DRAFT

ACCESS CONTROL STIG

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 0

25 August 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This Access Control Security Technical Implementation Guide (STIG) supports DOD's implementation of the government's mandate which calls for security systems and procedures that provide appropriate levels of assurance for efficiently verifying the identity of individuals seeking physical and electronic access to federally-controlled government facilities and information systems. Security controls are discussed according to the type of environment and the sensitivity of the system being accessed. For example, the enclave areas will be at locations from in a commercial building, federal building not on any government installation, government installation, to a deployed or tactical site. Not all countermeasures will be the same depending on the environment.

Recent events have led to the need for development of a Security Technical Implementation Guide (STIG) to enable Department of Defense (DOD) compliance with Homeland Security Presidential Directive, HSPD12. HSPD12 mandates that all government agencies implement Federal Information Processing Standards (FIPS) 201-compliant personal identity verification for federal employees and contractors. FIPS201 defines the Personal Identity Verification (PIV) card, which is a cryptographically enabled smart card, with both a current-state and a future-state definition. At a minimum, HSPD12 requires that all new federal agency employees and contractors will be identity-proofed in accordance with the current-state PIV (PIV-1) by October 2005 and that the backlog of all current employees and contractors will be identity-proofed in accordance with PIV-1 by October 2007. The current-state PIV is defined by the Federal Identity Credential (FIC), which was based largely on the requirements defined by the DOD Common Access Card and modified by input from the other federal agencies.

Section 2 discusses and compares various authentication technologies, which can be implemented in a single layer or in combination. Security assurance levels attainable using the various authentication technologies on the CAC (which roughly corresponds to DOD's PIV-1 credential) will be considered. Section 3 discusses physical considerations for access control. Section 4 provides guidance for logical access control to DOD information systems.

1.2 Authority

DOD Directive 8500.1 requires that "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 DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

1.3 Scope

To be developed.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**," indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1.1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

2. TECHNOLOGY OVERVIEW

NIST's Computer Security Division, responsible for development and support of the Federal Information Processing Standard (FIPS 201) for Personal Identity Verification of Federal Employees and Contractors has completed the first draft of NIST SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, for public comment. Homeland Security Presidential Directive 12 specified that only organizations whose reliability has been accredited may issue PIV Cards to Federal employees and contractors. The Guidelines describe the tasks to be performed during the certification and accreditation processes, which lead to accreditation and an approval to operate the PIV Card issuing services required in FIPS 201. The Guidelines may be used by Federal agencies in planning and designing their PIV Card issuing services. They may later be used by the agency to self accredit their capability and reliability to provide the services.

NIST Special Publication 800-79 can be accessed from the Drafts Publications page. Comments on SP 800-79 are being solicited until July 10, 2005, from Federal agencies, industrial organizations, public interest groups, and individuals. Comments should be prepared using the Comment Form Template (MS Excel) (16 KB) and the completed Comment Form should then be saved to the memory of the site's computer. The completed comment form should then be attached to a short message stating the name and address of the source of comments, an email address that can be made public, and then e-mailed to PIVaccreditation@nist.gov. Comments received after July 10, 2005 will not be considered when revising SP 800-79. Additional information in question and answer format is available in Questions & Answers about Draft SP 800-79: (Adobe PDF)

2.1 Types of Access Control Systems

This section discusses the security assurance requirements that authentication technologies and techniques can achieve, with particular emphasis on (1) CAC authentication technology components, (2) authentication techniques employed by DOD force protection personnel, and (3) fingerprint and facial biometrics options.

Administrative/Privileged Access
User level access
Limited User access

2.2 Overview of Access Control Technologies

HSPD12 compliance will begin with use of the CAC within DOD. DOD has force protection personnel who can be leveraged to enhance security assurance for personal authentication applications. Biometrics, particularly fingerprint and facial recognition technologies, are required by HSPD12, however, the implementation date is currently under debate. Note that because FIPS201 is currently defining requirements for fingerprint biometrics technology implementation, the contractor will need to stay apprised of corresponding NIST and IAB requirements definition efforts. DOD needs to be prepared to prudently use biometrics technologies either alone or in combination with the CAC to address information assurance. The deliverable for task 2 will be a report discussing the inherent assurance capabilities of CAC

technology components, various authentication techniques to be employed by DOD force protection personnel, and fingerprint and facial recognition biometrics.

2.2.1 Card Access

All federal agencies must process new staff and contractors in accordance with HSPD12 (and the PIV-1 requirements defined by FIPS201) by October 2005. The backlog of existing staff and contractors must have their identities verified in accordance with HSPD12 by October 2007. The deadline for implementation of the biometric verification that is a part of this process (and which will result in storage of finger and facial data on the PIV) is being debated.

