IIS 7.0 WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 16

26 January 2018

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Internet Information Services 7.0 Web Server Overview is a published document that can be used to improve the security posture of a Department of Defense (DoD) web server and its associated websites. This document is meant for use in conjunction with the Enclave, Network Infrastructure, Application Security and Development, and other appropriate operating system Security Technical Implementation Guides (STIGs). Guidance for deployment of web servers within the DoD intranet and the Demilitarized Zone will be governed by the appropriate Network Infrastructure STIG provided by the Defense Information Systems Agency.

The web server must be configured to protect classified, unclassified, and/or restricted data such as Personally Identifiable Information, as well as data approved for public release. Immediate risks inherent to this role are external attacks and accidental exposure. Although security controls and infrastructure devices (such as firewalls, intrusion detection systems, and baseline integrity checking tools) offer some defense against malicious activity, security for web servers is best achieved through implementing a comprehensive defense-in-depth strategy. This strategy should include, but is not limited to, server configuration to prevent system compromise, operational procedures for posting data to avoid accidental exposure, proper placement of the server within the network infrastructure, and the allowance or denial of ports, protocols, and services used to access the web server.

This document is a requirement for all DoD-owned information systems and DoD-controlled information systems operated by a contractor and/or other entity on behalf of the DoD that receive, process, store, display, or transmit DoD information, regardless of classification and/or sensitivity. These requirements are designed to assist Security Managers (SMs), Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD information system design, development, implementation, certification, and accreditation efforts, but is restricted to policies and configurations specific to web servers and sites.

Guidance for the configuration of Operating Systems (OSs) will be governed by the specific OS STIG provided by DISA.

Guidance for use and configuration of technologies, such as mobile code and Common Gateway Interface (CGI) scripts, used by hosted applications will be governed by sources such as the Application and Security Development STIG, and guidance on mobile code will be provided by DISA.

Enclave requirements will be governed by the Enclave STIG provided by DISA.

All STIGs are available on the Information Assurance Support Environment (IASE) website: http://iase.disa.mil/.

This guidance is scoped to the Web Server role, using IIS 7.0, of Microsoft's Windows Server 2008, and no other server role or OS will be addressed. Additionally, certain feature extensions of IIS such as, but not limited to, File Transfer Protocol (FTP) publishing are not addressed by this publication.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: 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.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval 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 (AOs) 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.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

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

2. WEB SERVER AND SITE REQUIREMENTS

2.1 Web Server and Site Definition

A web server is an automated information system that manages one or more websites by passing or serving up web pages to an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer. This document is only applicable to web servers and sites.

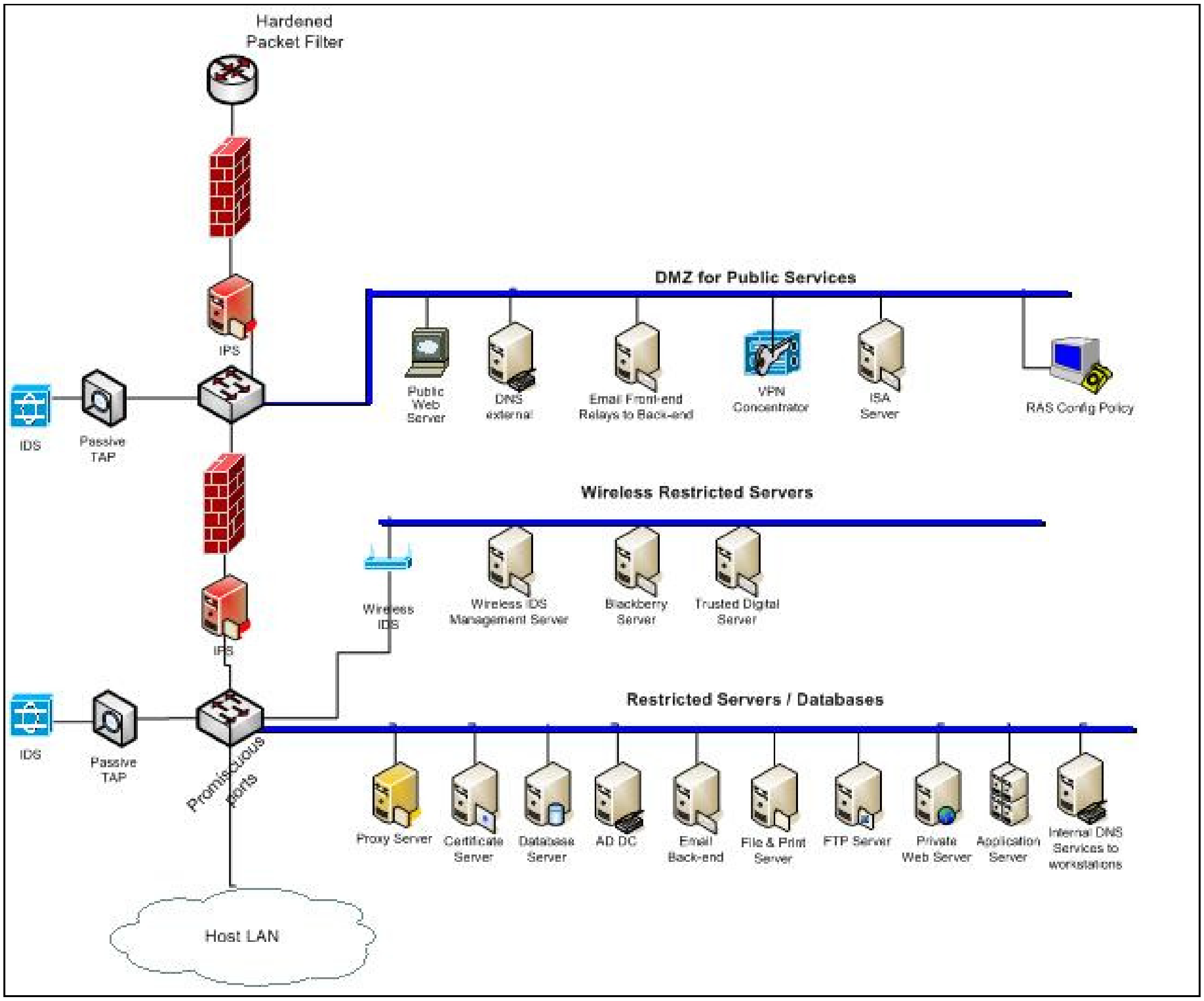
2.2 Web Policy – Applicable to All Web Servers and Sites

