DATABASE

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 8, Release 1

19 September 2007

Developed by DISA for the DoD

Trademark Information

Microsoft, Windows, and Windows server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

TABLE OF CONTENTS

Page

SUMMARY OF CHANGES VII

1. INTRODUCTION 1

1.1 Background 1
1.2 Authority 2
1.3 Scope 2
1.4 Writing Conventions 2
1.5 Vulnerability Severity Code Definitions 3
1.6 DISA Information Assurance Vulnerability Management (IAVM) 3
1.7 STIG Distribution 4
1.8 Document Revisions 4

2. COMMON DATABASE SECURITY ELEMENTS 5

2.1 Introduction 5
2.2 Authentication 6
2.2.1 Database user accounts 6
2.2.2 Password Authentication 7
2.2.3 Certificate Authentication 8
2.2.4 External authentication 8
2.2.5 Credential Storage 8
2.2.6 Other Connection Data Storage 9
2.3 Database Authorizations 9
2.3.1 Default Database User Accounts 11
2.4 Confidentiality 11
2.5 Data Integrity 12
2.6 Audit 12
2.7 Replication and Federation 14
2.8 Database Clustering 15
2.9 Backup and Recovery 15
2.10 Operating System Protections 16
2.11 Application Protections 17
2.12 Network Protections 18

3. DATABASE SECURITY REQUIREMENTS 19

3.1 Security Design and Configuration 20
3.1.1 Procedural Review (DCAR) 20
3.1.2 Configuration Specifications (DCCS) 20
3.1.3 Compliance Testing (DCCT) 21
3.1.4 Functional Architecture for AIS Applications (DCFA) 21
3.1.5 Non-repudiation (DCNR) 24
3.1.6 Partitioning the Application (DCPA) 24
3.1.7 Ports, Protocols, and Services (DCPP) 25

3.1.8 Configuration Management (CM) Process (DCPR) ... 25
3.1.9 IA Documentation (DCSD) ... 25
3.1.10 System Library Management Controls (DCSL) ... 26
3.1.11 Security Support Structure Partitioning (DCSP) ... 26
3.1.12 System State Changes (DCSS) ... 26
3.1.13 Software Baseline (DCSW) ... 27
3.2 Identification and Authentication ... 27
3.2.1 Group Identification and Authentication (IAGA) ... 27
3.2.2 Individual Identification and Authentication (IAIA) ... 27
3.2.3 Key Management (IAKM) ... 29
3.2.4 Token and Certificate Standards (IATS) ... 29
3.3 Enclave and Computing Environment ... 30
3.3.1 Access for Need-to-Know (ECAN) ... 30
3.3.2 Audit Record Content (ECAR) ... 30
3.3.3 Audit Trail, Monitoring, Analysis and Reporting (ECAT) ... 31
3.3.4 Changes to Data (ECCD) ... 31
3.3.5 Encryption for Confidentiality - Data at Rest (ECCR) ... 32
3.3.6 Encryption for Confidentiality - Data in Transit (ECCT) ... 32
3.3.7 Data Change Controls (ECDC) ... 32
3.3.8 Interconnections among DoD systems and Enclaves (ECIC) ... 33
3.3.9 Audit of Security Label Changes (ECLC) ... 33
3.3.10 Logon (ECLO) ... 33
3.3.11 Least Privilege (ECLP) ... 34
3.3.12 Marking and Labeling (ECML) ... 36
3.3.13 Conformance Monitoring and Testing (ECMT) ... 36
3.3.14 Privileged Account Control (ECPA) ... 36
3.3.15 Production Code Change Controls (ECPC) ... 37
3.3.16 Resource Control (ECRC) ... 37
3.3.17 Audit Reduction and Report Generation (ECRG) ... 37
3.3.18 Audit Record Retention (ECRR) ... 37
3.3.19 Security Configuration Compliance (ECSC) ... 38
3.3.20 Software Development Change Controls (ECSD) ... 38
3.3.21 Audit Trail Backup (ECTB) ... 38
3.3.22 Audit Trail Protection (ECTP) ... 39
3.3.23 Warning Message (ECWM) ... 39
3.3.24 Account Control (IAAC) ... 39
3.4 Enclave Boundary Defense ... 39
3.4.1 Boundary Defense (EBBD) ... 39
3.4.2 Remote Access for Privileged Functions (EBRP) ... 40
3.5 Continuity ... 40
3.5.1 Protection of Backup and Restoration Assets (COBR) ... 40
3.5.2 Data Backup Procedures (CODB) ... 41
3.5.3 Disaster and Recovery Planning (CODP) ... 41
3.5.4 Backup Copies of Critical Software (COSW) ... 41
3.5.5 Trusted Recovery (COTR) ... 41

3.6 Vulnerability and Incident Management 41
3.6.1 Vulnerability Management (VIVM) 41

LIST OF TABLES

Table 1-1. Vulnerability Severity Code Definitions 3
Table 1-2. Database Vulnerability Severity Code Definitions 3

SUMMARY OF CHANGES

This document has been rewritten in its entirety.

This page is intentionally left blank.

1. INTRODUCTION

This *Database Security Technical Implementation Guide* (STIG) is published as a tool to assist in the improvement of the security of Department of Defense (DoD) information systems utilizing database management systems (DBMS). This document provides general guidance to apply to any DBMS. Security configuration for specific vendor products is provided in the related Database Checklist. This document is not intended to be used to configure database applications such as Microsoft Access that are designed to be used by a single user or a small number of users. Due to their limited security and integrity capabilities these desktop database applications are not recommended where access to and security of the data is critical. Security guidelines for securing single-user or workgroup-user databases are included in the *Desktop Applications STIG*.

This document is meant for use in conjunction with the database host platform Operating System (OS) STIG as well as other Defense Information Systems Agency (DISA) STIGs related to the requirements of any applications accessing the database. Most often other STIGs that should be used in conjunction with this STIG include the *Application Security and Development STIG*, *Web Server STIG*, and the *Network STIG*. Where authentication to the database occurs using a directory service, integration between database and directory services must be configured in accordance with the *Directory Services STIG*.

The most effective way to improve security in DoD database systems is to include security in the initial design and development of the application accessing the database. To that end, this document is also intended to be useful to application program managers/developers in the design phase of DoD applications. As such, it provides the technical security policies, requirements, and implementation details for applying security concepts to the use of database systems by an application.

1.1 Background

With the proliferation of public access to sensitive data previously protected within private networks and the improvement of network security controls, malicious attacks against web applications accessing backend databases has increased. For some time, Structured Query Language (SQL) injection attacks that take advantage of vulnerable applications and their fully-privileged access to the backend database have provided the means for many cases of privacy and financial loss. By exercising the security capabilities of the DBMS, many such attacks can be thwarted. If the application is designed to use rather than bypass the native database security mechanisms, then the overall protection of the data is considerably improved.

This STIG presents the known security configuration items, vulnerabilities, and issues required to be addressed in accordance with DoD policy. In addition to this STIG, compliance validation tools and checklists are available to customers to assist in the efforts to implement the required configuration.

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.

It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

1.3 Scope

This document applies to all DBMSs presently in use within DoD. Requirements specific to a particular product are provided in the Database Security Checklist. All requirements in this document are meant to apply to any DBMS on any host operating system. This STIG does not apply to database products designed primarily to support single-user, standalone database applications. Single-user database products may be provided as part of a desktop application suite such as Microsoft's Office products. Security for these products is addressed in the *Desktop Application STIG*. However, this STIG does apply to distributable versions of DBMSs intended to support distributed applications such as Microsoft’s MSDE/SQL Express. This STIG also assumes accessibility to the database for configuration. Where databases are embedded within an application and access to the database is not possible except via the supported application, this STIG cannot be applied. Instead, the security of an embedded database must be reviewed as an application component in accordance with the *Application Security and Development STIG*.

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**” indicates 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.

Each policy bullet includes the STIG Identifier (SDID) in parentheses that precedes the policy text and references the corresponding vulnerability check in the SRR Checklist and Vulnerability Management System (VMS). An example of this will be as follows: "(*G111: CAT II*)." If the item presently does not have an STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*"). Throughout the document

accountability is directed to the IAO to "ensure" a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.
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. All reasonable attempts to meet this criterion will be made.

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.

