

UNCLASSIFIED



Web Policy

Technology Overview

Version 1, Release 1

28 October 2011

Developed by DISA for the DoD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Background	1
1.2 Authority	1
1.3 Scope	1
1.4 Vulnerability Severity Code Definitions	2
1.5 STIG Distribution.....	4
1.6 Document Revisions	4
2. WEB SERVER AND SITE REQUIREMENTS	6
2.1 Web Server and Site Definition	6
2.2 Web Policy – Applicable to All Web Servers and Sites	6
2.3 Web Server and Site Topology	6
2.4 Clarification of Terms	7
2.4.1 Private vs. Public Web Server	7
2.4.2 Roles	8
APPENDIX A. RELATED PUBLICATIONS	9
Government Publications.....	9
Government and Technical Web Sites.....	9
APPENDIX B. ACRONYMS.....	10

The page is intentionally left blank.

1. INTRODUCTION

1.1 Background

The web policy STIG should be used in conjunction with web server specific guidance (i.e. IIS, Apache, etc.) when performing a web server review. The web policy STIGs intent is to consider the non-computing aspects of web server security management.

1.2 Authority

DoD Directive 8500.1 requires “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA”. This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in this document provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance Category I through III, applicable DoD Instruction 8500.2 Information Assurance (IA) controls need to be applied to all systems and architectures.

The Information Operations Condition for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

1.3 Scope

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 Assurance Managers (IAMs), Information Assurance Officers (IAOs), 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 the use and configuration of technologies, such as mobile code and Common Gateway Interface (CGI) scripts utilized by hosted applications, will be governed by the Application Security and Development STIG and mobile code guidance 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) web site: <http://iase.disa.mil/>.

1.4 Vulnerability Severity Code Definitions

Severity Category Code (CAT) is a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a severity code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability. Table 1-1 provides the severity code definitions.

Table 1-1. Vulnerability Severity Category Code Definitions

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
CAT I	<p>Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability or Integrity. An ATO will not be granted while CAT I weaknesses are present.</p> <p>Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.</p>	<p>Includes BUT NOT LIMITED to the following examples of direct and immediate loss:</p> <ol style="list-style-type: none">1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure.2. Allows unauthorized access to security or administrator level resources or privileges.3. Allows unauthorized disclosure of, or access to, classified data or materials.4. Allows unauthorized access to classified facilities.5. Allows denial of service or denial of access, which will result in mission failure.6. Prevents auditing or monitoring of cyber or physical environments.7. Operation of a system/capability which has not been approved by the appropriate Designated Accrediting Authority (DAA).8. Unsupported software where there is no documented acceptance of DAA risk.
CAT II	<p>Any vulnerability, the exploitation of which, has a potential to result in loss of Confidentiality, Availability or Integrity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.</p> <p>Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone</p>	<p>Includes BUT NOT LIMITED to the following examples that have a potential to result in loss:</p> <ol style="list-style-type: none">1. Allows access to information that could lead to a CAT I vulnerability.2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission.3. Allows unauthorized access to user or application level system resources.

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
	device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	<ol style="list-style-type: none"> 4. Could result in the loss or compromise of sensitive information. 5. Allows unauthorized access to Government or Contractor owned or leased facilities. 6. May result in the disruption of system or network resources that degrades the ability to perform the mission. 7. Prevents a timely recovery from an attack or system outage. 8. Provides unauthorized disclosure of or access to unclassified sensitive, personally identifiable information (PII), or other data or materials.
CAT III	<p>Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability or Integrity. Assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.</p> <p>Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.</p>	<p>Includes BUT NOT LIMITED to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data:</p> <ol style="list-style-type: none"> 1. Allows access to information that could lead to a CAT II vulnerability. 2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information. 3. Allows the running of any applications, services or protocols that do not support mission functions. 4. Degrades a defense in depth systems security architecture. 5. Degrades the timely recovery from an attack or system outage. 6. Indicates inadequate security administration. 7. System not documented in the sites C&A Package/System Security Plan (SSP). 8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).

For web server installations and sites, policies are classified as CAT I if failure to comply may lead to an exploitation which has a high probability of occurring, does not require specialized

expertise or resources, and leads to unauthorized access to sensitive information (e.g., classified). Exploitation of CAT I vulnerabilities allows an attacker physical or logical access to a protected asset, privileged access, bypass the access control system, or access to high value assets (e.g., classified).

