USAID
FROM THE AMERICAN PEOPLE

Baseline Configuration Standards and Guidelines for Agency Hardware and Software: Guidance for CM-6 Compliance

A Mandatory Reference for ADS Chapter 545

New Edition Date: 10/18/2024
Responsible Office: M/CIO/IA
File Name: 545mbk_101824

1. Introduction

1.1. Authority

ADS 101 states that: The Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) develops, enforces, and promotes USAID information security policies, procedures, and standards. **ADS 545.3.6.6** states that the Chief Information Security Officer (CISO) “Must establish and document baseline configuration settings for various information technology (IT) equipment, that reflect the most restrictive mode consistent with operational requirements.”

1.2. Purpose

This document further defines the technical policies established in **ADS 545** which mandate compliance for end-user and network devices that handle USAID information, and require documented secure configurations for the various operating systems and devices deployed through the Agency. This document also supports compliance with the Federal Information Security Modernization Act of 2014 (FISMA). NOTE: This document is not meant to be a policy or procedures document for general baseline configuration or change management.

These controls map to requirements stated in **NIST Special Publication 800-53 Revision 5 - CM-6 Control**, **NIST core Framework PR.IP-1** and the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program, CSM: Configuration Settings Management. The NIST SP 800-53 Revision 5 CM-6 control is a guideline for the Agency to manage its technology systems’ settings to ensure they are secure and involves the following:

- **Establish and Document:** M/CIO must approve and document the security settings for its technology systems. The security systems should ensure appropriate levels of security, balancing system risk against the needed functionality of the system.

- **Implement:** Once the settings are established, M/CIO/ITO must put the settings into place on the systems.

- **Deviation Approval:** If these settings are changed, M/CIO/ITO must document the change and the Change Management Board must approve based on USAID's requirements.

- **Monitor and Control:** M/CIO should monitor these settings and control any changes according to their policies and procedures.

1.3. Audience

The guidance in this document is intended for management and technical personnel who are responsible for the management, operation, or administration of information systems at USAID. This includes Operations and Management (O&M) Personnel, System Managers (SMs), System Owners (SOs), Information System Security Officers (ISSOs), Systems Administrators (SAs), as well as members of the Computer Security Incident Response Team (CSIRT), and the Security Operations Center (SOC).

**Some links in this policy can only be accessed by users who can access the Agency intranet.

1.4. Scope

The guidance in this policy applies to all information systems at USAID or to Agency information systems that contractors maintain on behalf of USAID, including but not limited to: network infrastructure and platform equipment, desktops/laptops, servers, printers, mobile devices, and any software and systems that store, process, or transmit USAID data.

This policy and guidance applies to IT products that store, process, or transmit USAID data, and for which privacy and security-related configuration settings can be defined. This includes:

- All servers including cloud service providers, on-premises, and virtual machines (VMs);
- Workstations, laptops, and mobile devices;
- Input/output devices (e.g., scanners, copiers, printers, and Video Teleconferencing [VTC]);
- Network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, and sensors);
- Operating systems;
- Middleware; and
- Applications and tools (e.g., appliances, browsers, IT systems/productivity tools, and databases).

2. Configuration Settings Baseline (CM-6)

Following a secure standard configuration is critical in eliminating the easy vectors hackers use to launch attacks. A critical defense mechanism against malicious activities is a securely-configured device. This includes the device’s operating system, as well as installed applications that are able to be run as background services or daemons that allow remote access to the covered device.

A Secure Baseline (referred to herein as "**Baseline**") is a type of baseline configuration designed to lower the security and privacy risks presented by the system's presence on interconnected environments. Security Technical Implementation Guides (STIGs) are implementation guides geared to a specific product and version. Each STIG provides technical guidance to secure information systems/software that might otherwise be vulnerable to an attack. The STIGs specify how operating systems, applications, network devices, and other assets should be configured, in order to be secure. For each asset type, the corresponding STIG contains a number of checks to determine if the current configuration meets the approved standards. Each of the checks in a Defense Information Systems Agency (DISA) STIG has a severity level.

2.1. Baselines - General Guidance

1. The USAID CISO, or as a function delegated to Information Assurance (IA) (Security Engineering), establishes organization-wide Baselines and settings, from which SOs can subsequently derive specific configurations for systems.

