Communications Protection	Mandatory	SC-15(01)	Physical Disconnect
381 System and Communications Protection	Mandatory	SC-17	Public Key Infrastructure Certificates
382 System and Communications Protection	Mandatory	SC-18	Mobile Code
383 System and Communications Protection	Mandatory	SC-19	Voice Over Internet Protocol

Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES
V-76717	None	Java software installed on a production IIS 8.5 web server must be limited to .class files	Mobile code in hosted applications allows the developer to add functionality	Search the system for files with either .java or .jsp extensions.	Remove all files from the web server with both .java and .jsp extensions.	CCI-001166 The information system identifies organization defined unacceptable mobile code.	(not in ARS) Add to Overlay: desc, 'caveat': "Not applicable for this CMS ARS 3.1 overlay, since the related security control is not included in CMS ARS 3.1"

9. Similarly, if developing an overlay for systems categorized as only Moderate or Low:

- Color the first column to **Bad (changed)**
- Set Severity (Impact) to **"None"**
- But add the following to the NOTES:

(not in ARS)

Add to Overlay:

desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not applied to this system categorization in CMS ARS 3.1'

	A	B	C	D	E
1	Control Family	Control Type	Control Number	Control Name	Baseline
380	System and Communications Protection	Mandatory	SC-15(01)	Physical Disconnect	High; Moderate; Low
381	System and Communications Protection	Mandatory	SC-17	Public Key Infrastructure Certificates	High; Moderate
382	System and Communications Protection	Mandatory	SC-18	Mobile Code	High; Moderate
383	System and Communications Protection	Mandatory	SC-19	Voice Over Internet Protocol	High; Moderate
384	System and Communications Protection	Mandatory	SC-20	Secure Name/Address Resolution Service	High; Moderate; Low
385	System and Communications Protection	Mandatory	SC-21	Secure Name/Address Resolution Service	High; Moderate; Low
386	System and Communications Protection	Mandatory	SC-22	Architecture and Provisioning for Name/Address Resolution Service	High; Moderate; Low
387	System and Communications Protection	Mandatory	SC-23	Session Authenticity	High; Moderate
388	System and Communications Protection	Mandatory	SC-24	Fail in Known State	High
389	System and Communications Protection	Mandatory	SC-28	Protection of Information at Rest	High; Moderate

Set Severity (Impact) to **"None"**

Color the first column to **Bad (changed)**

But add the following to **NOTES:**

(not in ARS)

Add to Overlay:

desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not applied to this system categorization in CMS ARS 3.1'

10. Some controls in the ARS are included as something ISSOs may choose but are not required. For these:

- Color the first column to **Bad (changed)**
- Set Severity (Impact) to **"None"**
- But add the following to the NOTES:

(not in ARS)

Add to Overlay:

desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not mandatory in CMS ARS 3.1'

	A	B	C	D	E
1	Control Family	Control Type	Control Number	Control Name	Baseline
380	System and Communications Protection	Mandatory	SC-15(01)	Physical Disconnect	High; Moderate; Low
381	System and Communications Protection	Mandatory	SC-17	Public Key Infrastructure Certificates	High; Moderate
382	System and Communications Protection	Mandatory	SC-18	Mobile Code	High; Moderate
383	System and Communications Protection	Mandatory	SC-19	Voice Over Internet Protocol	High; Moderate
384	System and Communications Protection	Mandatory	SC-20	Secure Name/Address Resolution Service	High; Moderate; Low
385	System and Communications Protection	Mandatory	SC-21	Secure Name/Address Resolution Service	High; Moderate; Low
386	System and Communications Protection	Mandatory	SC-22	Architecture and Provisioning for Name/Address Resolution Service	High; Moderate; Low
387	System and Communications Protection	Mandatory	SC-23	Session Authenticity	High; Moderate
388	System and Communications Protection	Mandatory	SC-24	Fail in Known State	High
389	System and Communications Protection	Mandatory	SC-28	Protection of Information at Rest	High; Moderate
390	System and Communications Protection	Non-Mandatory	SC-28(01)	Non-Mandatory: Cryptographic Protection	
391	System and Communications Protection	Non-Mandatory	SC-32	Non-Mandatory: Information System Partitioning	
392	System and Communications Protection	Mandatory	SC-20	Process Isolation	High; Moderate; Low

Set Severity (Impact) to "None"

Color the first column to Bad (changed)

But add the following to **NOTES:**

(not in ARS)

Add to Overlay:

desc, 'caveat', 'Not applicable for this CMS ARS 3.1 overlay, since the related security control is not mandatory in CMS ARS 3.1'

11. Some InSpec tests just can't be adapted technically. For example, DoD has specific root CAs, but CMS environments vary. Hence, the CMS ARS 3.1 doesn't specify a lists of root certificates to check. In these situations, the test should be coded in InSpec as needing manual review. Add the following to NOTES:

describe "For this CMS ARS 3.1 overlay, this control must be reviewed manually" do

skip "For this CMS ARS 3.1 overlay, this control must be reviewed manually"

end

cms-ars-3.1-high-microsoft-iis-8.5-server-stig-overlay_20181218.xlsx - Excel									
File Home Insert Page Layout Formulas Data Review View Tell me what you want to do									
Y18 describe "For this CMS ARS 3.1 overlay, this control must be reviewed manually" do									
A	B	F	G	I	J	X	Y	Z	
1	Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES	
	V-76715	medium	The IIS 8.5 web server must perform RFC 5280-compliant certification path validation.	This check verifies the server certificate is actually a CMS-issued certificate used by the organization being reviewed. This is used to verify the authenticity of the website to the user. If the certificate is not issued by the CMS or if the certificate has expired, then there is no assurance the use of the certificate is valid. The entire purpose of using a certificate is, therefore,	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Double-click the "Server Certificate" icon. Double-click each certificate and verify the certificate path is to a CMS root CA. If not, this is a finding.	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Double-click the "Server Certificate" icon. Import a valid CMS certificate and remove any non-CMS certificates.	CCI-000185 The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information. NIST SP 800-53 :: IA-5 (2) NIST SP 800-53A :: IA-5 (2).1 NIST SP 800-53 Revision 4 :: IA-5 (2) (a)	describe "For this CMS ARS 3.1 overlay, this control must be reviewed manually" do skip "For this CMS ARS 3.1 overlay, this control must be reviewed manually" end	