Exploitation of CAT II vulnerabilities also leads to unauthorized access to high value information; however, additional sophistication, information, or multiple exploitations are needed. Exploitation of CAT II vulnerabilities provides information with a high potential of allowing access to an intruder but requires one or more of the following: Exploitation of additional vulnerabilities, exceptional sophistication or expertise, or does not provide direct or indirect access to high value information (e.g., classified).

A policy with a CAT III severity code requires unusual expertise, additional information, multiple exploitations, and does not directly or indirectly result in access to high value information. Exploitation of CAT III vulnerabilities provides information potentially leading to a compromise. It requires additional information or multiple exploitations to be effective but does not provide direct access to high value information.

1.5 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the IASE web site: <http://iase.disa.mil/>. This site contains the latest copies of any STIGs, scripts, and other related security information.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to the following address: fso_spt@disa.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally left blank.

2. WEB SERVER AND SITE REQUIREMENTS

2.1 Web Server and Site Definition

A web server is an automated information system managing one or more web sites 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) used to process, transmit, store, or connect to DoD information or enclave resources. These checks should be reviewed before web server and web site specific technology checks are implemented. These policies are listed in the Vulnerability Management System (VMS) under the Non-Computing assets, Web Policy asset posture. The reviewer should create one non-computing asset for policy checks, one computing asset for a web server review, and one computing asset for each web site hosted on the reviewed web server.

2.3 Web Server and Site Topology

Web server and sites operating within an enclave use segregation as a hardening technique. This approach is intended to quarantine and protect public-facing applications. Additionally, protections are built into the architecture to segregate restricted and unrestricted applications from private applications. Figure 2-1 below provides a visual representation of a typical Enclave.

