Report Number: I733-033R-2006
Date: December 2006

Oracle Application Server Security Recommendations and DoDI 8500.2 IA Controls

Enterprise Applications Division of the Systems and Network Attack Center (SNAC)

Information Assurance Directorate

**National Security Agency
ATTN: I733
9800 Savage Road STE 6704
Ft. Meade, Maryland 20755-6704
410-854-6191 commercial
410-859-6510 facsimile**

This page intentionally left blank

Acknowledgment

We thank the MITRE Corporation for its collaborative effort in the development of this guide. Working closely with our NSA representatives, the MITRE team—John Carlson, Yi-Fang Koh, Harvey Rubinovitz, and Jackson Wynn—generated the security recommendations in this guide.

This Page Intentionally Left Blank

Warnings

This document discusses security guidance for Oracle Application Server 10g Enterprise Edition installed on Windows Server 2003 platforms. The recommendations contained herein are not applicable to other versions of Oracle Application Server, other commercial J2EE application server products, or to other Windows or non-Windows platforms.

Do not attempt to implement any of these recommendations without first testing in a non-operational environment. Application of these recommendations to systems deployed in a production environment may result in loss or corruption of stored data, and/or may temporarily affect the operational status of those systems.

This Page Intentionally Left Blank

Trademark Information

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the U.S.A. and other countries.

Java® is a registered trademark of Sun Microsystems.

All other names are registered trademarks or trademarks of their respective companies.

This Page Intentionally Left Blank

Table of Contents

Table of Tables

Introduction

This document discusses the mapping between security guide recommendations defined in the Oracle Application Server (OAS) Security Guide, referred to as the companion security guide, and IA Controls specified in DoD Instruction 8500.2. IA Controls defined in DoDI 8500.2 specify safeguards and operational restrictions that must be implemented by a DoD information system in order to assure the integrity, availability and confidentiality of the system and its data.

Information systems operated by the Federal government are subject to an alternative set of IA Controls defined in NIST Special Publication 800-53 “Recommended Security Controls for Federal Information Systems”. Analysis of the mapping between OAS Security Guide recommendations and NIST 800-53 IA Controls is out of scope for this document.

Though this document is primarily intended for evaluation of DoD-deployed Oracle Application Server (OAS) systems, many of the security recommendations provided in the companion security guide can be applied to OAS 10g EE systems deployed in a commercial environment. This is so because parallels exist between the DoD and the commercial sector in terms of operational requirements for data integrity, availability and confidentiality. In the commercial sector, high availability is an important requirement for information systems used to generate revenue, e.g., orders processing, financial transaction systems, and etc., just as information systems operating in the commercial sector may impose stringent confidentiality requirements to protect strategic business plans, trade secrets and/or proprietary information.

The organization of this document is as follows. Chapter 1 details DoDI 8500.2 IA Controls that apply to enterprise information systems such as OAS 10g EE. Chapter 2 cross references these IA Controls with security recommendations provided in the companion security guide. It is assumed that the reader is familiar with OAS 10g EE security capabilities, and will refer to the companion security guide for details on the security recommendations discussed herein.

This Page Intentionally Left Blank

Chapter

1

DoDI 8500.2 IA Controls

This chapter discusses DoD Instruction (DoDI) 8500.2 IA Controls. DoDI 8500.2 establishes policies, roles and responsibilities for the application of layered security protections to information systems used within the Department of Defense. These security protections are referred to as IA Controls, which specify safeguards or operational restrictions that must be implemented to assure the integrity, availability or confidentiality of an information system and its data.

DoDI 8500.2 specifies IA Controls in terms of Mission Assurance Categories (MACs). MAC levels characterize operational requirements for system availability and data integrity, and reflect the relative importance or criticality of a system in order to accomplish DoD mission objectives. DoDI 8500.2 specifies three MAC levels, distinguished in terms of the effect(s) of loss of availability:

- MAC I systems handle information vital to the DoD mission; loss of availability would result in immediate and sustained loss of mission effectiveness.
- MAC II systems provide direct support to MAC I systems; sustained loss of availability would seriously degrade mission effectiveness.
- MAC III systems perform day-to-day information processing; however, sustained loss of availability would not affect mission effectiveness.