2. The CISO establishes and documents Baselines for various IT equipment, which reflects the most restrictive mode consistent with operational requirements in the M/CIO USAID Security Baselines.

3. The DISA STIGs are the required common secure configuration standards that must be applied.

4. STIGs need to be applied at the operating system, application, and device (firmware) levels. Depending on the purpose and functionality of the system or device, multiple STIGs or checklists may be required for a single asset.

5. If a STIG has Security Content Automation Protocol (SCAP) Benchmarks associated with it, the benchmarks should be used to verify compliance using an approved SCAP compliance scanning tool.

6. M/CIO must review and approve any CAT I or CAT II controls/requirements in the STIG that can't be applied, using the risk decision process outlined in section 4.4 Deviation Approval and Retesting Process.

7. Other high-level security configurations may need to be applied to complement the STIGs. Security engineering may be able to provide additional required configuration settings (i.e., USAID Checklists, USAID Runbooks, DISA Secure Requirements Guides (SRGs), etc.).

8. If STIGs are not available, additional secure configuration standards, checklists, or benchmarks, must be considered and applied (see section 2.3).

9. The use of Enterprise and Local Group Policy Objects[1] (GPOs), as well as scripts for automated system hardening[2], must be inventoried, documented, and kept up-to-date by M/CIO/ITO.

10. GPO containing most applicable GPO STIG settings contained in the STIG files can be found on the DISA website.

11. Standards obtained via downloadable packages that contain recommended security settings must be used carefully, since they are not meant to replace well-structured policy. These recommendations do not address site-specific configurations.

12. Baselines for cloud applications, services, or solutions must be reviewed, evaluated, tailored, and continually monitored by M/CIO.

    a. The Cloud Computing Security Requirements Guide (CC SRG) can be found on the USAID Device Security Baselines web page.

    b. Other security standards and best practices may be considered for each specific cloud provider/vendor (Amazon Web Services, Azure, and the Google Cloud Platform (GCP)).

2.2. Security Technical Implementation Guides

DISA[3] STIG, Mission Assurance Category Level 2 (MAC2) Sensitive, is the minimum approved MAC Level for USAID end-points, including, but not limited to: devices, systems, network components, and applications, categorized at the Moderate or High Impact Level.

DISA Severity Categories:

[1] (Important: “It must be noted that the Group Policy Objects (GPO) provided should be evaluated in a local, representative test environment before implementation within production environments. The extensive variety of environments makes it impossible to test these GPOs for all potential enterprise Active Directory and software configurations. For most environments, failure to test before implementation may lead to a loss of required functionality.

It is especially important to fully test with all GPOs against all Windows Operating Systems, internet browsers, specific and legacy applications which are targeted by each STIG GPO which are currently used in the environment.”

[2] A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.

[3] Defense Information System Agency Security Technical Implementation Guidelines

The Defense Information Systems Agency (DISA) releases the Security Technical Implementation Guidelines (STIG). STIGs provides recommendations for secure installation, configuration, and maintenance of software, hardware, and information systems. STIG is one of the bases of configuration standards that the U.S. Department of Defense uses. For more information about DISA and STIGs, see http://www.disa.mil/.

- CAT I – Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity (CIA).

- CAT II – Any vulnerability, the exploitation of which has a potential to result in loss of CIA. These are equal to a High vulnerability.

- CAT III – Any vulnerability, the existence of which degrades measures to protect against loss of CIA.

USAID systems are required to follow the STIGs, available for download on the Department of Defense (DoD) Cyber Exchange STIGs Document Library webpage.The M/CIO/IA Engineering Team collects, validates, and distributes Baselines for devices that connect to AIDNet, and monitors the STIGs for updates. This site provides up-to-date configuration Baselines required for systems/devices to connect to AIDNet.

2.3. Additional Security Checklists, Standards, and Repositories

Common secure configurations can be developed by a variety of organizations, including IT product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors. The figure below shows an overview of the process used to identify the STIGs, DISA Security Requirements Guides (SRGs), and other applicable checklists that need to be applied for compliance.

If no STIG is defined and available for a specific product, application, and application component, or version of a product or application, follow the guidance provided by DISA below:

1. Determine if a STIG has been published for an earlier version of the same product. Many checks and fixes in earlier versions of STIGs can be applied to the new version of the product.

    a. If a STIG for an older version of the product is available, review the configuration setting, check and fix procedures to determine which of these work with the new product version. Where possible, use the checks and fixes that work directly with the new version.

