Vendor STIG Process

Version 4, Release 1

15 August 2022

Developed by DISA for the DOD

REVISION HISTORY

Date	Section	Revision
10 Aug 2022	3.2	Revised text to reflect a mix of the first 10 requirements.
10 Aug 2022	3.5	Revised bullets to reflect acceptance of the STIG for validation with additional time for revisions/work with the vendor.
10 Aug 2022	4.0, 4.1.6, 4.1.8, 4.1.10, 4.1.11, 4.1.11.1, 4.1.12, 4.1.13, 4.1.14, 4.1.15, 4.1.16, 4.1.17, 5, 5.1	Reworded sentences for clarification.
10 Aug 2022	5.2	Removed reference to RME.
10 Aug 2022	5.3.1, 5.4.1	Removed end sentence for clarification.
10 Aug 2022	6	Removed RME Approval and replaced with DISA AO Approval.
13 Aug 2021	6	Revised bullet to reference Controlled Unclassified Information (CUI).
14 Aug 2020	2.1	Added the request for the vendors time zone.
14 Aug 2020	3.1	The Requirements Cheat Sheet was added for discussion during the Orientation Meeting.
14 Aug 2020	3.2	Clarified that the first 10 requirements should be Applicable-Configurable.
14 Aug 2020	4	Added the Requirements Cheat Sheet to be used alongside the STIG Template when developing STIG content.
14 Aug 2020	4.1.8	Requirements evaluated to be Not Applicable do not require a VulDiscussion.
14 Aug 2020	4.1.14	Requirements evaluated to be Not Applicable no longer require a severity.
14 Aug 2020	5.2	Added a Transition section.
14 Aug 2020	5.3, 5.3.1	Removed DISA RME SME.
19 Feb 2020	4.1.6	Clarified that requirements must not state that a technology is "capable" of doing something but that the technology must be "configured" to do something.
19 Feb 2020	4.1.15	Added guidance on writing a Mitigation statement for an Applicable – Does Not Meet requirement that is fully mitigated by another check or underlying system.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

The Defense Information Systems Agency (DISA) Standards and Analysis Division plays a critical role in enhancing the security posture of the Department of Defense's (DOD) security systems through its Security Technical Implementation Guides (STIGs). The STIGs provide DOD and other federal agencies with operational configuration guidance to harden computer systems and protect cyber infrastructure that might otherwise be vulnerable to a malicious computer attack.

DISA has developed a process through which vendors can request to write a STIG for possible publication.

This Vendor Process contains the following major milestones. "Decision points" indicate when DISA will determine if a vendor continues in the process.

Figure 1-1: Vendor STIG Process Major Milestones

Vendor STIG Intent Form Submission	Planning	Development	Validation	Review and Approval
• Form validation • Sponsor verification • Decision point	• Introductory meeting between vendor and DISA • Decision point	• Vendor orientation • STIG Development Stage 1 (2 weeks) • Stage 2 (+30 days) • Stage 3 (+30 days) • Stage 4 (+30 days) • First Draft STIG completion • Decision point	• DISA review of vendor-provided documents • STIG simulation • DISA feedback to vendor/revisions by vendor • Final Draft STIG completion	• DISA internal review • Editorial review • RME decision briefing • Vendor notification • Public Affairs Office (PAO) approval • STIG publication

To begin the process, the vendor submits the Vendor STIG Intent Form through the DOD Cyber Exchange website at https://public.cyber.mil/stigs/vendor-process. DISA validates the information on the form, notifies the vendor if more information is needed, and determines if the vendor will move on to the Planning stage.

2. PLANNING

2.1 Introductory Meeting

The Planning stage kicks off with an introductory meeting between the vendor and DISA. Prior to the meeting, the vendor provides DISA with the following information:

- Marketing material.
- Product website addresses.
- Product usage in the DOD.
- Vendor meeting participants.
- Time zone.

The success of this meeting depends on participation by the correct individuals. Vendor attendees should not be sales representatives but rather a technical team whose members can answer questions about securing the product in line with DOD standards.