Table 1-1. Vulnerability Severity Code Definitions

Below are the severity code definitions interpreted for databases:

Category I	Vulnerabilities that allow immediate unauthorized database administrator privileges to the DBMS, immediate unauthorized access to unencrypted sensitive data stored within the DBMS, immediate unauthorized privileged access to the host server services, data, or objects via the DBMS, or immediate access to or via the DBMS that could lead to a compromise of required DBMS audit trail data.
Category II	Vulnerabilities that contribute to any unauthorized access to the DBMS administrative privileges, data stored within the DBMS, the supporting host services and objects, or that may compromise the integrity of the audit trail.
Category III	Vulnerabilities that have some potential to contribute to any unauthorized access to the DBMS administrative privileges, data stored within the DBMS, the supporting host services and objects, or may compromise the integrity of the audit trail.

Table 1-2. Database 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 vulnerabilities and alerts require 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: https://www.jtfgno.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. COMMON DATABASE SECURITY ELEMENTS

2.1 Introduction

A DBMS provides several capabilities that control or affect the security of the data stored within its files. This section lists and discusses the variety of security items that are most commonly found in DBMSs. The security of the DBMS depends upon how well each of these items is addressed and configured. These security items are presented in this section for use as general guidelines for reviewing the security of any DBMS. Section 3 of this document presents the security requirements for DBMSs within DoD based on DoD IA policies.

The list of DBMS security capabilities includes:

- Authentication – the DBMS may provide its own authentication mechanism or use the host operating system or another external authentication system such as a directory service to identify and authenticate users.
- Authorization – the DBMS provides three types of privileges: 1) privileges that control the definition of data and application objects; 2) privileges to access and manipulate the data stored within the database objects; and 3) privileges to administer the database configuration and operation. Access to database resources including storage and memory usage may also be assignable.
- Confidentiality – the DBMS may provide the capability to encrypt data and applications within the data files. It may also provide encryption of network communications to the database.
- Integrity – the DBMS provides mechanisms to validate data before storage, maintain the integrity of data relationships, recover data to a known reliable state when interruptions occur (rollback), log changes to data items, and control simultaneous actions by different users to the same data.
- Audit – the database provides auditing of privileged operations and changes to data.
- Backup and Recovery – the database provides mechanisms to recover from loss or corruption of the database data and software.

The application may also require that the database take advantage of one or more of the following remote database features:

- Replication – part or all of the database data objects may be copied and maintained in a separate remote database.
- Federated or distributed databases – these provide access to data stored in remote databases to local database users and applications.
- Database clustering – database clustering provides high-availability to data by providing instant access to duplicate databases in the event of access failure to a primary database.

A DBMS is typically used as a component of an application to store and report data. As such, security of the data stored in the database depends upon the security configuration of many supporting external elements including:

- The host operating system – the host provides protection of the database software and data files, network access to the database, and is also used to protect itself against vulnerabilities the database may introduce to it.
- The database front-end application – the application provides a path from a client to the data in the database. If the application does not include security in its design, it can provide fully-privileged, un-audited access to the database and data to which it connects.
- Network protections – databases accessible via network communications require protections provided by network devices and applications.
- The web and/or application server – web servers provide access to the applications that connect to the backend database. The web server or the application server that provides the security framework for all hosted web applications may control access to the served applications.
- Other database component services – the DBMS installation may come with optional services that operate externally from the database including Simple Network Management Protocol (SNMP) agents, reporting services, email or Simple Mail Transport Protocol (SMTP) agents, etc.

The security of data in the database depends upon all of these elements. Each introduces vulnerabilities to the DBMS as well as provides methods to protect the DBMS and should be considered as contributors to the overall security posture of the database.

2.2 Authentication

Identification and authentication (I&A) provide the foundation for access control. DBMSs provide standard mechanisms for identifying and authenticating users. Users are identified to the database as database accounts and may be identified via the host operating system, a directory service, a network authentication service, or by the database itself. The DBMS is likely to support many methods for providing evidence of identity including, but not always limited to passwords, certificates, and tokens.

2.2.1 Database user accounts

Database users are defined to the database using database accounts. The DBMS may allow for the mapping of database account names to external authentication services including directory servers, operating system, Kerberos, or other accounts. The database account name may be the same as the external account name.

For the purposes of this document, database user accounts are defined as belonging to one of the following functional categories:

- Application User – is accessed by an interactive user and requires only access to read (select), insert, update, or delete data in existing database tables. These are referred to as Database Manipulation Language (DML) actions.
- Database Administrator (DBA) – for the purposes of this document, the database administrator is defined as the responsible account category for configuring and

operating the database. The DBA has full privileges to all objects and resources in the database and can manage all users in the database.

- Application Owner – an application owner account owns all objects defined and used by an application. The application owner defines application roles and assigns user object privileges to the application objects to the application roles. Application owner privileges are restricted to creation, deletion (dropping), or altering of database objects (commonly referred to as Database Definition Language (DDL) actions).
- Application User Manager – an application user manager has the privileges to create and manage application users within the database and assign application roles to application users.
- Application Account – an application account is a specialized user account and is not accessed by interactive users. An application account is used by an application, service, or local batch job. It may have special restrictions to restrict access for its use due to elevated privileges assigned to perform privileged functions.
- Database Auditor – A database auditor account is defined for use to manage database auditing records. Use and assignment of a database auditor account allows there to be a separation of duties between database and auditing and database administrator activities. Without this separate account assignment, DBA actions cannot be reliably monitored.
- Database Operator – this type of database may be assigned limited administrative privileges to support operation functions such as backup and database startup.

The category of the account created plays an important role in assigning privileges within the database as discussed later in this document.

Database account management, as with operating system and other account management, is critical to restricting access to authorized users of the database and must be diligently maintained and managed. Unused, expired, or unauthorized accounts left active in the database provide opportunity for undetected access attempts. Use of available automated controls such as account locking after a number of failed logins can help protect against attacks aimed at unauthorized access to accounts and should be employed when available.

2.2.2 Password Authentication

Most databases support username/password authentication. Although DoD requires authentication using DoD Public Key Infrastructure (PKI) certificates, some databases may not support it. Where passwords are used, password management is a necessity. Password management includes configuring mandatory password specifications for complexity, reuse, expiration, and encryption. Use of passwords for authentication also requires that the login sequence be encrypted. Many native DBMS connection protocols provide this encryption, but some do not or do not use or provide a strong encryption method.

Where applications manage usernames and passwords to authenticate application users, the responsibility for password management and protection falls to the application. Application protection of passwords is reviewed during an application security review.

2.2.3 Certificate Authentication

Some DBMS's provide a native capability for the database to identify itself to clients and to authenticate users to the database using certificates. Others depend upon the host OS or a directory service to provide certificate-based authentication. If a certificate authentication method native to the database is used, it must carefully be configured to meet certificate validation and protection requirements. Self-signed certificates are not secure and should not be used.

2.2.4 External authentication

Authentication to the database may occur by exercising a trust defined between the DBMS and the external authentication service. Most frequently used for this purpose are operating system and directory service authentication.

When operating system authentication is used, the user authenticates to the host operating system and the DBMS confirms with the OS that the user has been authenticated. The host operating system account name is added as a matching database account name or mapped to another database account name. The database account name is marked or configured as requiring authentication by the host. The DBMS may employ different methods to accomplish the authentication trust. In some cases, the database will make a call to the host operating system to process the authentication request and will grant access when the operating system returns a successful authentication. In other cases, the database may require that the user be authenticated to the host before connecting to the database.

When external directory services are used to authenticate users to the database, the database directs the authentication process through the directory server. Typically, this requires use of the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols for communication between the database and directory service servers. Please see the *Directory Services STIG* for detailed information. The database user accounts are then created and configured to be mapped to the directory service X.509 name. Some DBMS's may provide extensions to directory service schemas to provide other account mapping options as well as database authorizations for the user.

2.2.5 Credential Storage

Access to external resources including other databases may utilize storage of credentials within database tables. Credentials may include passwords or keys used to authenticate the user specified in the stored credential to the external resource. One example of this is database linking. A database link record may be defined that includes the name of the remote database and the username and password used to connect to the remote database. Consideration for the access and storage of remote resource credentials requires strict control.

Credentials used by database maintenance or management jobs or any other application that stores credentials to access the database, requires protection and encryption. Encryption must exercise strong methods and access to the credentials should be granted only to authorized accounts.