Web policy requirements are applicable to all web servers and sites. Review Web Policy checks for all web servers or sites (classified or unclassified) that are used to process, transmit, store, or connect to DoD information or enclave resources. These checks should be reviewed before web server- and website-specific technology checks are implemented. These policies are listed in the Vulnerability Management System (VMS) under the Non-Computing Assets, Web Policy asset posture, and in VMS under the Computing Assets, Generic Web Server Instance, and Generic Web Server Site asset postures. The reviewer should create one non-computing asset for policy checks, and then apply one computing asset for a web server review and one computing asset for each website hosted on the reviewed web server.

2.3 Web Server and Site Topology

Web server and sites operating within the DoD are segregated as one of the many hardening initiatives in order to protect the NIPRNet. The approach to meet this initiative is to quarantine public-facing applications and to protect them. Additionally, protections are built into the architecture to segregate restricted and unrestricted applications from private applications. Figure 2-1 provides a visual representation of the DoD Enclave Network.

Figure 2-1: Typical Enclave Network



2.4 Clarification of Terms

2.4.1 Data Hosting – Public vs. Private vs. Restricted

Information served from DoD web servers will be categorized by both service and data types as follows:

- Service Types:
  - Unrestricted: Any service that is intended to provide unclassified and non-sensitive information accessible from outside the NIPRNet, to include anonymous access.
  - Restricted: Any service that is intended to be accessible from the Internet and serves sensitive information to a limited set of users. Access controls are in place to limit the user set that can access the service.
  - Private: Any service that is only meant to be accessed from the NIPRNet or the SIPRNet location or method.

- Data Types:
  - Unrestricted: Informational data that is available from the Internet to anyone and authentication is not required for access. Examples of where this type of data resides includes sites such as www.army.mil and www.usmc.mil.
  - Restricted: Informational data that must be available from the Internet, but access is restricted to authorized users and authentication is required. Examples of where this type of data resides include the Army Knowledge On-Line portal (www.us.army.mil) or email web portals where authentication is required to access the site. A potential subset of restricted data is partner data where access is further restricted to a specific group of individuals, perhaps by source Internet Protocol (IP) address.

Restricted data and services refer to data and services that are restricted to a specific target audience. Restricted data and services may exist within the NIPRNet, the SIPRNet, or the DMZ. The term sensitive information simply means information that is not for general consumption and should not be confused with the definition for classified or unclassified information.

A DoD web server or site, existing within and available across either the NIPRNet or the SIPRNet, will be considered *private* for the purposes of this document.

A DoD web server or site operating within the DoD DMZ *may be considered restricted or public* for the purposes of this document, depending on the *service and data type* of the information being hosted.

Information hosted by web servers in the DoD DMZ falls into one of two categories:

- Unrestricted information that has been reviewed and approved for release to the general public
- Restricted information that is limited to specific target groups such as government, industry partners, DoD employees, and retirees

A web server or site having an unrestricted service and data type will be considered *public* for the purposes of this document. A web server or site having a restricted service and data type will be considered *restricted* for the purposes of this document.

2.4.2 Roles

The roles of the SA and the web administrator or web master are generally understood but sometimes, these terms are used interchangeably. The SA is responsible for the OS, while the web administrator or web master usually manages the website or sites. In some cases, the SA is also the web administrator/web master, which is why guidance tends to be written in a certain fashion. The application development group should refer to the organization that actually wrote the web application that is hosted on a website for further guidance, where applicable.