The meeting consists of a 15-minute introduction by DISA covering the STIG development process and overview of requirements and a 15-minute presentation by the vendor. The vendor presentation should consist of:

- A demonstration or explanation of the product.
  - Main functional areas that are accessible and configurable.
  - Functional areas that are National Information Assurance Partnership (NIAP) Protection Profile (PP) tested/approved.
- Justification for the STIG.
- The product's current DOD use cases and density.

2.2 Decision Point

Following the Introductory Meeting, DISA determines the level of need for the proposed STIG and notifies the vendor via email of the decision.

If the decision is to move forward, the vendor enters the Development stage of the process.

3. DEVELOPMENT

3.1 Vendor Orientation

The STIG development process begins with a vendor orientation, which includes a discussion of:

- Vendor resource availability and timeline.
- Security Requirements Guides (SRGs) applicable to the technology.
- Requirements "Cheat Sheet."

If vendor resources are not immediately available for STIG development, the process is pushed six months, at which time the vendor is responsible for contacting DISA to restart the process.

If vendor resources are available and the vendor wishes to continue, the process moves to the next stage of development.

3.2 Stage 1 STIG Development

- DISA provides the vendor with a STIG template based on the applicable SRG. This template contains requirements the STIG must address.
- Within two weeks, the vendor returns the STIG template to DISA with 10 requirements completed. This must be a mix of all statuses: Applicable – Configurable, Applicable – Inherently Meets, Applicable – Does Not Meet, and Not Applicable.
- DISA reviews the requirements and either accepts them and notifies the vendor to move forward with development or asks for updates and resubmission.

3.3 Stage 2 STIG Development

- Within 30 days after the DISA decision to proceed, the vendor submits the STIG as a work in progress to DISA for review.
- DISA reviews the STIG and notifies the vendor to move forward with current development or offers feedback on areas for improvement.

3.4 Stage 3 STIG Development

- Within 60 days after the DISA decision to proceed, the vendor submits the STIG as a work in progress to DISA for review.
- DISA reviews the STIG and notifies the vendor to move forward with current development or offers feedback on areas for improvement.

3.5 Stage 4 STIG Development

- Within 90 days after the DISA decision to proceed, the vendor submits the completed initial draft STIG to DISA for review.
- DISA reviews the STIG and takes one of the following actions:
  - Accepts the STIG.
  - Accepts the STIG with time for development.
  - Rejects the STIG.
  - Rejects the STIG with request for revisions.

4. WRITING THE STIG

The vendor will use the technology-specific STIG template, Vendor STIG Process Guide, and Requirements Cheat Sheet provided at the orientation meeting to develop the STIG content. This includes:

- Requirements Analysis.
  - Vendor populates the Status column of the spreadsheet.
  - Vendor populates the Status Justification column for "Does Not Meet," "Inherently Meets," and "Not Applicable" requirements.
  - Vendor populates the Mitigation column with mitigation information for "Does Not Meet" requirements.
  - Vendor populates the Artifact Description column for "Inherently Meets" requirements.
- Check and Fix Procedure Development.
  - Vendor identifies configurable settings relevant to the requirement.
  - Vendor populates the Check column with the setting requirements and verification instructions.
  - Vendor populates the Fix column with details on how to configure the relevant settings.

The following sections describe in detail the STIG template fields and how they should be completed.

Note: In the spreadsheet, please do not use any enhanced formatting features such as **bold**, *italics*, underline, ~~strikethrough~~, different fonts, or smart (curly) quotes.

4.1 STIG Template Field Descriptions

Fields designated by an asterisk (*) below are prepopulated and should not be changed.

4.1.1 IA Control*

This is a prepopulated reference to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Information Assurance (IA) control from which the requirement is sourced. The STIG developer may wish to read the source material for more information.

4.1.2 CCI*

The Control Correlation Identifier (CCI) enables DOD organizations to trace STIG compliance to IA controls specified by NIST and mandated for federal government agencies.

4.1.3   SRGID*

This is the ID for the SRG requirement. It may also contain identification information for a "parent" SRG document.

4.1.4   STIGID

This will be the identifier of the requirement in the STIG. DISA populates the STIGID during finalization. The vendor will not complete this field.

4.1.5   SRG Requirement*

This is a sentence stating the requirement and is prepopulated from the Technology SRG.

4.1.6   Requirement

This is a STIG-specific requirement that focuses the scope of the SRG requirement on the product for which the STIG is being written.