2.2.6 Other Connection Data Storage

Client systems may also store remote database access information that identifies available network database services. This information can be useful to attackers as it provides a roadmap to database resources available on the network. Limiting database access information to only those databases to which the client is authorized to connect can help prevent unwanted discovery of other database resources by attackers.

A malicious user may also take advantage of remote database connection information by defining spoofed databases. A spoofed database service may be accessed instead of the intended database target where the database name is not complete or fully defined in the remote connection file. Any database names defined in the connection file should be fully defined to help prevent a redirection attack.

2.3 Database Authorizations

Database authorizations may be referred to as either privileges or permissions within the database. The DBA is granted by default in most installations full privileges. Full privileges include privileges to all objects stored in the database, privileges to configure and operate the database, and privileges to create and manage database user accounts.

Database user accounts that have been assigned privileges to create objects are granted by default full privileges to the objects they own. Object ownership grants the privilege to assign access to the owned object to other database users. The privilege of the object owner to define access to the owned objects is referred to as Discretionary Access Control (DAC) and is the most common access control method found in popular DBMSs. Thus, any assignment of object creation privileges within the database needs to be carefully considered for security implications. Further, by virtue of creating objects, the object owner causes changes to the database metadata (database system tables where object definitions and other related object specifications are maintained) and thus impacts storage and other resource usage by the database.
Database application user accounts require the least privileges of all database account types to function with a database; they require only the ability to access the data stored in objects that are already defined within the database. These privileges may be more finely controlled by using other DBMS objects such as views to restrict access to data in database tables. In fact, the most secure access control implementations restrict users to holding only execute access privileges on stored procedures where the privileges assigned to the procedure itself are used to access data in a specific and limited way. Other secure methods may assign the execute privilege to applications that can enable or disable object privileges only via the application. Some databases may provide additional granularity for access controls by assigning controls to specific data cells.

Good security practice demands both the separation of duties and the assignment of least privilege. Role Based Access Control (RBAC) is the most accepted method for meeting these two demands. A securely designed database implementation includes the definition of database roles based on user functions required by the database application and the assignment of the fewest privileges to these roles. Roles are then assigned to database users based on the application functions they are required to perform.

For example, an accounting application may define user roles based on discrete financial application functions such as General Ledger, Accounts Receivable, Accounts Payable, and the Financial Manager. General Ledger functions require read/select access to some specific data, insert access to other data, and update or delete access to still other data. The same would be true for Accounts Payable and Accounts Receivable functions. Although all functions may require access to the same data, the same access to the same data may not be required. In this example, roles can be created for General Ledger users, Accounts Payable users, and Accounts Receivable users. The specific access type required to the data is then assigned to these roles. Database user accounts are then assigned the role and thereby the privileges appropriate to perform their assigned function(s). In other words, database user JDOE is assigned the General Ledger database role and is then able to perform General Ledger functions. Security is optimal when each function can be broken down to a level of least privilege and the user assigned all the roles required to perform all of their assigned functions. Some application functions may share the same access privileges as others or may always be coupled with other functions in which case multiple distinct roles would be unnecessary.

Most applications require that a specific function to assign application user roles be defined. In the example above, the Financial Manager role would be created and assigned the privilege to assign application roles to database application users within the database. The use of application manager accounts puts the responsibility to assign application privileges directly in the hands of the person who has the functional authority to do so.

Multi-tier applications may utilize a single database account to access the database for application user functions and enable database roles per the requesting user's authorized privileges. The application may also choose to use multiple database accounts based on the job function being performed. The use of multiple accounts may provide a better means to employ the database to assist in auditing functions or other security functions, but the final solution would be dependent on the specific application.

The DBMS privilege to pass on granted privileges to other database users is accomplished using the WITH GRANT OPTION or a variation of GRANT statement options. For example, when an object owner grants READ access to a table using the statement: GRANT READ ON TABLE MYTABLE TO USERNAME WITH GRANT OPTION, the user USERNAME has the privilege to grant read access to other users in the database to MYTABLE. From a separation of duties and security viewpoint, the privilege to assign permissions to others should be assigned only to authorized administrators. This promotes management control of authorizations and aids in the administration of privilege assignments. Application roles are roles that are enabled by an application during runtime. The application connects to the database and enables the role and thus the privileges. Typically, the enabling of application roles is protected by a password supplied by the application at runtime. This restricts use of authorized privileges by individual users outside of the application.

Specific database implementations may offer additional methods for authorization and access control. Whatever authorization assignment tools are used, best practice requires that they be assigned according to least privilege and user function. A secure application design will take advantage of the security capabilities of the backend database to enhance its security posture.

2.3.1 Default Database User Accounts

Most databases create one or more default database accounts during installation. A default DBA account is an example of a default account most often found. Other default accounts may be provided for various database utilities, functions, or demonstrations. After initial database installation and creation, the list of defined database user accounts needs to be reviewed carefully to determine their necessity. Some databases allow disabling or removal of some or all default accounts. In some cases, default accounts may be renamed. Renaming default accounts limits attacks against the known account name. When renaming default accounts, care must be taken to maintain the proper authorizations and object ownership. Utilities may be provided by the database software to accommodate reassignment of default account authorizations to custom accounts.

2.4 Confidentiality

Sensitive Information is defined in DODD 8500.2. The definition is not repeated here, but to paraphrase the definition, sensitive information is unclassified information that, if released, could compromise national security or personnel privacy. The Information Owner, also defined in DODD 8500.1, is the person responsible for data or information served by an AIS and establishing or defining the access controls appropriate for it. In addition to access control, protection of sensitive data stored in the database may also require that the data not be viewable by any user that is not authorized specifically to do so. This most often includes the DBA as well as other database users. Encryption of the data is typically how the data is protected from privileged administration and other accounts in the database. Strong encryption methods must be employed and encryption keys require secure storage.

When data is transmitted from the database to a requesting client, it may traverse a network that is exposed to others who are not authorized to view the data. To protect transmitted data, encryption of the communication is required. Encryption of communications may be provided by the database communications software, the operating system, or network-based devices. However or wherever it is employed, it must encrypt the data along any path exposed to users not authorized to view the sensitive data. Strong encryption must be used.

Sensitive data stored in database tables is not the only data that requires encryption. Application code, found most frequently in procedures and functions stored in the database, may offer to a malicious user sufficient information to discover sensitive calculations, data derivations, data relationships, or hidden database object names. (Passwords or encryption keys should not be stored within application code.) This information could lead to a more successful and focused attack. Most databases provide the ability to encrypt or encode source code within the database. Where the code is not already public and especially where the code may be sensitive or proprietary, the code should be encrypted or encoded. This may not be appropriate or necessary for a development database.

Sensitive data stored within the database is found in the data files used by the database that are stored on the local host. The protection of the database data files is another critical consideration for protecting the data. In addition to the data itself, the data files include the database metadata and other database configuration information that requires protection. Database files may also require encryption.

Database configuration, transaction log, and audit trails and other files storing data used or produced by the database require consideration for encryption. In all cases where the data contains sensitive application data in clear text, the files should be encrypted.

Authentication credentials are a special case of sensitive data and are discussed under authentication considerations.

2.5 Data Integrity

Databases that support transaction processing frequently provide transaction logging and journaling to help protect data integrity against inconsistencies. Transactions may require many actions to occur to be considered successful or complete. Should an interruption occur before all actions of a transaction are complete, any actions of the transaction will be undone or returned to the last known good status. A common example of this is an automated teller machine transaction. A bank customer may have completed a request to withdraw money when connection to the database by the machine was lost and before cash was dispersed. In this case, the correct action would be to cancel the withdraw request sent to the database and return the customer’s bank balance to the amount prior to the request.

This critical protection provided by databases requires careful consideration to ensure transaction logs are secured and maintained. Transaction logs may contain sensitive data and should be considered for encryption. They are necessary to maintain availability and should thus be protected against hardware loss or interruption by using solutions that provide redundancy. Where transaction data is also used to provide an audit trail for data change, the logs or log reports require the same protection as other audit data.

The integrity of the data stored in database tables may be further ensured by using database capabilities to prevent storage of invalid data types, inconsistent data relationships (referential integrity), and invalid values. Use of these data value constraints defined in the database provides a more robust capability consistently across the application than those defined within the application itself.

2.6 Audit

Decisions for auditing configuration must always take into account what activities occurring in the database may indicate malicious or unauthorized actions. They must also be complete enough to follow the trail of unauthorized access or change to the data or database configuration.