Add the following to NOTES:

describe "For this CMS ARS 3.1 overlay, this control must be reviewed manually"

do

skip "For this CMS ARS 3.1 overlay, this control must be reviewed manually"

end

12. "DoD" Search

- Baseline STIGs commonly refer to the DoD or Department of Defense specifically. Search through the baseline content and change accordingly, especially the title, discussion, check and fix text:

cms-ars-3.1-high-microsoft-iis-8.5-server-stig-overlay_20181218.xlsx - Excel

File Home Insert Page Layout Formulas Data Review View Tell me what you want to do

Y18 describe "For this CMS ARS 3.1 overlay, this control must be reviewed manually" do

	A	B	F	G	I	J	
1	Vuln ID	Severity	Rule Title	Discussion	Check Content	Fix Text	CC
	V-76715	medium	The IIS 8.5 web server must perform RFC 5280-compliant certification path validation.	This check verifies the server certificate is actually a CMS -issued certificate used by the organization being reviewed. This is used to verify the authenticity of the website to the user. If the certificate is not issued by the CMS or if the certificate has expired, then there is no assurance the use of the certificate is valid. The entire purpose of using a certificate is, therefore,	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Double-click the "Server Certificate" icon. Double-click each certificate and verify the certificate path is to a CMS root CA. If not, this is a finding.	Open the IIS 8.5 Manager. Click the IIS 8.5 web server name. Double-click the "Server Certificate" icon. Import a valid CMS certificate and remove any non- CMS certificates.	CCI 000 The info authent by cons certific anchor status in NIST SP NIST SP NIST SP (a)

13. Identifying user-defined settings - Sometimes the profiles require the user to identify specific settings. This usually comes from the base profile, but just the same, it's nice to include in the Notes column when this is needed. It helps the overlay author instruct the user in the Readme for the profile.

- Add to the following to NOTES:

User-defined attribute needed to provide the system-specific '<user' account> for this system. See Readme for this profile.

- Or for a simplified version:

User-defined attribute(s) needed. See Readme for this profile.

	A	F	G	I	J	X	Y
1	Vuln ID	Rule Title	Discussion	Check Content	Fix Text	CCI	NOTES
13	V-67383	Database Master Key passwords must not be stored in credentials within the database.	Storage of the Database Master Key password in a database credential allows decryption of sensitive data by privileged users who may not have a need-to-know requirement to access the data.	From the query prompt: SELECT COUNT(credential_id) FROM [master].sys.master_key_passwords If count is not 0, this is a finding.	Use the stored procedure sp_control_dbmasterkey_password to remove any credentials that store Database Master Key passwords. From the query prompt: EXEC SP_CONTROL_DBMASTERKEY_PASSWORD D @db_name = '<database name>', @action = N'drop'	CCI-001199 The information system protects the confidentiality and/or integrity of organization-defined information at rest. NIST SP 800-53 :: SC-28 NIST SP 800-53A :: SC-28.1 NIST SP 800-53 Revision 4 :: SC-28	User-defined attribute needed to provide the system-specific '<user' account> for this system. See Readme for this profile.

Add to the following to **NOTES**:

User-defined attribute needed to provide the system-specific '<user' account> for this system. See Readme for this profile.

Or for a simplified version:

User-defined attribute(s) needed. See Readme for this profile.

14. Check key controls with CMS-specific requirements:

Control Number	Control Name
AC-07	Unsuccessful Logon Attempts
AC-08	System Use Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-12	Session Termination
AU-04	Audit Storage Capacity
AU-05	Response to Audit Processing Failures
AU-05(01)	Audit Storage Capacity
AU-08(01)	Synchronization with Authoritative Time Source
CM-06	Configuration Settings
IA-02(02)	Network Access to Non-Privileged Accounts
IA-04	Identifier Management
IA-05(01)	Password-Based Authentication
SC-08	Transmission Confidentiality and Integrity
SC-10	Network Disconnect
SI-02	Flaw Remediation
SI-03	Malicious Code Protection
SI-06	Security Function Verification
SI-07	Software, Firmware, and Information Integrity
SI-07(01)	Integrity Checks
SI-07(02)	Automated Notifications of Integrity Violations
SI-07(05)	Automated Response to Integrity Violations

Acronyms

Acronym	Definition
ARS	Acceptable Risk Safeguards
CIS	Center for Internet Security
CMS	Centers for Medicare & Medicaid Services
CVE	Common Vulnerabilities and Exposures
DevOps	Development (and) Operations (working together)
DevSecOps	Development, Security, Operations (working together)
DISA	Defense Information Systems Agency
FISMA	Federal Information Security Modernization Act (2014)
ISPG	Information Security and Privacy Group
ISSO	Information System Security Officer
JSON	JavaScript Object Notation
NIST SP	National Institutes of Standards and Technology Special Publication
SME	Subject Matter Expert
STIG	Security Technical Implementation Guide