Adhere to the following standards when writing the requirements:

- Use the word "must" rather than "should".
  - *Correct example:* The [operating system] **must** protect audit information from unauthorized deletion.
  - *Incorrect example:* The [operating system] **should** protect audit information from unauthorized deletion.
- For Applicable-Configurable requirements, replace the generic terminology from the SRG requirement (such as application, operating system, etc.) with the specific name of the technology.
- Use the wording "must be configured to" instead of "must be capable of" or "must have the capability to".
  - *Correct example:* The [technology name] **must be configured to** prevent browsers from saving user credentials.
  - *Incorrect example:* The [technology name] **must be capable of** preventing browsers from saving user credentials.

4.1.7   SRG VulDiscussion*

The SRG vulnerability discussion describes the risk of not complying with the requirement. This is prepopulated from the SRG.

4.1.8 VulDiscussion

This is a STIG-specific adaptation of the risk and vulnerability information described in the SRG VulDiscussion. The VulDiscussion should address the vulnerability as it affects the product in question. Requirements evaluated to be Not Applicable do not require a VulDiscussion.

Do not use the VulDiscussion field to address specific information about particular settings or products.

The Vulnerability Discussion should not be overly long or detailed, but it should be complete enough to:

- Explain the vulnerability from a security perspective.
- Discuss how it affects the product.
- Include a statement that identifies the risk created if the requirement is not met.

4.1.9 Status

Determine the status by analyzing the SRG requirement as it relates to the product for which the STIG is being written.

This is a required field. Select from a drop-down list that contains the following four statuses:

Table 4-1: Statuses

Status	Description
Applicable – Configurable	The product requires configuration or the application of policy settings to achieve compliance.
Applicable – Inherently Meets	The product is compliant in its initial state and cannot be subsequently reconfigured to a noncompliant state.
Applicable – Does Not Meet	There are no technical means to achieve compliance.
Not Applicable	The requirement addresses a capability or use case that the product does not support.

Use the following additional guidance in determining the status:

- If the product can be configured to meet the SRG requirement, the status is **Applicable-Configurable**.
- If the product natively meets the SRG requirement and cannot be reconfigured to be out of compliance, the status is **Applicable – Inherently Meets**.
- If the product **DOES NOT** natively meet the SRG requirement and **CANNOT** be reconfigured to meet the SRG requirement, the status is **Applicable – Does Not Meet**.
- If the product features and functions or overall architecture do not align with the SRG requirement, the status is **Not Applicable**. (For example, if the requirement addresses encryption of removable data storage media but the product does not support removable media, the requirement is Not Applicable.)

The inability to meet an SRG requirement will be used to make residual risk decisions for information systems employing the product.

4.1.10 SRG Check*

The SRG Check content provides a generic approach to assess the SRG requirement. The vendor developing the STIG can reference the SRG Check, as a guide, to create product-specific STIG Check content as described in Section 4.1.11.

4.1.11 Check

Complete this cell only for rows where the status is Applicable – Configurable. Leave it blank for all other status types.

The Check is used to provide specific instruction on how to validate product configuration settings. It must include any information and procedures necessary for validating the configured value.

The Check should also state:

- What system privileges, if any, are necessary to perform the check.
- Whether the check procedure requires local access or can be performed remotely.
- Whether performing the check impacts system reliability or availability.

If the vendor is leveraging third-party tools to satisfy a requirement, identify in the Check the product and the specific steps to check compliance.

If the product is expected to be compatible with a number of third-party tools, include in the Check general instructions that would enable a systems administrator with reasonable familiarity with the third-party tool to perform the necessary procedure.

For example, if the requirement is to block certain TCP ports on a firewall, a general instruction to this effect may suffice.

4.1.11.1 Check Writing Style

Write the Check so the user can easily follow the steps to assess and determine compliance.

- If the check procedure is not applicable for a specific condition, state that at the top of the Check. (Refer to "Check text example" below.)
- Do not restate the requirement in the Check.
- Do not include steps to alter values or settings.
- Do not use words such as "should," shall," or "please."