The first activity for audit consideration is connections to the database. The decision to audit all connection requests or just failed attempts depends on the intended use of the database. Some databases may have a large number of user connection requests that makes auditing of both failed and successful connections impossible to support. Databases where few connections occur can take advantage of the added benefit of auditing for both.
Auditing of privileged activities including assignment of database privileges, database administration activities, addition, updates, or deletion of database objects, and access to audit data stored within the database should always be enabled. Any sensitive application data stored within the database should be identified and auditing configured appropriately for changes to the sensitive data. Depending on the sensitivity of the data, it may be appropriate to report changes to sensitive data since last access or when it occurs.

Audit log content may always be considered to house sensitive data that requires protection. If audit data is available for review or modification when stored either inside or outside the database, a malicious user can alter the contents to remain undiscovered. The audit data may also provide a means for the malicious user to determine the extent of audit records in order to plan unauthorized activities that exploit audit weaknesses. Audit data may also include sensitive data such as usernames and passwords. Only authorized auditors and the database audit functions should be granted access to database audit data.

DoD requires a minimum retention period of one year for most required audit data (5
five years is required for sources and methods intelligence (SAMI) data). Where audit records are part of an active investigation, longer retention may temporarily be required. Auditing of changes to data as required by the application data owner may be set to other periods based on storage availability and other factors. Audit data should always be closely reviewed for indication of malicious activity prior to the end of the required retention period if not sooner. Audit data may be stored offline, i.e., on storage media not immediately accessible by the system, but it has proven useful to maintain one week of audit data or more online if possible to provide an immediate short-term review where suspicious activity or other concerns arise.

Frequent and regular monitoring of audit data for suspicious activity should be mandated. Automated tools may be employed to assist in the sometimes daunting task of audit data reviews. Because the use of any particular database and the purpose and function of the applications that depend upon it can vary greatly, it isn’t meaningful to apply a detailed standard requirement for all databases and declare it sufficient. What activities should be targeted for review will always depend on what functions offer the greatest risk to that specific database and application. For example, some databases may be accessed by a large number of external services including remote management or web services and so may require a robust audit reporting tool with rules to monitor the various connection types and accounts be reviewed. Other databases may provide support only to a local web application with local administrative access and may be reviewed manually. Databases hosting applications that manage sensitive or privacy data require close scrutiny of data access and changes. In all cases, an automated reporting capability, whether provided by an external tool or local database procedures should be considered for notifying administrators automatically of suspicious activity.

Development databases, where it is assumed no sensitive data is stored, require protection of the application code under development as well as the development or use of the auditing capability itself. The details of audit access for development of audit functions would be determined by the application development manager or auditor. Access to any audit of application changes would be granted only to users whose responsibility it is to track and maintain changes to the code under development.

2.7 Replication and Federation

Many database products support connections initiated from one database to one or more remote databases. These connections are defined within the database and often stored with credentials within the database as discussed earlier. The simple implementation of remote database connections is referred to as database links.

A compromise of one database may, through the use of defined database links, provide an easy path to extend the compromise to remote databases. For this reason, the definition and use of database links should not be casually employed. Careful consideration of access to and protection of the connection definition and supporting credential data is required. Also, auditing to provide accountability across systems should be reviewed. Additional considerations for securely configuring use of database links include:

1. Use of a single or multiple accounts for remote connections
2. Use of individual user database accounts or a shared account
3. Use of a directory service and domain name service instead of database links
4. Auditing the use of a database link
5. Protection of use of the database link
6. Protection of the data in a database link definition
7. Security of the communication channel to the remote database
8. Encryption of the communication channel to the remote database
9. Location and protection of replication data stored externally to the database for transmission
10. Sensitivity of the replicated data; encryption of the replication data file
11. Privileges assigned to database accounts on remote databases accessed by database links.

Database links are used by some database availability and backup/recovery services. Database replication, a feature that provides automated duplication of selected data in one database to a remote database, uses database links to move replicated data. Databases are designated as either providers or recipients of duplicated data and the data may be pushed or pulled from one database to the other. In addition to the security considerations listed earlier, the accounts used for replication should be carefully considered. It is generally best to use a single replication account between all of the participating databases. Use of a single account improves accountability and restricts privileges required by replication to a single account. However, separate replication accounts should be used where replication requirements do not overlap. In other words, where replication between two databases exists, a single account should be used. Where one database replicates some data to one database and other data to another database, two separate accounts may be more secure. In such a case, separate accounts would provide a separation of responsibility and accountability would be improved.

Federated databases are databases that support data distributed across two or more remote databases. They may provide load balancing capabilities and generally support high-availability requirements. They are designed to use database links. Again, special consideration is necessary to address risks associated with account usage, credential storage, database link access, preservation of accountability, and data in transit across networks.

2.8 Database Clustering

Database clustering, like its OS counterpart, is used to provide a hot-backup level of availability. In a cluster configuration, should one database fail, transparent rollover to another database in the cluster occurs. The client may not notice any interruption. Database clustering shares many of the same security concerns as other activities involving remote database dependencies including:

- database and operating system accounts required to support clustering activities need to be closely scrutinized to ensure they are restricted to only privileges required to support their defined function and the accounts are available only to authorized users
- a trail of accountability needs to be maintained between actions occurring on one database and their related actions in the remote database
- the communications path needs to be protected as appropriate for the sensitivity level of the data

2.9 Backup and Recovery

Backup and recovery procedures for databases are an important part of overall database availability and integrity. After installation, most DBMS products are not automatically configured to provide backups and are not automatically included with host operating system backups. Additionally, due to open file requirements, many host-based backup products may not support database backups and may not accommodate other special needs for database recovery from backups. Most often backup and recovery functions built into the DBMS or third-party backup and recovery products designed specifically to accommodate database products are used. Databases must maintain strict attention to the timing of events to preserve data integrity. This attention must also be preserved by the backup and recovery products to ensure a reliable recovery. In fact, most databases may fail to restart if discrepancies in event timing are discovered. Due to the sensitivity of database recovery, testing of database backup and recovery is particularly vital.

Backup data will contain any sensitive data stored in the database. It is imperative that the backup data be protected with the same protections or equivalent protections as the live data. It must be protected by encryption and be accessible only to authorized personnel. The backups should require authentication and authorization for access.

2.10 Operating System Protections

Like other applications, DBMS installations depend upon the security posture of the host operating system. A weak security configuration of either the operating system or the database can affect the security of the other. The host operating system must be secured with not only its own security in mind, but also the protection of the applications it hosts. The host system and database application should be carefully reviewed for dependency on local installation of other applications. Examples of frequently associated applications are web servers, application servers, and directory services. Only where a dependency is required for operation of the application should the database share the host system with other applications. Such a separation helps protect each application component from the vulnerabilities of the other. Additionally, the host system should be reviewed to disable any processes or services that are not required to support the functioning of the database. This limits the vulnerabilities on the host system and presents a smaller target for attack.

Installation documentation should be consulted prior to the installation and operating system requirements reviewed for security implications. The first configuration item that requires security in the design is the storage of the database software and the configuration, audit, and data files. Database directories and files should always be stored on disk partitions dedicated to the database. Disk partitions should not be shared with any other applications, either web servers or application software used to access the database. Other applications as well as the host operating system have separate and distinct access requirements. Where multiple installations of database software occur, the same principle may apply, that is, that distinct security requirements may be needed to protect one installation separately from another. Disk partitions housing database software and data files require robust access control lists (ACL) and data and recovery files should be further protected from disk hardware failure by means of a Redundant Array of Inexpensive Disks (RAID) or mirrored disk solution.

OS accounts used by the database should be dedicated to distinct functions required by database software installation and maintenance, database processes, and by DBAs. An OS account dedicated to installation and ownership of the database software files should be used. The permissions granted by default to the owner account can then be restricted to an account not used for other purposes. Typically, a DBMS will support a separate account for the primary database processes as well as optional database service processes. Each separate database process should be reviewed for its individual access requirements to both operating system and database resources. Dedicated OS accounts should be used where possible. They should be assigned the least privileges required to function and be restricted to accessing only those database files and directories that are required. In some cases, separate installations of database components may be required to provide the desired level of separations. Component separation of directories and files also provides consistent file ownership within directories where components maintain files.