DoDI 8500.2 also specifies IA Controls for data confidentiality based on the sensitivity of information processed or stored by an information system. DoD information systems that process classified data have more stringent protection requirements than systems that process either Sensitive But Unclassified (SBU) or public data.

The rest of this chapter details the subset of DoDI 8500.2 IA Controls applicable to an enterprise information system, namely Oracle Application Server 10g EE. DoDI 8500.2 contains approximately 130 IA Controls. Many of these controls do not directly apply to a deployed information system, and are omitted, e.g., physical security, personnel security, etc. Similarly, details on concepts, definitions and terminology used in DoDI 8500.2 are omitted and can be obtained directly from reading the DoD Instruction.

DoDI 8500.2 IA Controls by Mission Assurance Category (MAC)

This section enumerates DoDI 8500.2 IA Controls requirements associated with each Mission Assurance Category (MAC) that are applicable to OAS 10g EE.

The following table identifies DoDI 8500.2 IA Controls that apply to all systems.

Table 1. IA Controls for Systems at all Assurance Levels

DCBP-1	The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.
DCCT-1	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.
DCII-1	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.

DCMC-1	Restrictions on the acquisition, development, and/or use of mobile code include the following: 1. Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO cannot be used. 2. For Category 1 mobile code signed with a DoD-approved PKI code signing certificate: use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited. 3. Category 2 mobile code that executes in a constrained environment without access to system resources may be used 4. Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured. 5. Category 3 mobile code may be used. 6. DoD workstation and host software are configured to prevent download and execution of mobile code that is prohibited. 7. Automatic execution of mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.
DCNR-1	Utilize NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.
DCPD-1	Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available.
DCPP-1	DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.
DCPR-1	A configuration management (CM) process is implemented that includes: (1) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and (2) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.
DCSL-1	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.
DCSQ-1	Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.
ECPA-1	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments.
ECRG-1	Tools are available for the review of audit records and for report generation from audit data.
ECSC-1	For Enclaves and AIS applications, all applicable DoD security configuration or implementation guides have been applied.
ECTP-1	The contents of audit trails are protected against unauthorized access, modification or deletion.
ECVP-1	All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.

The following DoDI 8500.2 IA Controls apply to MAC III systems.

Table 2. IA Controls for Non-Critical Information Systems

DCCS-1	A DoD reference document, such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the following are acceptable in descending order as available: • Commercially accepted practices (e.g., SANS); • Independent testing results (e.g., ICSA); or • Vendor literature.
DCSS-1	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.
ECAT-1	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.
ECCD-1	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.
ECND-1	An effective network device (e.g., routers, switches, firewalls) control program is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA).
ECPC-1	Application programmer privileges to change production code and data are limited and are periodically reviewed.
ECSD-1	Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented.
ECTM-1	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).
IAKM-1	Symmetric Keys are produced, controlled, and distributed using NIST-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 certificates or pre-placed keying material.
IATS-1	Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token (when available).

The following DoDI 8500.2 IA Controls apply to mission critical or mission support systems. These systems are referred to as MAC I or MAC II systems, respectively.

Table 3. IA Controls for Mission Critical and Mission Support Systems

DCCS-2	Same as DCCS-1, except if a DoD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.
DCSS-2	Same as DCSS-1. Additionally, Tests are periodically run to ensure the integrity of the system state.
DCPA-1	User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.
DCSP-1	The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.
ECAT-2	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically

	disable the system if serious IA violations are detected.
ECCD-2	Same as ECCD-1. Additionally, access and modification of data is recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.
ECTB-1	The audit records are backed up not less than weekly onto a different system or media than the system being audited.
ECDC-1	Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.
ECID-1	Host-based intrusion detection systems are deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS).
ECND-2	An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.
ECPC-2	Application programmer privileges to change production code and data are limited and reviewed every 3 months.
ECSD-2	Same as ECSD-1. Additionally, change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.
ECTM-2	Same as ECTM-1. Additionally, mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).
IAKM-2	Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.
IATS-2	Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.