- Use action verbs such as "verify," "navigate," "identify," "type," "obtain," etc.
- Give exact steps to test compliance with the requirement.
- For checks that require a sequence of actions, use numbered steps as shown below:
    1. Log on to…
    2. Open the…
    3. Click….
    4. Determine…
- Include a "finding" statement written as: "If….this is a finding".

Check text example:

If Bluetooth connectivity is required to facilitate use of approved external devices, this is not applicable.

> To determine if any hardware components for Bluetooth are loaded in the system, run the following command:
>
> # sudo kextstat | grep -i Bluetooth
>
> If a result is returned, this is a finding.

In some cases, determining when an item is NOT a finding might be appropriate.

Check text example:

If the "xyz" parameter is set to "5", this is not a finding.

When using a command to inspect the status of a host, listing example output can be helpful. The output must comply with STIG requirements unless an example of a failure is needed and is clearly explained.

Check text example:

Find the file systems that contain the directories being exported with the following command:

# cat /etc/fstab | grep nfs
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d   /store   nfs   rw,nosuid   0 0

If a file system found in "/etc/fstab" refers to NFS and does not have the "nosuid" option set, this is a finding.

4.1.12 SRG Fix*

The SRG Fix content provides a generic approach to bringing the product into compliance with the SRG requirement. The vendor developing the STIG can reference the SRG Fix, as a guide, to create product-specific STIG Fix content as described in Section 4.1.13.

4.1.13 Fix

Complete this cell only for rows where the status is Applicable – Configurable. Leave it blank for all other statuses.

The Fix is used to provide specific instructions on how to configure the product to comply with the requirement.

After steps in the Fix text are implemented, the resulting system state should be the same no matter how many times the instructions are followed.

4.1.13.1 Fix Writing Style

When writing the Fix content, the vendor must include all steps needed to configure the product to comply with the requirement.

- Do not use general language. When writing the criteria statement in the Fix text, be specific. Use the exact steps to take to bring the product into compliance with the requirement.
- Do not restate the requirement in the Fix.
- In the Fix procedures, do not use such words as "should," shall," or "please."
- Use action verbs such as "ensure," "configure," "set," "select," etc.
- For Fix procedures that require a sequence of actions, use numbered steps as shown below:
    1. Log on to…
    2. Open the…
    3. Click the….
    4. Ensure…
- Do not include a finding statement in the Fix.

4.1.14 Severity

The Severity Category Code (CAT) is an indicator of the risk associated with noncompliance.

The vendor can adjust the severity based on the definitions below.

DOD subject matter experts (SMEs) will verify the CAT value after considering the impact of noncompliance in the overall security architecture of the product and the environment in which it is expected to operate.

The CAT is a required field selected from a drop-down list that contains the following three codes:

Table 4-2: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of confidentiality, availability, or integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of confidentiality, availability, or integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of confidentiality, availability, or integrity.

Requirements evaluated to be Not Applicable do not require a severity.

The severity selection for requirements deemed Applicable – Does Not Meet must reflect the severity **BEFORE** any mitigation steps are taken by an organization.

4.1.15 Mitigation

The Mitigation offers a method for minimizing risk. Mitigations do not eliminate the need for the requirement.

The "Mitigation" field must be populated if the status of the requirement is Applicable – Does Not Meet.

After the mitigation, include a summary statement to address any impact to the overall risk associated with this requirement.

> **Example summary statements**:
> - With the implementation of this mitigation, the overall risk can be decreased to a CAT [II or III].
> - With the implementation of this mitigation, the overall risk is fully mitigated.
> - Although the listed mitigation is supporting the security function, it is not sufficient to reduce the residual risk of this requirement.

An "Applicable – Does Not Meet" vulnerability may be fully mitigated by the application of another STIG check or by the underlying operating system. In these instances, include a statement in the Mitigation as shown in the example below.

Examples of risk mitigated by other STIG requirements:

- This requirement is fully mitigated by the Apache Server 2.4 Windows Server STIG. The Apache Web Server accounts not used by installed features (e.g., tools, utilities, specific services) must not be created and must be deleted when the Apache web server feature is uninstalled. (AS24-W1-000280)
- This requirement is fully mitigated by the underlying operating system. (WN16-SO-000430)

4.1.16 Artifact Description

Populate this information for requirements that have a status of Applicable – Inherently Meets. The Artifact Description describes the artifacts or substantiating information that shows how the product inherently meets the requirement.