The DBA function is a separate responsibility from the host system administrator (SA) responsibility. Thus, accounts separate from the SA account should be created. This separation of accounts also helps to protect a compromise of the operating system from having full access to the database. The assignment of OS privileges required by the DBA is best assigned to a DBA role or group defined on the host. Assignment to the role should then be assigned to the authorized DBA. A host OS administrative group or role should not be assigned the DBA role or group membership. This promotes the requirement for individual authorization of each privilege role assignment. The DBA OS role is also used for assignment of access to DBMS directories and files.

Depending on the DBMS backup and recovery procedures defined, backup and recovery may be configured and protected by the OS. As overall responsibility for the administration of the database belongs to the DBA function, the DBA is responsible at a minimum for monitoring the status of DBMS backups. Where DBMS backups are included in the OS activities and performed by the SA, the DBA is responsible for ensuring the coordination is complete. Responsibility for reviewing the design of the backup and recovery security as it applies to the DBMS also falls to the DBA. The SA cannot always be expected to have a full understanding of the backup and recovery security required.

Database software as with other application software installed on a host system should be included in a system baseline record and reviewed in order to discover unauthorized changes to the software. This is a vital step to securing the host and applications as it is the only method that may provide the ability to detect and recover from otherwise undetected changes.
Updates to DBMS software that are provided by DBMS software vendors is usually restricted to specific versions of the software. DBMS vendors will also rarely test older versions of their software to see if they are susceptible to published vulnerabilities. It is imperative that the DBMS software is maintained to a version that still receives security patching and that security patches are installed as soon as possible. Where available, the DBA and/or SA should subscribe to vulnerability and security patch availability alert services. It may also prove helpful for the DBA to remain aware of host platform security alerts to review their affect on the DBMS. Regular maintenance plans can be scheduled to include anticipated DBMS upgrades and security patch releases.

2.11 Application Protections

Applications introduce some of the most common database attack avenues. Poorly designed applications available to the Internet provide a pathway for an unlimited number of malicious users to access sensitive data. An application that accesses the database with any more privileges than those required to manipulate the data in anyway other than what is intended is subjecting the data to unauthorized exposure. Databases and applications that do not audit access to elevated privileges or sensitive data leave no trail that exposure has occurred. Further, when an application uses elevated privileges to the database (it is not unusual to find an application that uses a DBA account that owns all application database objects to operate), then the entire database is at risk. Where input validation does not occur, the database process can be compromised which can lead to attack of the host system.

It is therefore, important to review any application to discover how the most stringent security can be applied. Like other services or process that access the database, review the authentication method that the application uses to connect to the database. The authentication used must meet all the requirements for that method, that is, passwords must meet complexity, expiration, and history requirements. Passwords must be encrypted when stored and transmitted. Ensure credentials are stored in a secure, restricted location.

Review database accounts used by the application to access the database and determine if the minimum privileges required have been granted. Frequently, applications may unnecessarily require elevated privileges. Any stated requirement for elevated privileges should be verified. Determine and set application protections to prevent the return or display of unauthorized database information such as product and version, table names or other database object information when queried or when errors occur.

The *Application Security and Development STIG* provides requirements for securing applications. If both the database and application are secured, then the attack surface of the database can be greatly reduced.

2.12 Network Protections

Access to databases can be controlled by network architecture and devices. With the increase in direct access to databases by web services and web-based protocols, the configuration of network access to the database has become more critical. Some databases now provide direct access via http or the web protocol to stored procedures meaning that the database itself houses the executable directly available to the web.

When considering security protections related to network access to the database, the first determination needs to be what remote systems and/or users require connection to the database. This is followed by determining how best to restrict database access to these users and systems by means of network architecture and devices. Network access may also be controlled by the host OS or database listener process configuration. Network access restrictions should be employed wherever they are available and complimentary so that unauthorized systems are simply not able to access the database to even request a connection. While not guaranteed, it should be the goal for securing network-based access to the database.

In addition to controlling the ability to request a database connection, other restrictions can be defined to further restrict network sessions to the database and deter or prevent attacks. These restrictions can include time and count limits on network session parameters. Limiting these parameters can prevent some Denial of Service (DoS) attacks and the hijacking of open sessions. All network session and communication parameters should be reviewed for their applicability to help protect against network-based attacks.

As discussed earlier, the transmission of authentication credentials and other sensitive data across a network requires protection against unauthorized disclosure. Where the data traverses network segments exposed to systems or users not authorized to view the data, the data requires encryption. The encryption may be employed by network devices such as Virtual Private Network (VPN) devices or provided by the host or database for network communications. Whatever method is employed, the communications must be viewable by required intrusion detection systems and configured in accordance with other network security requirements.

3. DATABASE SECURITY REQUIREMENTS

As the repository for business data, databases are an important component in providing data confidentiality, integrity, and availability. The security mechanisms native to the database itself must be employed in consideration of their interoperability and security dependency on the hosted platform, the network architecture and security devices, as well as the applications that provide the client interface to the database.

This section provides the specific requirements for security elements that relate to the protection of access to data stored in the database as well as operation of the database itself. The security requirements are presented as they relate to subject sections, subsections, and Information Assurance (IA) controls as listed in DoD Instruction (DoDI) 8500.2, IA Implementation. IA controls are listed by the name and 4-letter acronym (in parentheses) assigned in DoDI 8500.2. Where a requirement is derived from other DoD policy a specific reference to the other policy is included. The subject sections are as follows:

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Continuity
- Vulnerability and Incident Management

Subject sections from DoDI 8500.2 not addressed in this document indicate that the security controls are outside the scope of this document and the responsibilities of DBAs, SAs, and IAOs as they relate specifically to the security of a database. Subject areas that may overlap are included in this document where attending to the inclusion of the DBMS security in the underlying or overarching technology may be overlooked.

Compliance with some requirements in this document may involve a significant effort or expense to configure that may be beyond the risk associated with the specific vulnerability or the sensitivity or value of the DBMS or data to DoD or business operations. The risk is determined and, therefore, the criticality of compliance with the security requirement in association with the assigned importance to the mission and the confidentiality level of the application data. Where there is variance in the risk, the requirements listed here are broken out based on the criticality and sensitivity level assigned to the DBMS as defined in DoDI 8500.2. DoD requires that all Automated Information Systems (AIS) be assigned a criticality and sensitivity level. As a standalone AIS or component of an AIS, a DBMS is required to have such an assignment within DoD.

This document assigns responsibilities to the following roles:

- Information Assurance Manager (IAM)
- Information Assurance Officer (IAO)
- Database Administrator (DBA)

The IAM and IAO responsibilities are assigned in accordance with the associated roles as defined in DODI 8500.2. The role of the DBA is a “privileged user with IA functions” as defined in DODI 8500.2. Any security responsibilities that require configuration and operation that are related to the DBMS are assigned to the DBA in this document. Different organizations may assign some specific DBMS security responsibilities to the host SA. Other responsibilities assigned to DBAs in this document may be managed by the organization responsible for an application dependent upon the DBMS. Where a single DBA is not responsible for all aspects of the DBMS security, the IAO is responsible for assigning the specific DBA responsibilities to the appropriate individuals and providing the necessary oversight to ensure no DBA responsibilities are left unassigned. It is also the IAO’s responsibility to know the overall security posture of the DBMS by having an awareness of non-compliant DBMS security configurations and operations.

3.1 Security Design and Configuration

3.1.1 Procedural Review (DCAR)

A regular review of current database security policies and procedures is necessary to maintain the desired security posture of the DBMS. Policies and procedures should be measured against current DoD policy, STIG guidance, vendor-specific guidance and recommendations, and site-specific or other security policy.

- *(DG0096: CAT III) The IAO will ensure database IA policies and procedures are reviewed at least annually and are current and consistent with all IA requirements.*

3.1.2 Configuration Specifications (DCCS)

Where available, security configuration guidance can be vital to securing the database against known threats or vulnerabilities. This STIG as well as vendor-provided guidance, other security organization guidance, and results from trusted database security testing labs can help the IAO and DBA choose the most comprehensive security configuration appropriate for the use and environment of the installed DBMS.

- *(DG0007: CAT II)The IAO will ensure the database is secured in accordance with STIG or NSA guidance where such guidance is available for the specific database product. Where not available, the IAO will ensure the database is secured in accordance with the general security requirements provided in this STIG and with specific security guidance in this order of preference as available:*

  Commercially available practices from independent security organizations such as SANS, the Center for Internet Security (CIS), and the National Institute of Standards and Technology (NIST);

  Independent testing labs such as ICSA (http://www.icsalabs.com);

  Vendor security recommendations and literature.