Important: Any STIG or SRG labeled "Sunset" [4] *can't be used for configuration guidance to meet compliance.*

[4] Sunset products are older SRGs, STIGs, Checklists, or Tools (i.e., DISA products) that may be relevant to the vendor products they address, but are no longer supported by DISA for various reasons. The most common reason for this lack of DISA support is that the vendor product is outdated, superseded by a newer vendor product, or may be vendor non-support. The lack of DISA support means that there is no active maintenance of the DISA product, therefore no updates of the product will be published. Lack of DISA maintenance means that any new vulnerability in the vendor's product will not be captured for mitigation, and the DISA product is either, or will quickly become, out-of-date. Since DISA is no longer maintaining a given product, a SME responsible for, and knowledgeable about, the product may not be available; customer support questions will likely not be answerable.

b. M/CIO must evaluate the remainder of checks and fixes that no longer work with the new product version and proper check and fix procedures need to be determined for each requirement.

c. New product features and configuration settings must also be accounted for based on any relevant SRG.

d. If there is no related STIG, the most relevant SRG can be used to determine compliance.

NOTE: In fulfilling a requirement, whether from an SRG or an earlier version of a STIG, vendor documentation may be followed for configuration guidance.

2. If no STIG is available for the current version, or a previous version of the **specific product, or application and application components,** they must be configured using the following checklists**,** starting with the top of the list, and moving to the next checklist, only if the first is not available (see SP800-70 Revision 4).

3. NIST-produced checklists, which are tailored for civilian agency use, at: NCP - National Checklist Program Checklist Repository.

The National Checklist Program (NCP) is the U.S. Government's repository of publicly available security checklists (or benchmarks), that provide detailed low level guidance on setting the security configuration of operating systems and applications.

4. Checklists produced by the National Security Agency (NSA), available at: NCP - National Checklist Program Checklist Repository.

5. If formal government-authorized checklists do not exist, use vendor-produced checklists.

6. If vendor-produced checklists are not available, use other checklists that are posted on the NCP website from other trusted third parties, such as the Center for Internet Security (CIS).

7. If no third-party checklists exist, use industry leader's accepted best practices, independent testing results, or vendor literature and hardening lock down guides.

8. If you are unable to find the necessary checklists, or you need further assistance, you can open a Service Central ticket with the following information:

- **Category:** CISO Secure Baseline
- **Type:** Compliance Checklist Request
- **Item:** Compliance Checklist / Hardening Information
- **Group:** "Information Assurance Security Engineering"