All self-certification claims must be accompanied by supporting vendor documentation, which taken as a whole, provides DISA with reasonable assurance that the particular requirement has been met.

This field provides citations to the documentary evidence that describe how each requirement is satisfied. Examples of artifacts include:

- A test report describing the test procedures used to verify compliance and corresponding results, including the specific version of tools used to test and date of test.
- A published administrative manual or configuration guide explaining how compliance can be achieved.
- An attestation from the product developer that the product is compliant, accompanied by a brief statement describing the technical means by which compliance is achieved.
- Steps to verify the product cannot be configured to be out of compliance with the requirement.

Note: Blogs and email messages are not sufficient documentation to support an Applicable – Inherently Meets status.

4.1.17 Status Justification

This information must be populated for requirements that have a status of Not Applicable, Applicable – Does Not Meet, or Applicable – Inherently Meets.

For requirements that have a status of Not Applicable:

- Explain in the Status Justification text why the requirement is not applicable.
- The most common explanations are that the requirements concern a capability that is not present on the device (e.g., encryption of removable data storage media where the

product does not support removable media) or the requirement pertains to an operational environment in which the product will not be placed (e.g., the requirement applies to classified processing when the product is intended only for unclassified applications).

For requirements that have a status of Applicable – Does Not Meet:

- Explain in the Status Justification text what function or feature is not present.
- If some part of the requirement is achievable, the Status Justifications should explain what part of the requirement is unmet and what is met (e.g., the system can lock an account after certain failed logon attempts, but these failures are not limited to a specific window of time).
- If no part of the requirement can be fulfilled, note this information.
- Describe the residual risk after any mitigation is applied.

For requirements that have a status of Applicable – Inherently Meets

- List in the Status Justification text the specific feature of the product that supports this requirement and that cannot be changed.
- Note the type of evidence used to establish compliance (e.g., test report, vendor documentation, or vendor attestation).

4.2 STIG Template Additional Rows

In some cases, multiple configuration settings may be needed to achieve compliance with a single requirement. If this is the case, insert multiple rows into the spreadsheet by:

- Copying the content from the row that contains the requirement.
- Inserting a duplicate row.
- Updating with the specific content.

The IA Control, CCI, SRG ID, SRG Requirement, SRG Check, etc., for the new line must contain the information from the original requirement.

Additional rows are also used when some attack vectors related to a single requirement can be addressed while others cannot. If this is the case, add different STIG-specific requirements to the template and select appropriate statuses for each. As noted above, each new line will retain the same, unchanged items from the root SRG requirement, including IA Control, CCI, SRG ID, SRG Requirement, SRG Check, etc.

4.2.1 Security Features Without Associated SRG Requirement

In some situations, security features in the product will not seem to align with any SRG requirement. If the vendor recommends specific configuration settings as a security best practice, use CCI-000366 to include that information.

CCI-000366 is specifically intended for this purpose. Copy the line in the template containing this CCI as a starting point for adding best practice requirements to the spreadsheet.

5. VALIDATION

After the vendor completes STIG development, the first draft STIG will move to the STIG Validation stage. The steps in this stage assess the accuracy of the Check and Fix instructions on a system, evaluate the requirements in the STIG compared to those of the SRG, and validate additional documentation.

5.1 STIG Review

The DISA SME starts with a high-level review of the package. This includes determining the completeness and rationale of each requirement's status, along with any associated justifications.

5.2 Transition

Once the package is considered complete and is ready for simulation, a transition meeting will be held with the vendor, DISA SME, and a Technology SME. From this point on, the Technology SME will complete the STIG Process, but the vendor may be called on for STIG-related questions.

5.3 STIG Simulation

The Technology SME develops a test plan to validate the STIG content's accuracy in determining what is a finding and what is not a finding and in bringing a system into compliance.

5.3.1 STIG Simulation on Product

During the STIG validation, the vendor may be called on for questions related to the setup of the product or the STIG content submitted. The Technology SME will document the outcome of the testing for each requirement.

The Technology SME will work with the vendor to address any items that are found to be technically incorrect or need substantial rework.