NOTE: No independent testing labs for security of database products are known at this time. One or more vendors provide vulnerability testing tools for database products.

3.1.3 Compliance Testing (DCCT)

Updates and patches to existing software have the intention of improving the security or enhancing or adding features to the product. However, it is unfortunately common that updates or patches can render production systems inoperable or even introduce serious vulnerabilities. Some updates also set security configurations back to unacceptable settings that do not meet security requirements. For these reasons, it is a good practice to test updates and patches offline before introducing them in a production environment.

- *(DG0097: CAT II) The IAO will ensure comprehensive testing plans and procedures for database installations, updates, and patches are defined and implemented before being deployed in a production environment.*

3.1.4 Functional Architecture for AIS Applications (DCFA)

The DCFA IA control in DoDI 8500.2 provides a list of requirements to be included in a functional architecture that must be defined for the AIS. The requirements are broken down here into the categories as listed in the DCFA control. As an application, a secure DBMS implementation must be in accordance with a planned or designed usage or architecture. Security concerns are frequently specific to the planned usage. For example, a database initially planned for use by a single application using a single database connection from a remote host would have a far different set of security concerns from a database shared by multiple applications supporting many individual client sessions and in addition to dedicated connections from external web application hosts. Whenever changes to the usage or environment or configuration of a DBMS are made or considered, a review of the DBMS functional architecture needs to be completed.

3.1.4.1 External interfaces and information being exchanged are protected

External interfaces include any remote or local connection to or from the DBMS. They may include locally run processes on the same host system that are not part of the base DBMS processes in addition to connections from the DBMS to remote database clients or applications. They may be initiated by the DBMS as a client or from remote clients to the DBMS. External connections provide an opportunity for unauthenticated and/or unauthorized access to the DBMS and need to be protected accordingly. External connections also frequently mean that data, authentication data at a minimum, is being transferred and is also at risk. DBMS's may also spawn additional external processes to execute procedures defined in the DBMS, but stored in external host files (external procedures). The spawned process used to execute the external procedure may operate within a different OS security context than the DBMS and provide unauthorized access to the host system.

As the alternate consideration of what connections are expected and authorized, what is not authorized and expected also needs to be addressed. Included in the requirements below, are requirements for protecting against unauthorized connections from both local and remote sources.

- *(DG0016: CAT III) The DBA will ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the DBA will ensure the unused component or feature is disabled.*

- *(DG0014: CAT II) The DBA will ensure database applications, user accounts, and objects installed for demonstration of database features, experimentation, or other non-production support purposes have been removed from the database and host system.*

- *(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.*

- *(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.*

- *(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.*

- *(DG0190: CAT II) The DBA will ensure use of credentials used to access remote databases or other applications are restricted to authorized database accounts and used only for mission and/or operationally required and documented purposes.*

- *(DG0191: CAT II) The DBA will ensure credentials stored in or used by the DBMS that are used to access remote databases or other applications are protected by encryption and access controls.*

- *(DG0192: CAT II) The DBA will ensure credentials used to access remote databases or other applications use fully qualified names, i.e., globally unique names that specify all hierarchical classification names, in the connection specification.*

- *(DG0100: CAT II) The DBA will ensure database accounts used for replication or distributed transactions are not granted DBA privileges.*

- *(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.*

- *(DG0102: CAT II) The DBA will ensure each database service or process runs under a custom, dedicated OS account that is assigned the minimum privileges required for operation where applicable.*

- *(DG0103: CAT II) The DBA will ensure database and host system listeners that provide configuration of network restrictions are configured to restrict network connections to the database to authorized network addresses and protocols.*

- *(DG0104: CAT III) The DBA will ensure all local and network-advertised named database services are uniquely and clearly identified.*

3.1.4.2 User roles and required access privileges identified

A core security concern of the DBMS is to protect access to the data stored within it. Unauthorized access to the data can lead to loss of confidentiality and integrity of the data. The responsibility of understanding and assignment of the sensitivity falls to the Information Owner. As part of this responsibility, the Information Owner must also understand and identify the job functions that require access to sensitive data. Without this identification and assignment of appropriate authorizations by the Information Owner, sensitive data is vulnerable to unauthorized access.

- *(DG0105: CAT II) The DBA will ensure all database application user roles and the privileges assigned to them are authorized by the Information Owner in the AIS functional architecture documentation.*

3.1.4.3 Unique security requirements (encryption of sensitive data)

Access to sensitive data may not always be sufficiently protected by authorizations and requires encryption. In some cases, the required encryption may be provided by the application accessing the database. In others, the DBMS may be configured to provide the data encryption. When the DBMS provides the encryption, the requirement must be implemented as identified by the Information Owner to prevent unauthorized disclosure or access.

- *(DG0106: CAT II) The DBA will ensure security requirements specific to the use of the database are configured as identified in the System Security Plan.*

3.1.4.4 Categories of sensitive data handled by the database are identified

A DBMS that does not have the correct confidentiality level identified or any confidentiality level assigned stands the chance of not being secured at a level appropriate to the risk it poses.

- *(DG0107: CAT II) The IAO will ensure all categories of sensitive data stored or processed by the database are identified in the AIS functional architecture documentation.*

3.1.4.5 Restoration priority of subsystems is identified

When DBMS service is disrupted, the impact it has on the overall mission of the organization can be severe. Without the proper assignment of the priority to be placed on restoration of the DBMS and its subsystems, restoration of DBMS services may not meet mission requirements.

- *(DG0108: CAT III) The IAO will ensure the restoration priority of the database and its supporting subsystems are identified in the System Security Plan.*

3.1.5 Non-repudiation (DCNR)

To be effective, cryptography must be implemented using proven strong algorithms and functions. Use of weak cryptography can undermine attempts to protect the integrity and confidentiality of sensitive data.

- *(DG0025: CAT II) The DBA will ensure FIPS 140-2 validated cryptography is used where encryption, digital signature, key exchange, and secure hashing is required and is configured to use NIST approved standards.*

3.1.6 Partitioning the Application (DCPA)

In the same way that added security layers can provide a cumulative positive effect on security posture, multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system. A DBMS not installed on a dedicated host both threatens and is threatened by other hosted applications. Applications that share a single DBMS may also create risk to one another. Access controls defined for one application may by default provide access to the other application's database objects or directories. Any method that provides any level of separation of security context assists in the protection between applications.

- *(DG0109: CAT II) The IAO will ensure the DBMS host is dedicated to support of the DBMS and is not shared with other application services including web, application, file, print, or other services unless mission or operationally required and documented in the System Security Plan.*

- *(DG0012: CAT II) The DBA will install and maintain database software directories including DBMS configuration files in dedicated directories or disk partitions separate from the host OS and other applications.*

- *(DG0111: CAT II) The DBA will install and maintain database data directories including transaction log and audit files in dedicated directories or disk partitions separate from software or other application files.*

- *(DG0112: CAT II) The DBA will ensure DBMS data files that store DBMS system tables and other system objects dedicated to support the entire DBMS are not shared with data files used for storage of third-party application database objects.*

- *(DG0113: CAT II) The DBA will ensure database data files used by third-party applications are defined and dedicated for each application.*

3.1.7 Ports, Protocols, and Services (DCPP)

Perimeter network defenses play an important role by protecting internal network resources. Their effectiveness is diminished in proportion with the controls they relinquish. When internal systems are configured or designed to communicate across network boundaries in open, uncontrolled ways, then that same lack of control can be utilized by malicious users for attack. To support the effectiveness of network perimeter defenses, DBMS communications are best configured to use known and consistent ports, protocols, and services that comply with defined network protection rules. DoD policy requires that use of ports, protocols, and services within DoD adhere to DoDI 8551.1, Ports, Protocol, and Services Management (http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf).

- *(DG0151: CAT II) The SA/DBA will ensure random port assignment to network connections is disabled when traversing network firewalls.*

- *(DG0152: CAT II) The SA/DBA will ensure DBMS network communications comply with DoDI 8551.1 Ports, Protocols, and Services Management.*

3.1.8 Configuration Management (CM) Process (DCPR)

Configuration management is as important to a DBMS implementation as it is for any other AIS. Uncontrolled, untested, or unmanaged changes result in an unreliable security posture. All software libraries related to the database and its used need to be reviewed, considered, and the responsibility for CM assigned. CM responsibilities may appear to cross boundaries. It is important, however, for the boundaries of CM responsibility to be clearly defined and assigned to ensure no libraries or configurations are left unaddressed. Related database application libraries may include third-party DBMS management tools, DBMS stored procedures, or other end-user applications.