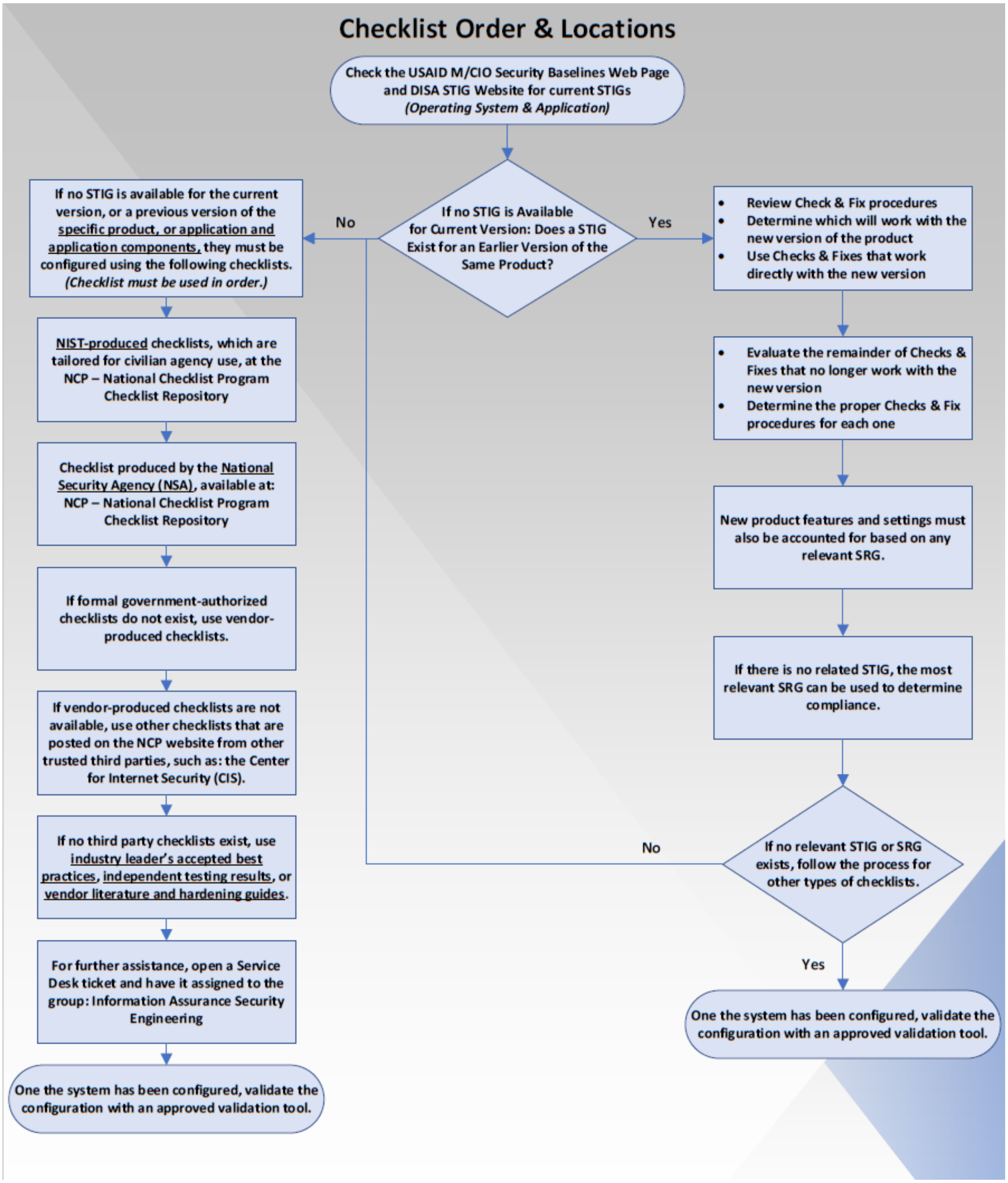
Checklist Order & Locations
Check the USAID M/CIO Security Baselines Web Page and DISA STIG Website for current STIGs (Operating System & Application)
If no STIG is Available for Current Version: Does a STIG Exist for an Earlier Version of the Same Product?
No
Yes
If no STIG is available for the current version, or a previous version of the specific product, or application and application components, they must be configured using the following checklists. (Checklist must be used in order.)
NIST-produced checklists, which are tailored for civilian agency use, at the NCP – National Checklist Program Checklist Repository
Checklist produced by the National Security Agency (NSA), available at: NCP – National Checklist Program Checklist Repository
If formal government-authorized checklists do not exist, use vendor-produced checklists.
If vendor-produced checklists are not available, use other checklists that are posted on the NCP website from other trusted third parties, such as: the Center for Internet Security (CIS).
If no third party checklists exist, use industry leader's accepted best practices, independent testing results, or vendor literature and hardening guides.
For further assistance, open a Service Desk ticket and have it assigned to the group: Information Assurance Security Engineering
One the system has been configured, validate the configuration with an approved validation tool.
• Review Check & Fix procedures
• Determine which will work with the new version of the product
• Use Checks & Fixes that work directly with the new version
• Evaluate the remainder of Checks & Fixes that no longer work with the new version
• Determine the proper Checks & Fix procedures for each one
New product features and settings must also be accounted for based on any relevant SRG.
If there is no related STIG, the most relevant SRG can be used to determine compliance.
No
If no relevant STIG or SRG exists, follow the process for other types of checklists.
Yes
One the system has been configured, validate the configuration with an approved validation tool.

Figure 1: Checklist Order & Locations

2.4. Applicable Checklist Process Overview

This section describes a high-level process to follow when retrieving and using checklists.