DoDI 8500.2 IA Controls by Data Sensitivity Level

This section details DoDI 8500.2 IA Controls for protecting the confidentiality of data processed or stored by DoD information systems.

The following DoDI 8500.2 IA Controls apply to systems that process public data, i.e. data that is neither sensitive nor classified.

Table 4. IA Controls for Public data

DCSR-1	At a minimum, basic-robustness COTS IA and IA-enabled products are used to protect publicly released information from malicious tampering or destruction and ensure its availability. The basic-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Basic Robustness published under the IATF.
EBBD-1	1. Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network. 2. Internet access is permitted from a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means. 3. All Internet access points are under the management and control of the enclave.

EBPW-1	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ)
ECAR-1	Audit records include: - User ID. - Successful and unsuccessful attempts to access security files. - Date and time of the event. - Type of event.
ECAT-1	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.
ECLP-1	Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.
ECMT-1	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures, such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

The following DoDI 8500.2 IA Controls apply to systems that process non-public data, i.e. data that is either sensitive or classified.

Table 5. IA Controls for Non-Public data

EBRP-1	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.
EBRU-1	All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.
ECAN-1	Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access: • **Open access** to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction. • **Controlled access** to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction. • **Restricted access** to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions.
ECLP-1	Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is

	limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.
ECML-1	Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.
ECNK-1	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality – data in transit).
ECRC-1	No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object.
IAAC-1	A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.

The following DoDI 8500.2 IA Controls apply to systems that process sensitive data.

Table 6. IA Controls for Sensitive but Unclassified (SBU) data

DCSR-2	At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.
EBBD-2	1. Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and at layered or internal enclave boundaries and at key points in the network, as required. 2. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.
EBPW-1	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ)
ECAR-2	Audit records include: - ECAR-1 data - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system.
ECAT-1	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.
ECCR-1	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.
ECCT-1	Sensitive But Unclassified (SBU) data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2)
ECLO-1	Successive logon attempts are controlled using one or more of the following: - access is denied after multiple unsuccessful logon attempts. - the number of access attempts in a given period is limited. - a time-delay control system is employed. If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon

	sessions.
ECMT-1	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures, such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.
IAIA-1	1. Guidelines for passwords: - Must be 8-characters in length or longer - Must include at least one of each: upper case, lower case, numeric and special characters - To the extent system capabilities permit, system mechanisms enforce automatic expiration of passwords and prevent password reuse - Passwords are encrypted both for storage and for transmission. - All factory set, default or standard-user IDs and passwords are removed or changed. - At least four characters must be changed when a new password is created. 2. Passwords and other authenticators are protected commensurate with the classification or sensitivity of the information accessed: - Passwords are not shared - Passwords are not embedded in access scripts, or stored on function keys

The following DoDI 8500.2 IA Controls apply to systems that process classified data.

Table 7. IA Controls for Classified data

DCSR-3	Only high-robustness GOTS or COTS IA and IA-enabled IT products are used to protect classified information when the information transits networks that are at a lower classification level than the information being transported. High-robustness products have been evaluated by NSA or in accordance with NSA-approved processes. COTS IA and IA-enabled IT products used for access control, data separation or privacy on classified systems already protected by approved high-robustness products at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.
DCSS-2	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are periodically run to ensure the integrity of the system state.
ECAR-3	Audit records include: - ECAR-2 data - Data required to audit the possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information.
ECAT-2	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically disable the system if serious IA violations are detected.
ECCD-2	Same as ECCD-1. Additionally, access and modification of data is recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.
ECLC-1	The system automatically records the creation, deletion, or modification of confidentiality or Integrity labels, if required by the information owner.
ECLO-2	Successive logon attempts are controlled using one or more of the following: - access is denied after multiple unsuccessful logon attempts.