- *(DG0011: CAT III) The IAO will ensure configuration management procedures are documented and implemented for changes to the DBMS configuration, software libraries, and other related application software libraries.*

3.1.9 IA Documentation (DCSD)

A System Security Plan defines the security procedures and policies applicable to the AIS. It includes definition of responsibilities and qualifications for those responsible for administering the security of the AIS. For databases, this includes specifically the DBA in addition to the standard SA and IAO roles. Without a security plan, unqualified personnel may be assigned responsibilities that they are incapable of meeting and the database security is prone to an inconsistent and incomplete implementation.

- *(DG0153: CAT III) The IAO will assign and authorize DBA responsibilities for the DBMS.*

- *(DG0156: CAT III) The IAM will assign and authorize IAO responsibilities for the DBMS.*

- *(DG0154: CAT III) The IAO will ensure the DBMS is included in or has defined for it a System Security Plan.*

3.1.10 System Library Management Controls (DCSL)

The DBMS software files and directories as well as the files and directories of dependent applications are vulnerable to unauthorized changes if not adequately protected. An unauthorized change could affect the integrity or availability of the DBMS and the application data.

- *(DG0009: CAT II) The SA/DBA will ensure access to DBMS software is restricted to authorized OS accounts.*

- *(DG0010: CAT III) The IAO will ensure DBMS software is monitored on a regular basis no less frequently than weekly to detect unauthorized modifications.*

- *(DG0050: CAT II) The DBA will ensure database application software is monitored to detect unauthorized modification every week or more often.*

- *(DG0019: CAT III) The DBA will ensure database application software is owned by the authorized application owner account.*

- *(DG0091: CAT III) The DBA will ensure custom application and Government-Off-The-Shelf (GOTS) source code objects are encoded or encrypted within the production database where supported by the DBMS.*

3.1.11 Security Support Structure Partitioning (DCSP)

The Security Support Structure is a security control function or service provided by an external system or application. An example of this would be a Windows domain controller that provides identification and authentication that can be used by other systems to control access. The vulnerabilities and, therefore, associated risk of a DBMS installed on a system that provides a security support structure is significantly higher than when installed with other functions that do not provide security support. In cases where the DBMS is dedicated to local support of a security support function (e.g. a directory service), separation may not be possible.

- *(DG0110: CAT II) The IAO will ensure the DBMS is not installed on a host system that provides directory services or other security services except when serving as a required component of the security service.*

NOTE: This requirement includes the prohibition of a DBMS installation on a Windows Domain Controller.

3.1.12 System State Changes (DCSS)

A DBMS has special considerations for securing state changes. Many DBMS provide job queues for executing regular maintenance and other DBMS or application procedures. It may be possible for an unauthorized user to submit a job that could be run at DBMS startup that could sabotage a successful DBMS startup or the secure operation of the DBMS afterwards. Data files may be replaced by compromised versions that become active upon DBMS startup. The DBMS may be subject to an incomplete shutdown or abort that result in a compromise of data integrity.

- *(DG0155: CAT II) The DBA will ensure all applicable DBMS settings are configured to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.*

NOTE: This requirement includes the prevention of scanning for automated job submissions at startup and settings to allow only trusted known good data files at startup.

3.1.13 Software Baseline (DCSW)

Without maintenance of a baseline of current DBMS application software, monitoring for changes cannot be complete and unauthorized changes to the software can go undetected. Changes to the DBMS executables could be the result of intentional or unintentional actions.

- *(DG0021: CAT II) The DBA will ensure a baseline of database application software and DBMS application objects is maintained for comparison.*

NOTE: The baseline of database application software and DBMS application objects requires updating after installation or update.

3.2 Identification and Authentication

3.2.1 Group Identification and Authentication (IAGA)

Group authentication occurs when a single identifier is used to authorize a connection. Group authentication does not provide individual accountability for actions taken on the DBMS or data. Whenever a single database account is used to connect to the database, a secondary authentication method that provides individual accountability is required. This scenario most frequently occurs when an externally hosted application authenticates individual users to the application and the application uses a single account to retrieve or update database information on behalf of the individual users.

- *(DG0060: CAT II) The IAO/DBA will ensure actions by a single database account that is accessed by multiple interactive users are attributable to an individual identifier.*

3.2.2 Individual Identification and Authentication (IAIA)

A database connection without identification and authentication allows unauthorized and unaccountable actions on the DBMS and data. Usernames created by default during installation of the DBMS and components are well-known to potential attackers and provide a known target for malicious intent.

- *(DG0078: CAT II) The DBA will ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.*

- *(DG0131: CAT III) The DBA will change or delete default account usernames where supported.*

3.2.2.1 Password Storage Requirements

Unprotected passwords are more easily discovered by unauthorized users and can aid in compromise of the DBMS and data. Weakly protected passwords also result in lost accountability for actions as a single account can no longer be attributed to a single person.

- *(DG0067: CAT I) The DBA will ensure database account passwords are stored in encrypted format whether stored in database objects, external host files, environment variables or any other storage location.*

- *(DG0129: CAT I) The DBA will ensure all database account passwords are encrypted when transmitted across the network.*

- *(DG0130: CAT II) The DBA/IAO will ensure database account passwords are not stored in batch jobs or application source code.*

3.2.2.2 Password Attribute Requirements

Weak passwords are a primary target for attack to gain unauthorized access to databases and other systems. Where username/password is used for identification and authentication to the database, requiring the use of strong passwords can help prevent simple and more sophisticated methods for guessing at passwords. All default passwords assigned at installation are the easiest and more common targets for attack. Unfortunately, they are also still the most commonly successful attack against accessible databases.

- *(DG0066: CAT II) The DBA will assign a database account password at database account creation.*

- *(DG0071: CAT II) The DBA will ensure database passwords differ from previous values by more than 4 characters when changed where supported by the DBMS.*

- *(DG0072: CAT II) The DBA will ensure users are not allowed to change their database account passwords more than once every 24 hours without IAO approval where supported by the DBMS. (This requirement does not apply to password changes after password reset actions initiated by the DBA or application administrator).*

- *(DG0079: CAT II) The DBA will ensure database password complexity standards meet current minimum requirements for length (9 characters or more for database application user accounts and 15 characters or more for privileged database accounts) and composition (at least two uppercase characters, two lowercase characters, two special characters, two digits) where supported by the DBMS.*

- *(DG0125: CAT II) The DBA will set expiration times for interactive database user account passwords to 60 days or less where supported by the DBMS.*

- *(DG0193: CAT II) The DBA will set expiration times for non-interactive database application account passwords to 365 days or less where supported by the DBMS.*

- *(DG0126: CAT II) The DBA will configure database account passwords to be prevented from reuse for a minimum of five changes or one year where supported by the DBMS.*

- *(DG0127: CAT II) The DBA will configure or test database account passwords to prevent use of easily guessed or discovered values.*

- *(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.*

3.2.3 Key Management (IAKM)

Strong cryptography does not guarantee protection without the additional protection of the encryption keys. While not normally a concern for the DBMS itself, these requirements are presented in this STIG to raise the awareness of cryptographic key protections. Use of weak encryption and key storage may be under consideration by DBAs to accommodate use of DBMS maintenance jobs where a username and password must be stored and retrieved.

- *(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.*

- *(DG0166: CAT II) The DBA will ensure asymmetric keys used for encryption of sensitive data used by or for the DBMS use DoD PKI certificates and will ensure the private keys are protected and stored in accordance with NIST (unclassified data protection) or NSA (classified data protection)-approved key management technology and processes.*

3.2.4 Token and Certificate Standards (IATS)

DoDI 8500.2 and DoDI 8520.2 require the use of certificates for identification and authentication (I&A). Within DoD, certificates are presented for I&A by users with the Common Access Card (CAC) serving as the hardware token. The DoD CAC is the implementation of Personal Identity Verification (PIV) required for all Federal employees and contractors in the Homeland Security Presidential Directive 12/HSPD 12. Component certificates for servers and code-signing certificates for applications are issued in software form. Use of username and password is not a sufficiently secure I&A method to restrict access to sensitive data.