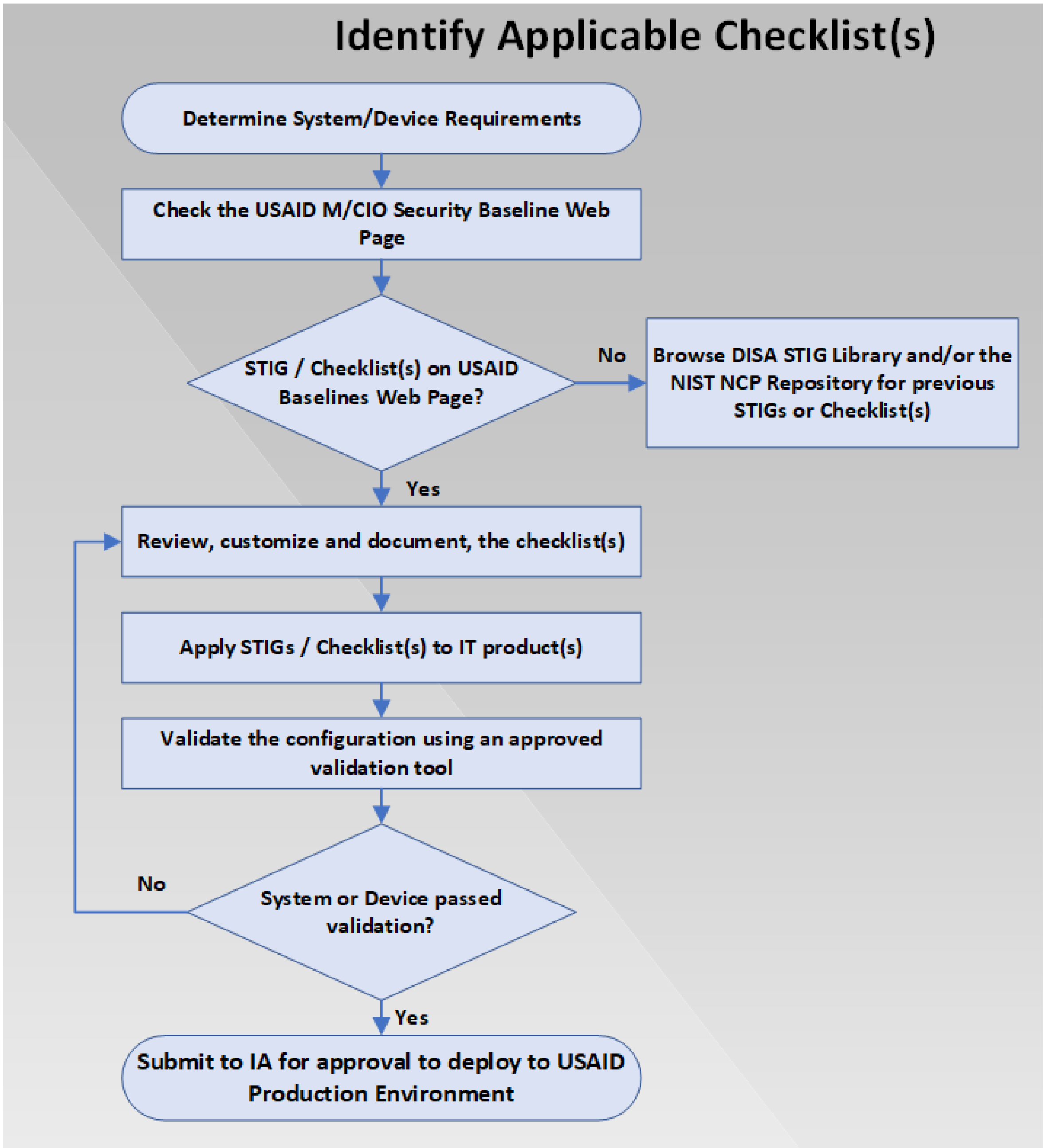
Identify Applicable Checklist(s)
Determine System/Device Requirements
Check the USAID M/CIO Security Baseline Web Page
STIG / Checklist(s) on USAID Baselines Web Page?
No
Browse DISA STIG Library and/or the NIST NCP Repository for previous STIGs or Checklist(s)
Yes
Review, customize and document, the checklist(s)
Apply STIGs / Checklist(s) to IT product(s)
Validate the configuration using an approved validation tool
No
System or Device passed validation?
Yes
Submit to IA for approval to deploy to USAID Production Environment

Figure 2: Applicable Checklist Process Overview

Figure 2 shows an overview of the general process for identifying and using checklists.