5.3.2 Access to the Vendor's Product

To perform STIG simulation, DISA will require access to the software for which a STIG is being developed. This can be accomplished in a variety of ways:

- Vendor lends the software to DISA; this will require the vendor to complete a product loan agreement.
- Vendor provides an environment at either its site or another DOD site, and DISA uses that environment for the validation.
- Vendor provides a solution that allows the SME to access the environment remotely.

DISA is open to exploring other options based on the situation.

5.3.3   Product Loan Agreement

This form (available upon request) is used as an agreement between DISA and a vendor to allow DISA to use hardware and software owned or licensed by the vendor for STIG testing and evaluation. This is required if the product will be used in the DISA lab. Do not update the language in the document.

5.4 Review of Vendor-Provided Documents

DISA may require other artifacts, in addition to the STIG content, to properly evaluate the entire package.

5.4.1   Published Manual

If a product's ability to fulfill a requirement is determined to be Applicable – Inherently Meets and the published description of this feature is used as an artifact, the DISA SME will validate this reference material. The SME will verify, for the specific product(s) and version(s) within the scope of the STIG, that the documented material establishes that the requirement is fulfilled by default and this state cannot be changed.

Relevant reference material may include citing specific sections of published configuration guides, instructional books, or administrative manuals, and the citation must be specific regarding applicable sections, charts, or graphs within the material.

5.4.2   Test Report

If a product's ability to fulfill a requirement deemed Applicable – Inherently Meets has been independently verified, the SME will inspect the test report to ensure the proper version of the software was used and the testing procedure demonstrates compliance.

5.4.3   Letter of Attestation

A Letter of Attestation is required for any items that have a status of Applicable – Inherently Meets but for which supporting evidence is not documented. A template letter is available upon request.

6. REVIEW AND APPROVAL

The Review and Approval stage is the last milestone in the vendor STIG process. It includes the following steps:

- DISA Internal Reviews.
  - o Technology SME develops a formal compliance report and a briefing for the DISA Authorizing Official.
- Style Guide Review.
  - o Materials are reviewed internally within DISA.
  - o Vendor and DISA collaborate on updates if needed.
- Decision Brief.
  - o Materials are presented to the DISA Authorizing Official.
- DISA AO Approval.
  - o DISA Authorizing Official approves the STIG.
  - o DISA Authorizing Official may limit the use of a product within certain environments or require specific mitigations for its use depending on the risks associated with the use of the product.
    - ▪ Any restrictions on use may be annotated in the signature memo upon approval of the STIG.
- Vendor Notification.
  - o DISA shares the outcome of the Decision Brief with the vendor.
  - o Vendor and DISA collaborate on updates if needed.
- STIG Publication.
  - o STIG (Applicable – Configurable requirements), along with a DISA-provided overview document, is sent to the DISA Public Affairs Office for review and approval.
  - o STIG (Applicable – Configurable requirements), along with a DISA-provided overview document, is published.
  - o STIG (Applicable – Configurable requirements) and overview document are publicly available on the Cyber Exchange website.
  - o STIG requirements (Not Applicable, Applicable – Inherently Meets, or Applicable – Does Not Meet), along with the compliance report, are made available to Authorizing Officials upon request for risk assessment purposes because the data is considered Controlled Unclassified Information (CUI).

7. DISCLAIMER

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DOD Risk Management Framework (RMF). DOD Authorizing Officials may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

DOD Authorizing Officials have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or preacquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

8. SPREADSHEET FIELD CROSS-REFERENCE

The table below identifies fields in the STIG template and defines how they are named in the STIG as it will be viewed from Cyber Exchange.

Table 8-1: Field Name Cross-Reference

Spreadsheet	STIG Viewer
IA	NA
CCI	CCI/CCI ID
SRGID	Rule Name
STIGID	STIG ID/Vul ID
SRG Requirement	NA
Requirement	Rule Title
SRG VulDiscussion	NA
VulDiscussion	Discussion
Status	NA (only Applicable – Configurable requirements are published)
SRG Check	NA
Check	Check Text
SRG Fix	NA
Fix	Fix Text
Severity	Severity
Mitigation	Mitigation Control
Artifact Description	NA
Status Justification	NA