	- the number of access attempts in a given period is limited. - a time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon
ECMT-2	Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.
ECTB-1	The audit records are backed up not less than weekly onto a different system or media than the system being audited.
IAKM-3	Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.

Chapter

2

Mapping of DoDI 8500.2 IA Controls to OAS Security Recommendations

This chapter maps DoDI 8500.2 IA Controls identified in the previous chapter to the recommendations provided in the companion security guide.

A one-to-one mapping between security guide recommendations and DoDI 8500.2 IA Controls is not possible. Certain security guide recommendations are not addressed by DoDI 8500.2 IA Controls. Security guide recommendations to restrict caching of volatile data by the OAS Web Cache, for example, have no corresponding IA Control. In addition, guide recommendations for selecting encryption algorithms and encryption key sizes based on the sensitivity of data are not specifically addressed in DoDI 8500.2.

Conversely, the companion security guide omits areas that are addressed by DoDI 8500.2 IA Controls. Product robustness, discussed in IA Controls [DCSR-1,2,3], is a non-configurable property that is inherent in OAS 10g EE software. This facet of the OAS product is not discussed in security guide recommendations. In addition, restrictions on the use of mobile code [DCMC-1] apply to Oracle application and content development, which was also considered out-of-scope for the security guide.

Security Recommendations from the OAS Security Guide

Overview

❑ For sensitive data, use of SSL can be an effective mitigation for many common communications vulnerabilities [ECCT-1].

❑ Select cryptographic algorithms and encryption key sizes based on the sensitivity of the data that must be protected.

❑ Develop or deploy Oracle Partner applications, which can take advantage of Oracle identity management capabilities for storing and managing password information [IAAC-1].

❑ Enforce “strong” authentication using client-side certificates for systems that process highly sensitive data [IATS-1].

❑ Limit and periodically review user membership to predefined Oracle administrative groups. Restrict user access to Oracle administrative accounts created during product installation.

❑ Practice the principle of least privilege when granting permissions to new administration groups or roles [ECLP-1].

OAS Deployment Considerations

❑ Deploy an external firewall and DMZ to isolate the enterprise network from the external environment. Deploy additional firewalls to provide greater protection for repositories containing sensitive data [EBBD-1,2,3][EBPW-1].

- ❑ Configure firewalls to restrict network traffic based on the protocols utilized by OAS products allocated within established protection zones.
- ❑ Enable SSL to protect information in transit through protection zones where threats exist and where the risk of compromise is high [ECCT-1].
- ❑ Look for opportunities to organize content so that sensitive data can be isolated and separately protected [ECAN-1].
- ❑ Verify that OAS 10g EE meets applicable NIST and/or CNSS cryptographic guidelines appropriate for the enterprise environment in which the system is being deployed [DCNR-1].
- ❑ If AES is required, contact Oracle technical support for information about compatible, FIPS-certified cryptographic libraries for use with OAS 10g EE [DCNR-1].
- ❑ Set the SQLNET.SSLFIPS parameter in the sqlnet.ora configuration file to TRUE in order for OAS 10g EE to operate in FIPS compatibility mode [ECSC-1] [DCNR-1].
- ❑ Install X.509 certificates for each server on which OAS product components are installed. In addition, install an X.509 certificate for each client if the deployment is required to utilize certificate-based authentication and/or SSL using client side certificates [IATS-1].
- ❑ Deploy OAS Web Cache to a standalone, dedicated server to avoid potential resource conflicts with other OAS product components.
- ❑ Enable only Apache software modules on an OAS HTTP Server that are minimally necessary in order for the system to be mission effective [DCSQ-1].
- ❑ Verify that web content development is a mission objective before deploying web server tier system(s) with OAS Portal installed [DCSQ-1].
- ❑ Never deploy OAS product components on the same host platform as Microsoft Active Directory
- ❑ Refer to Oracle product documentation for guidance on deploying OAS product components in clustered configurations.
- ❑ Deploy multiple OAS Web Caches in a clustered configuration when high availability is required.
- ❑ Consider deployment options that include full or partial replication of the OID directory tree and/or installation of Oracle Identity Management to redundant servers configured as an OAS cluster.