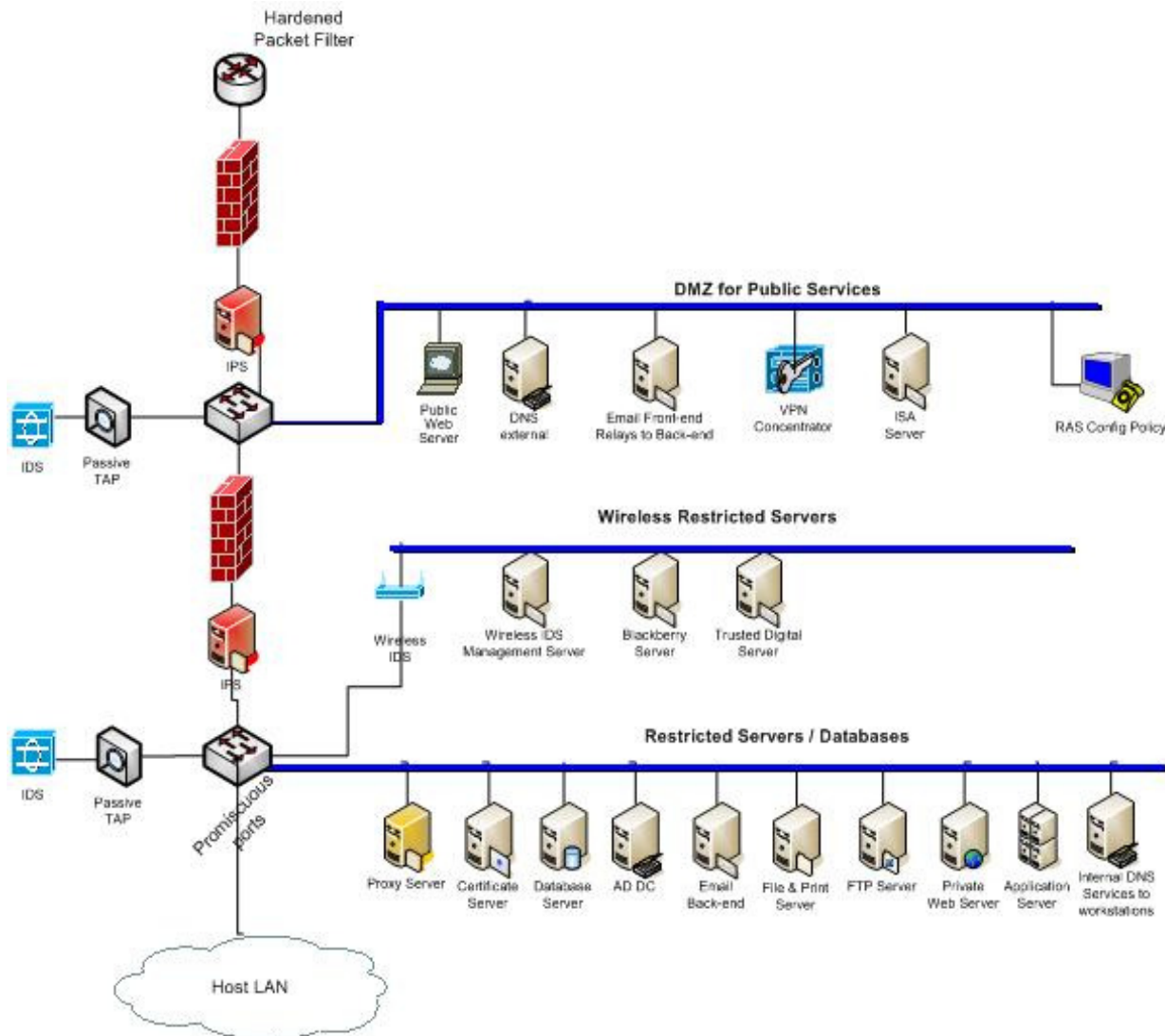


Figure 2-1. Typical Enclave Network

2.4 Clarification of Terms

2.4.1 Private vs. Public Web Server

A DoD private web server as defined by the *Department of Defense Instruction 8520.2* is: “E2.1.12. DoD Private Web Server. For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation.”

A DoD public web server is any DoD-owned, operated, or controlled web server providing access to information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29. Given the DoD definition of a private web server, a public web server may reside on the SIPRNet provided the information published does not require need-to-know control or compartmentalization.

While posting appropriate data to a properly protected public or private web server is necessary to facilitate operations, all personnel and other content providers must exercise extreme caution to ensure they do not post inappropriate material. Current examples of such material include classified data, data covered by the Privacy Act, unclassified but sensitive data (such as, Health Insurance Portability and Accountability Act (HIPAA) related information), contract (procurement) sensitive information, proprietary data, or For Official Use Only (FOUO) information.

2.4.2 Roles

The roles of the SA, web administrator, or web master are generally understood but the terms are often used interchangeably. The SA is responsible for the OS, while the web administrator or web master usually manages the web site 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 supporting organization for the application, when application issues arise from meeting STIG requirements. This guidance does not cover every unique application and configuration.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance," 24 October 2002.

Department of Defense, DoD Instruction (DoDI) 8500.2, "Information Assurance IA Implementation," 6 February 2003.

Department of Defense, DoD Instruction (DoDI) 8520.2 "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 2004.

Department of Defense, DoD Instruction (DoDI) 8551.1, "Ports, Protocols, and Services Management (PPSM)," 13 August 2004.

Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01A, "Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)," 24 June 2009.

Department of Defense, DoD Instruction (DoDI) 8510.01 "DoD Information Assurance Certification and Accreditation Process," April 2004.

National Institute of Standards and Technology (NIST), "Guidelines on Securing Public Web Servers," Special Publication 800-44.

Web Server Security Technical Implementation Guide (STIG) V7R1, 20 September 2010.

Government and Technical Web Sites

<http://iase.disa.mil>

<http://www.disa.mil/handbook/toc.html>

<http://www.cert.org>

<http://csrc.nist.gov/publications>

<http://www.defenselink.mil/Webmasters>

<http://www.w3.org/>

<http://www.owasp.org>

<http://cisecurity.org/en-us/?route=default&>

Defense Information Systems Agency

DISA Web Handbook

A Focal point for the computer security concerns of Internet users

National Institute of Standards and Technology's Computer Security Resource Clearinghouse

DoD Web Site Administration Policy

Information and Resources on everything Web

Foundation dedicated to improving web security

Center for Internet Security.

APPENDIX B. ACRONYMS

ATO	Authority To Operate
C&A	Certification and Accreditation
CAT	Category Codes (for Mission Assurance Category)
CIO	Chief Information Officer
CNDSP	Computer Network Defense Service Provider
COTS	Commercial Off The Shelf
CTO	Communication Tasking Order
DAA	Designated Accrediting Authority
DIACAP	Department of Defense (DoD) Information Assurance Certification and Accreditation (C&A) Process
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
FSO	Field Security Operations
GOTS	Government Off The Shelf
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
INFOCON	Information Operations Condition
JTF-GNO	Joint Task Force - Global Network Operations
MAC	Mission Assurance Category
NIPRNet	Non-classified Internet Protocol Router Network
OS	Operating System
PII	Personally Identifiable Information
PPS	Ports, Protocols, and Services
SA	System Administrator
SM	Security Manager
SSP	System Security Plan
STIG	Security Technical Implementation Guide
URL	Uniform Resource Locator