The general steps involved in acquiring and using checklists are:

1. SAs gather their requirements, including, but not limited to:

   - **a.** System or device being configured, upgraded, changed, etc.,
   - **b.** Operating system or firmware installed on the system or device, and
   - **c.** Any other software, applications, or functionality, installed or configured on the system or device.

2. SAs check the USAID CISO Secure Baseline web page to identify and obtain the following:

   - **a.** STIGs,
   - **b.** Other checklists that match the operational and security requirements, and
   - **c.** USAID specific runbooks and/or checklists.

3. If no STIGs or checklists are identified on the USAID CISO Secure Baseline web page, SAs browse the DISA STIG library, or the NIST NCP Repository, for STIGs for previous versions, or other checklists.

4. SAs review the checklists and select the checklist(s) that best meets their requirements, then tailor and document the checklist(s) as necessary, to take into account local policies and functional requirements.

5. SAs prepare to apply the checklist(s), such as making configuration or data backups, and then apply the checklist(s) to their system or device.

6. SAs apply all applicable USAID runbooks and/or checklists, etc.

7. SAs validate the configuration of their system or device by scanning it with an approved validation tool (i.e., SCAP Compliance Checker [SCC]).

8. After it has been scanned, SAs gather feedback on the configuration of the system or device, and document any necessary information. See section 3.4 Deviation Approval and Retesting Process for information about the deviation approval process.

2.5. Baselines for High-risk Systems and Components

When systems or system components will be in high-risk areas external to the organization, M/CIO may implement additional controls to counter the increased threat in such areas.

2.5.1. Devices Near or Within Restricted Spaces.

To comply with 5 FAM and ADS policies 552 and 568, a hardened baseline must be applied to unclassified computing devices used within ten feet of USAID restricted spaces that at least include controls on:

- The use of video or audio equipment and external interfaces in desktops, laptops, smartphones and VOIP phones.

- The use of collaborative equipment and capabilities, such as VTC and Web remote connections.

- The use of wireless capabilities, including active and passive mode of Wi-Fi, NFC, Bluetooth, IR, and broadband connections.

2.5.2. Devices Involved in High-Risk Travel

For elevated threat situations such as configuration of network devices before travel, or possible compromise during travel, please refer to ADS 545.3.6.2 for additional guidelines on devices involved in high-risk travel. A Diplomatic Pouch must be the default method of shipping of security devices to Missions.

2.5.3. Systems Used as Elevated Privilege Platforms / Devices

Administrators of high-value IT assets and security tools must not have administrator rights on the Privileged Access Workstation (PAW) itself. The PAW STIG is published as a tool to improve the security of information systems. The STIG is meant for use in conjunction with the appropriate version of the Windows STIG.

The PAW STIG provides configuration and installation requirements for dedicated Windows workstations used exclusively for remote administrative management of designated high-value IT resources, including servers, workstations, directory services, applications, databases, and network components. A high-value IT resource is defined as any IT resource whose purpose is considered critical to the organization or whose loss or compromise would cause a significant impact to the organization.

The STIG assumes the applicable controls have been applied to the PAW prior to the implementation. Note that some configurations required by this STIG may need to be implemented in the domain rather than on the PAW. In addition, and similar to the PAW paper, this STIG focuses on the setup and configuration of a PAW on a workstation rather than the setup of multiple PAWs in a VM environment. There are only two requirements in this STIG related to deploying PAWs in a VM environment. If one or more PAWs are installed as VMs on a host server, this STIG assumes the applicable VM product STIG has been applied.

2.5.4. Technical Security Requirements for Cloud Based Technologies

Cloud Systems must follow specific M/CIO/IA instructions provided in Technical Security Guidance documents for Containers and Kubernetes Hardening, Internet of Things (IoT) Devices, and other emerging information technologies. For additional information, open a Helpdesk ticket assigned to Information Assurance Security Engineering.

3. Security Content Automation Protocol (SCAP) Security Compliance Checker (SCC)

SCAP is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. SCAP is a multi-purpose framework of specifications that support automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. SCAP is an effective method of identifying system security controls, and standardizing system security management.