OAS Installation

- ❑ Restrict access to the Oracle installation directory, its subdirectories and the directory containing Oracle database files to administration personnel only [DCSL-1] [ECCD-1].
- ❑ Modify default port assignments in staticports.ini prior to installing OAS [DCPP-1].
- ❑ Review installation logs to verify that OAS installed correctly. Delete installation logs once reviewed, or restrict their access to administration personnel only [ECTP-1].
- ❑ Modify the XML start-mode attribute in the opmn.xml configuration file to ensure that SSL is enabled for the HTTP Server at startup [DCSS-1].
- ❑ Apply the appropriate Windows security template after OAS product components have been successfully installed [ECSC-1].
- ❑ Install only Oracle Identity Management when deploying the infrastructure tier into an enterprise environment where the Metadata Repository is already deployed.

❑ Install only infrastructure tier product components that are required in order for the system to be mission effective [DCSQ-1].

❑ Assign strong, unique passwords for administration databases created during the installation process [ECPA-1][IAIA-1].

❑ Assign a strong password for the ias_admin administration account [ECPA-1][IAIA-1].

❑ Change the default port assignment for the Oracle Database Listener to obscure this well-known port-to-protocol mapping [DCPP-1]

❑ Restrict access to the Oracle Database Listener by enabling TCP valid node checking and by specifying IP addresses for servers that have OAS web server, portal and infrastructure tier components installed.

❑ As with the infrastructure tier, install only web tier product components that are required in order for the system to be mission effective [DCSQ-1].

❑ Select the configuration option “Only use SSL connections with the Oracle Internet Directory” to protect user account information transferred between OID and the web server tier via LDAP [ECNK-1].

❑ Once installation is completed, assign strong passwords to all portal administration accounts [ECPA-1][IAIA-1].

❑ Once installation is complete, change default passwords assigned to each Database Access Descriptor (DAD), and specify strong passwords as described in Chapter 6 of the companion security guide [ECPA-1][IAIA-1].

❑ Restrict read access to the dads.conf configuration file to administrators only [ECCD-1].

❑ Upon installation of the OAS Portal, verify that the dads.conf configuration file excludes the following packages of PL/SQL stored procedures:

- PlsqlExclusionList sys.*
- PlsqlExclusionList dbms_*
- PlsqlExclusionList utl_*
- PlsqlExclusionList owa_util.

❑ Refer to product security updates and vendor configuration guidance for updated information regarding documented PL/SQL vulnerabilities.

❑ To prevent unauthorized access to cached portal content, configure the portal cache directory to restrict file access to cached pages [ECCD-1].

❑ Select the configuration option “Only use SSL connections with the Oracle Internet Directory” to protect user account information transferred between OID and the OAS Web Cache via LDAP [ECNK-1].

OAS HTTP Server

Virtual Hosts

❑ To minimize the use of security configuration overrides by virtual hosts, co-locate virtual hosts containing sensitive content on OAS HTTP Servers configured to protect sensitive content, and virtual hosts containing non-sensitive content on OAS HTTP Servers configured to host non-sensitive content.

❑ In cases where the virtual host is configured to override the default security settings of the OAS HTTP Server, verify that the virtual host is configured to adequately protect its content based on the sensitivity of that content.

- ❑ In cases where the virtual host does not override the default security settings of the OAS HTTP Server, verify that default OAS HTTP Server security settings are sufficient to protect the content provided by that virtual host.