2.2.1.1 SMART CARD/CAC

The FIPS201 future-state PIV is not commercially available at this point, but the future desired state of the PIV is defined in FIPS201. Given that the commercial industry develops products to satisfy these requirements, DOD's strategy is to migrate from the currently deployed CAC to the future-state PIV (PIV-2). DOD's ACO has conducted a gap analysis between the CAC and PIV-2. This effort will consider that gap analysis, commercial product announcements, and the research conducted in Tasks 1 and 2 above as input. When the CAC is modified and the STIGs developed in Task 3 above become obsolete, those STIGs will be revised accordingly. The deliverable for Task 4 will be a STIG for the future-state PIV (PIV-2), as supported by industry.

2.2.2 Cipher Locks

2.2.3 Biometric Systems

2.3 Criteria for choosing Access Control Method

All countermeasures will have to be and must be weight against cost of implementation and operational probabilities and possibilities.

Under what conditions should DOD accept PIVs generated by other federal agencies for physical or logical access control?

Which card authentication technologies should be leveraged for given applications?

Under what conditions are combinations of authentication technologies and/or techniques warranted? Which combinations should be employed? For example:

Under what circumstances should the digital photograph printed on the CAC be compared to the cardholder?

Which anti-counterfeit techniques should be validated and under what conditions?

Under what conditions should the digital certificate on the CAC be verified?

How should the CAC be used in off-line applications?

3. PHYSICAL ACCESS

The following section discusses area and cipher access to IT, which is supporting mission critical or essential operations.

3.1 Considerations for Access Control Environments

3.1.1 Commercial Building: Floor or Entire Building

3.1.1.1 Terrorist Threat

Control of vehicle access to the building may or may not be a possibility. Where it can be implemented, suggest control of vehicle traffic to within 25 meters or 81 feet of all sides of the building. A consideration when setting up in a commercial building with parking garage or facilities within the building is the need to control who and what enters and leave if possible. If not possible, consider a building that does not have internal garage. In those cases where there is not a choice and the vulnerability cannot be negated then the risk has to be identified as a known risk.

3.1.1.2 Establishment of a Perimeter

Try to establish a perimeter within the building where the entry/exit can be controlled. It helps diminish the level and complexity of internal area controls.

An ideal situation is to be able to control an entire floor. In this situation, elevators and stairway doors are used to gain access to that floor. An upper floor, which is at least 18 to 20 feet from ground level and roof level, would provide an easily securable environment. Most commercial buildings have windows, which at ground level can be a cause for concern.

If controlling an entire floor or floors is not possible, then try to control a wing of a floor or half of the floor. That way entry/exit controls can be established into the area.

3.1.2 Building on a Government Installation

Government installations need to develop access controls and a standard explosive standoff area for those buildings housing IT mission critical or mission essential equipment. If parking is a problem, then the site will use vehicle control access points and allows the parking of only known vehicles in the area. Access control cards and Personal Identification Numbers (PIN) are required to gain access to the control area.

Sites will establish individual access control at the nearest point to the entry into building or a sub-set area of that building. If possible, establish this control point as far from the perimeter of the classified operations of the building. Again, the ID Card and PIN or a control desk with entry control personnel would be the minimum level. This level controls the possibility of not having the terminal area established at an appropriate open storage level. This level also provides another physical countermeasure, which is the storage of the removable storage devices in GSA containers. SIPRNET ports must be turned off when the area is not occupied.

Finally, establish another control point to the computer room area where encryption and storage devices that are not removable are located. This area must meet minimum requirements of open storage IAW Appendix G, DOD 5200.1-R, DOD Information Security.

3.1.3 Tactical Area

Entry Control must be established for areas housing the enclave server, network, and crypto devices, the classified terminal areas, and the cabling that connects all these devices.

The tighter the control of this classified operation area and the stricter application escorting all personnel who do not have the applicable security clearance lessens the risks to the enclave.

3.2 General Access Control Requirements

3.2.1 Administrative and end user training

3.2.2 Unattended Access

Under what conditions should unattended access to physical spaces or logical information be granted?

3.3 SIPRNet and Classified Environments

3.3.1 Physical Control of Network Ports and Equipment

3.3.2 Physical Control of Removable Devices

3.3.2.1 Management of Storage Devices

Storage devices, such as hard drives must be removable when the area is not approved for open storage of classified information.

3.3.2.2 Management of Type 1 Encryption PC cards and devices

3.4 NIPRNet and Unclassified Environments

Physical Control of Network Ports and Equipment

3.5 Standalone Lab Access Controls

Physical Control of Network Ports and Equipment

4. SYSTEM ACCESS

Transmission must be encrypted or in a Protected Distribution System (PDS) if not encrypted. The level of access controls of an area where PDS is being used, based on security clearance level of personnel allow escorted access to the area, determines the hardness of the PDS and types and frequency of inspections.

4.1 Administrative Access

4.2 SIPRNet Access

4.3 NIPRNet Access

4.4 Standalone Lab Access

This page is intentionally left blank.