SCAP utilizes software flaw and security configuration standard reference data. This reference data is provided by the National Vulnerability Database (NVD), which is managed by NIST and sponsored by the Department of Homeland Security (DHS). The SCAP and the defined standards within the protocol, provide an effective method to uniquely identify, track, and control configuration settings.

DISA creates and publishes SCAP content to automate the verification of their STIGs, and DISA's SCAP content is the primary content used with SCAP SCC, but it can be customized so that any user could install their SCAP content into SCC.

SCAP SCC links:

- DISA SCAP Compliance Checker tool
- SCAP Compliance Checker - Video Tutorials
- SCAP project information (NIST)

SCAP Benchmarks: These types of checklists are available on the DISA STIG website, and in the National Checklist Program Repository at:

- DISA Website
- NIST Website

3.1. SCAP Compliance Validation for New or Changed Systems

M/CIO/ITO must use an Architecture Review Board (ARB) approved SCAP compliance validation tool to validate system compliance with all applicable DISA STIGs and/or DISA and USAID checklists.

3.2. Continuous Monitoring of Systems and Devices

The ability to monitor systems for continued adherence with a standard is just as important as having one to begin with. Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turn helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

In order for a tool to automatically determine the compliance level of networked systems against the STIGs, three things must occur:

- The tool must know the configuration of the systems on the network.
- The tool must know what the compliance standard should be.
- The tool must be able to match the actual configuration against the compliance standard and report the deltas no less than once a month.

M/CIO/ITO is responsible for the ongoing assessment of security control effectiveness [RMF 6, Steps: Assess, Monitor] and must monitor and control changes to the configuration settings in accordance with organizational policies and procedures [NIST 800-53, r5; CM-6, d]. ITO must perform validation scans on a representative sample of assessment objects.

A risk with sampling is that the sample population may fail to capture the variations in assessment outcomes that would be obtained from an assessment of the full population. This could result in an inaccurate view of security control effectiveness and organizational security status [NIST SP 800-137, 3.1.4].

NIST SP 800-53A, as amended, describes how to achieve satisfactory coverage when determining sample populations for the three named assessment methods: examine, interview, and test. The guidelines in NIST SP 800-53A for basic, focused, and comprehensive testing addresses the need for a “representative sample of assessment objects” or a “sufficiently large sample of assessment objects.” Statistical tools can be used to help quantify sample size [NIST SP 800-137, 3.1.4].

NIST 800-53A provides guidelines to help address the general issue of sampling and particularly that of coverage. In selecting a sample population, the coverage attribute is satisfied through consideration of three criteria [NIST SP 800-137, 3.1.4]:

When selecting a sample population, the coverage attribute is satisfied through the consideration of these three criteria [NIST SP 800-53A REV. 5, as amended, Appendix C, p. 709]:

- **Types of objects -** ensure sufficient diversity of types of assessment objects (e.g., servers, laptops, switches, routers, firewalls, etc.);
- **Number of each type -** choose **“**enough” objects of each type to provide confidence that assessment of additional objects will result in consistent findings; and
- **Specific objects per type assessed -** given all of the objects of relevance throughout the organization that could be assessed, include at least 10 percent of objects per type (test a sample of at least 10 percent of each type of object) in

the sample population to sufficiently account for the known or anticipated variance in assessment outcomes.

3.3. Independent SCAP Validation

M/CIO/IA may perform random Baseline validation scans on selected USAID devices, hosts, or applications. Baseline validation scans are done using an authorized automated configuration auditing tool.

3.4. Deviation Management

A Plan of Action and Milestones (POA&M) is required to track any deficiencies of CAT I or CAT II checks until a solution is identified or the risk is accepted (time delimited by Authorizing Official [AO] and ADS policy). M/CIO/ITO must disclose and document any CAT I or CAT II deviations from the DISA STIGs in updates/upgrades as a part of the CCB process. If a CAT I or CAT II finding can’t be remediated, the Information System Security Officer (ISSO) must provide a justification for an exemption to IA for review.

3.4.1. Threshold of Compliance

The minimum threshold for compliance is currently 85 percent with no CAT I or CAT II findings. The CISO must annually review this threshold level, and communicate the threshold to SOs.

3.5. Reporting Compliance to M/CIO

SOs must provide M/CIO with status reports of operational information systems baseline compliance against the baseline threshold on a monthly basis.

545mbk_101824