Apache Software Modules

- ❑ Disable Apache software modules that are not required [DCSQ-1].
- ❑ Only install and enable software modules obtained directly from Oracle [DCPD-1].
- ❑ Do not restrict access to content based on the IP address of the client.
- ❑ Enable the mod_osso software module in order for Oracle partner applications to utilize Oracle SSO authentication capabilities [DCBP-1].
- ❑ Enable the mod_auth software module so that external applications, which cannot utilize SSO authentication functions, can utilize Apache-supported user authentication capabilities.
- ❑ Enable the mod_ossl module in order to utilize SSL capabilities to protect sensitive data [ECCT-1].
- ❑ Enable mod_certheaders if certificate-based, client authentication is performed through the OAS Web Cache [IATS-1].
- ❑ Do not utilize mod_proxy with both forward and reverse proxy functions enabled at the same time. Enable forward proxy capabilities only if restrictions are defined to limit access to internal web servers.
- ❑ Do not use the open source version of mod_security that is bundled with OAS 10g EE in lieu of commercial-grade IDS solutions [DCPD-1].

Directory and File Access

- ❑ Restrict user access to directories where OAS HTTP Server log information is physically stored in order to protect logging data from accidental or malicious modification or deletion [ECTP-1].
- ❑ Restrict access to the OAS HTTP Server configuration files httpd.conf and ssl.conf to system administrators only [ECCD-1][ECAN-1].
- ❑ When changing default directory locations used by the OAS HTTP Server, verify that access permissions for the new directory locations restrict access to administration personnel [ECCD-1][ECAN-1].

OAS HTTP Server Configuration Directives

- ❑ Use the Timeout directive to specify a timeout value in the range 60-120 seconds, which is adequate for most deployments.
- ❑ Set ExtendedStatus to Off unless required for performance tuning. If enabled, use the Allow from and Deny from directives to restrict access to the HTML output.
- ❑ Use the Port directive to configure standalone HTTP Servers to listen on a port other than the default port [DCPP-1].
- ❑ Use the Listen directive to configure the HTTP Listener to utilize a port other than the default port [DCPP-1].
- ❑ Use the Directory directive to restrict user access to file system locations containing web content, and to ensure that only authenticated users can view information contained in these directories [ECAN-1].
- ❑ Do not use .htaccess files to specify access control information.

❑ Specify the client's hostname rather than its IP address when restricting access using the Allow from or Deny from directives.

❑ At a minimum, configure the LogFormat directive so that the following information is logged for each HTTP request:

- The date and time of the request
- The host name and/or IP address of the client
- The URL accessed, [ECAR-1].

❑ For systems that host sensitive content, configure the LogFormat directive to record additional information required for periodic audit reviews and/or forensic analysis [ECAR-1,2,3].

❑ Periodically review OAS HTTP Server logs in accordance with applicable security policies [ECAT-1].

❑ For deployments in which OAS Web Cache is running, set UseWebCacheIP to On to ensure that client IP addresses are property logged by the OAS HTTP Server [ECAR-1].

OAS HTTP Server SSL Directives

❑ Use the SSLCARevocationFile directive to specify the filename of the Certificate Revocation List (CRL) and assign file permissions that restrict access to administrators only [ECCD-1].

❑ Use the SSLCARevocationPath directive to specify the file system directory where the CRL file is stored and assign directory permissions that prohibit access to all users [ECCD-1].

❑ Set the SSLCipherSuite directive to 'ALL:!ADH:!EXPORT56:+HIGH:+MEDIUM-SSLv2' to eliminate use of low-strength ciphers and SSLv2 [DCNR-1].

❑ Set the SSLEngine directive to On if use of SSL is required [ECCT-1].

❑ Use the SSLLog directive to specify the file where SSL logging information will be stored and assign file permissions that prohibit access by all users [ECTP-1].

❑ Use the SSLLogLevel directive to set the logging level to collect logging information as needed [ECAR-1,2,3].

❑ Set the SSLMutex directive to sem to enable use of locking semaphores.

❑ With the SSLOptions directive, do not enable the FakeBasicAuth option, which allows unauthenticated access to a directory.

❑ Set the SSLProtocol directive to ALL –SSLv2 to disable use of SSLv2 protocol [DCNR-1].

❑ Do not use the SSLRequire directive to conditionally enable use of SSL. Enable use of SSL using the SSLEngine directive, based on the sensitivity of the data.

❑ Enable the SSLRequireSSL directive to force clients to use SSL when accessing a directory [ECCT-1].

❑ Enable the SSLVerifyClient directive if certificate-based client authentication is required [IATS-1].

❑ Use the SSLWallet directive to specify the location of the Oracle wallet, and assign directory and file permissions to prohibit access to all users [ECCD-1].

OAS Portal

- ❑ Enable use of SSL throughout the OAS Portal for deployments that handle or process sensitive information [ECCT-1][ECNK-1].
- ❑ Limit the granting of Manage Content privileges to Oracle users [ECLP-1].
- ❑ Enable the Approvals and Notifications page group property for all page groups that potentially incorporate sensitive content [ECSD-1][ECML-1].
- ❑ Enable the Override Approval Process page group property only when content published to the page group carries no risk for disclosure of sensitive information, or when content developers are qualified to perform page approvals.
- ❑ If a page approval process is enabled, ensure that the list of approvers includes qualified security review personnel.
- ❑ Enable the Display Page to Public page property only when content published to the page carries no risk for disclosure of sensitive information [ECML-1].
- ❑ Do not enable item level security for a portal page if that page implements functions intended exclusively for a single user, group or functional role.
- ❑ Create functional groups or roles that grant page item read or write access. Assign user membership to these functional groups based on the level of privileges that they require [ECPA-1][ECLP-1].
- ❑ Limit the granting of the manage page item privilege to Oracle users other than the page owner and page item creator [ECLP-1]
- ❑ Set the expiration period of a page item to be consistent with the volatility of the information it contains. Continued publication expired or out-of-date information diminishes the integrity of the system.
- ❑ To restrict access to content through Oracle Ultra Search, assign an ACL to each data source and specifies only those users and groups for which access is granted [ECAN-1].
- ❑ Assign strong passwords to pre-defined OAS Portal administration accounts. Limit access to Portal administration passwords, and limit user membership in OAS Portal administration groups such as DBA and PORTAL_ADMINISTRATORS [IAIA-1].
- ❑ If portal user self-registration is enabled, ensure that an approval process is established to evaluate registration requests relative to need-to-know access restrictions that are being enforced [ECPA-1].
- ❑ Review the set of privileges assigned to each Portal user and administration account to ensure that the right combination of privileges is being granted [ECLP-1].
- ❑ Limit and periodically review global privileges granted to OAS Portal users [ECLP-1].

OAS Web Cache

- ❑ Governing security policies may require user authentication based on client certificates. If so, configure the OAS Web Cache to require client-side certificates [IATS-1].
- ❑ Verify that OAS Web Cache and OAS HTTP Server are configured to accept and receive IP address and/or client certificate information from external users, as required [IATS-1]
- ❑ If sensitive content is delivered through the OAS Web Cache, enable use of SSL between the OAS Web Cache and external users [ECCT-1].

❑ Consider the tradeoff between throughput performance and the need to protect sensitive content transferred between each origin server and the OAS Web Cache, on a case-by-case basis.

❑ Enable use of HTTPS when configuring the OAS Web Cache to access an origin server that provides sensitive content, or when governing security policies require end-to-end protection of data as a mitigation strategy for insider threats [ECNK-1].

❑ If the OAS Web Cache is configured to cache both sensitive and non-sensitive content, regard all cached data as sensitive content stored in a high threat environment.

❑ Configure the OAS Web Cache with caching rules to restrict caching of sensitive information [ECRC-1].

❑ Verify that the use of HTTP Surrogate-Control header directives is consistent with security policies for restricting the caching of sensitive content [ECRC-1].

❑ If caching of dynamic content is required, define expiration rules that establish expiration timeframes consistent with the volatility of the content.

❑ Verify that the use of HTTP Surrogate-Control header directives in web pages containing dynamic content is consistent with security policies that define enterprise data integrity requirements regarding access to stale dynamic content.

OAS Identity Management

❑ Enable password policy settings to require a user to supply their original password when changing their password.

❑ Set the Password Expiry Time to 42 days, which is the standard password expiration period defined in NSA/Windows security templates [IAIA-1].

❑ Use the Reset Password upon Next Login policy setting to periodically force users to reset account passwords [IAIA-1].

❑ Enable the Use Reversible Encryption password policy setting only when synchronization between OID and Microsoft Active Directory requires exchange of user password information.

❑ Set the Global Lockout Duration and IP Lockout Duration password policy settings to 15 minutes, which is the standard lockout period defined in NSA/Windows security templates [ECLO-1].

❑ Reduce the Password Maximum Failure and IP Lockout Maximum Failure password policy settings from 10 attempts to 3 attempts [ECLO-1].

❑ Set the Minimum Number of Characters in Password policy setting to a value between 8 and 12 characters; use longer passwords in deployments where sensitive data is processed [IAIA-1].

❑ In the absence of capabilities that enforce use of uppercase and/or special characters in passwords, increase the Number of Numeric Characters in Password policy setting from 1 numeric character to 3 numeric characters [IAIA-1].

❑ Set the Number of Passwords in History policy setting to 24 passwords, which is the standard history length defined in NSA/Windows security templates [IAIA-1].

❑ Verify that the export connector profile omits from its mapping all sensitive OID user account attributes that are not intended to be exported to Active Directory.

❑ Enable secure LDAP to protect user account data being synchronized between OID and Microsoft Active Directory [ECNK-1].

- ❑ Verify that valid X.509 certificates are installed in the Microsoft domain controller that is hosting the Active Directory service, which OID is to synchronize with, and in the Oracle Wallet utilized by with Oracle Directory Integration and Provisioning (DIP) service [IATS-1].
- ❑ Enable secure LDAP if password reversible encryption is utilized [ECNK-1].
- ❑ Verify that Windows directory permissions restrict access to OID management tools to Windows administration personnel [DCSL-1].
- ❑ To configure OID auditing to monitor the system for unauthorized access, enable the following OID audit configuration options:
  - ■ Superuser login
  - ■ Bind unsuccessful
  - ■ Access Violation
- ❑ When directory auditing is enabled, periodically review audit data generated by the Oracle Directory Manager tool [ECRG-1][ECAT-1].
- ❑ Use the Oracle Directory Manager tool to configure OID to disable anonymous binding [ECCD-1].
- ❑ Apply the grantrole.ldif configuration file when configuring OID 10g EE to synchronize user account data with Microsoft Active Directory.
- ❑ . Limit use of the Oracle Directory Manager tool for modifying OID directory ACLs.
- ❑ Verify that SSL is enabled for OAS administration web pages, especially web pages used to configure the SSO Server or Oracle partner applications, or to access OID user account data [ECCT-1][ECNK-1].
- ❑ Restrict and periodically review user membership in Oracle administration groups, especially global and realm administration groups, which may grant authority over significant numbers of Oracle users [ECLP-1].
- ❑ Verify that pre-defined administration roles meet operational requirements of the target deployment. If a new role must be created, make sure that only the minimum set of privileges required for that role is granted to it. Periodically review the assignment of Oracle users to roles that grant administrative privileges [ECLP-1].
- ❑ Assign strong passwords to pre-defined Oracle administration accounts. Restrict access to administration password information and take steps to prevent its unauthorized disclosure [IAIA-1],
- ❑ If OAS Portal is not installed, disable the PORTAL and PORTAL_ADMIN administration accounts to reduce the risk of unauthorized users gaining administrative access. [ECPA-1].