- *(DG0065: CAT II) The IAO will ensure a DoD PKI class 3 or 4 certificate and an approved hardware security token (DoD CAC for DoD employees or contractors) or an NSA-certified product is used for identification and authentication to the database.*

3.3 Enclave and Computing Environment

3.3.1 Access for Need-to-Know (ECAN)

Sensitive data may hold information that, if discovered or released, could lead to a loss of privacy, a compromise to national security, or some other undesirable outcome. The least possible access to the fewest possible people provides the least opportunity for misuse of the data. The goal when making the decision to grant access is to take into consideration each person, each job function, and what level of access (read or modify) to the data is required. Any user not so authorized that gains access to sensitive data would constitute a compromise of the integrity and confidentiality of the data.

- *(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.*

- *(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.*

- *(DG0138: CAT II) The DBA will ensure all access to sensitive application data stored or defined within database objects is granted only to database application user roles and not directly to database application user accounts.*

- *(DG0076: CAT II) The DBA will ensure sensitive application data exported from the database for import to remote databases or applications is not provided to personnel or applications not authorized or approved by the Information Owner.*

- *(DG0069: CAT II) The DBA will ensure production data is not exported for import to development databases except in accordance with processes and procedures approved by the Information Owner.*

- *(DG0053: CAT III) The IAO will ensure database client software includes only database identification parameters of databases to which that user is authorized access.*

3.3.2 Audit Record Content (ECAR)

An event without record provides no accountability for action. Additionally, without auditing, unauthorized activities may go undetected.

- *(DG0029: CAT II) The DBA will ensure the DBMS auditing function is enabled.*

- *(DG0140: CAT II) The DBA will ensure all access to DBMS configuration files, database audit data, database credential, or any other DBMS security information is audited.*

- *(DG0141: CAT II) The DBA will ensure all database logons, account locking events, blocking or disabling of a database account or logon source location, or any attempt to circumvent access controls is audited.*

- *(DG0142: CAT II) The DBA will ensure privileged DBMS actions and changes to security labels or sensitivity markings of data in the DBMS are audited.*

- *(DG0145: CAT II) The DBA will ensure audit records contain the user ID, date and time of the audited event, and the type of the event*

- *(DG0146: CAT II) The DBA will ensure audit records include the reason for any blocking or blacklisting of database accounts or connection source locations.*

NOTE: Where resources are limited, auditing of logons may be reduced to recording only failed logon attempts.

3.3.3 Audit Trail, Monitoring, Analysis and Reporting (ECAT)

An audit trail that is not monitored for detection of suspicious activities provides little value. Regular or daily review of audit logs not only leads to the earliest possible notice of a compromise, but can also minimize the extent of the compromise.

- *(DG0052: CAT II) The DBA will include the name of the application used to connect to the database in the audit trail where available.*

- *(DG0054: CAT III) The IAO or Database Auditor will regularly review the audit trail to discover access by unauthorized application software.*

- *(DG0095: CAT II) The IAO will ensure the database audit data is reviewed daily to discover suspicious or unusual activity.*

- *(DG0161: CAT II) The IAO will ensure an automated monitoring tool or capability is employed to review DBMS audit data and immediately report suspicious or unauthorized activity.*

3.3.4 Changes to Data (ECCD)

The responsibility for managing the auditing configuration for data access may or may not fall to the DBA. In some cases, applications may incorporate their own auditing capability. Where the application depends on the DBMS to provide the auditing of changes to data, the responsibility for auditing for changes to data falls to the DBA. Auditing of changes to sensitive data can provide not only accountability, but also the ability to restore data to the correct value or content.

- *(DG0031: CAT II) The DBA will configure auditing of access or changes to data in accordance with the application requirements specified in the System Security Plan.*

3.3.5 Encryption for Confidentiality - Data at Rest (ECCR)

Where access controls do not provide complete protection of sensitive data, encryption can help to close the gap. Where privileged users do not have a need-to-know, where files are stored externally to the database, where application user roles cannot be restricted by privileges to single rows and columns of data to those they need to access, encryption can provide the required level of protection.

- *(DG0068: CAT II) The DBA will ensure applications that access the database are not used with options that display the database account password on the command line.*

- *(DG0090: CAT II) The IAO/DBA will ensure sensitive data is encrypted within the database where required by the Information Owner.*

- *(DG0092: CAT II) The DBA will ensure database data files are encrypted where encryption of sensitive data within the DBMS is not available.*

3.3.6 Encryption for Confidentiality - Data in Transit (ECCT)

When sensitive data is returned from a database to a remote client, it traverses the network. Sensitive data traversing networks may be viewed or collected by people or systems without a need-to-know authorization to do so.

- *(DG0093: CAT II) The DBA will ensure remote administrative connections to the database are encrypted.*

- *(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements.*

3.3.7 Data Change Controls (ECDC)

Data integrity is a primary responsibility of the DBMS. The maintenance of data integrity involves preservation and control of not only the data contents, but the relationships between two or more related data items and the actions taken on one that may affect others. A DBMS provides data integrity that may be affected by incomplete or interrupted transactions by means of logging transaction events. This allows the database to recover data content to a point where the data content and its relationships are known to be intact. This data integrity is maintained when the data is undergoing a change or update event. Most DBMS's enable transaction rollback or recovery by default and as an automatic feature of database recovery. Where not automatically enabled, this function is required to be made active.

- *(DG0170: CAT II) The DBA will configure the DBMS to enable transaction rollback and transaction journaling or their technical equivalent to maintain data consistency and recovery during operational cancellations, failures, or other interruptions.*

3.3.8 Interconnections among DoD systems and Enclaves (ECIC)

Applications that access databases and databases connecting to remote databases that differ in their assigned classification levels may expose sensitive data to unauthorized clients. Any interconnections between databases or applications and databases differing in classification levels are required to comply with interface control rules. This requirement is covered in depth in the *Enclave STIG* and is listed here to heighten awareness of the requirement during application and DBMS design and planning.

- *(DG0171: CAT II) The DBA will ensure interconnections between databases or other applications operating at different classification levels are identified and their communications configured to comply with the interface controls specified in the System Security PlanSYSTEM SECURITY PLAN.*

3.3.9 Audit of Security Label Changes (ECLC)

Some DBMS systems provide the feature to assign security labels to data elements. The confidentiality and integrity of the data depends upon the security label assignment where this feature is in use. Changes to security label assignment may indicate suspicious activity.

- *(DG0172: CAT II) The DBA will enable auditing of any changes to the classification or sensitivity level assigned to classified data in the DBMS where available and required by the Information Owner.*

3.3.10 Logon (ECLO)

The login process is most frequently the target activity used to launch a malicious attack. Without restrictions and controls, the logon process provides an unlimited access point for an attack to gain an unauthorized connection to the DBMS. Logon restrictions available to limit the success of attacks using automated attempts include the locking or disabling of accounts after a specified number of failures, limiting the number of failures to a specified period of time, and limiting the times during which accounts are accessible for logon. The logon process may also be used to exhaust database resources to process database connection requests thus denying authorized users access to the database. This form of a Denial of Service (DoS) attack may be thwarted by limiting the length of time the DBMS waits for a client to complete the logon process and the number of concurrent requests and connections a single user account may obtain. Inactive database connections may also be detected and terminated.

- *(DG0073: CAT II) The DBA will configure the DBMS to lock database accounts after three or an IAO-specified number of consecutive unsuccessful connection attempts within a 60 minute period. The counter may be reset to 0 if a third failed logon attempt does not occur before reset. Where this requirement is not compatible with the operation of a front-end application, the unsuccessful logon count and time will be specified and the operational need documented in the System Security Plan.*

- *(DG0133: CAT II) The DBA will configure the DBMS to set the duration of database account lockouts due to three consecutive unsuccessful logon attempts to an unlimited time that requires the DBA to manually unlock the account.*

- *(DG0134: CAT II) The DBA will configure where supported by the DBMS a limit of concurrent connections by a single database account to the limit specified in the System Security Plan, a number determined by testing or review of logs to be appropriate for the application. The limit will not be set to unlimited except where operationally required and documented in the System Security Plan.*

- *(DG0135: CAT II) For classified systems, the DBA will configure the DBMS to report to the interactive database user upon successful connection to the database the time and date of the last successful connection and the number of unsuccessful attempts since the last successful connection. Where not available in a DBMS configuration setting, a custom logon trigger or similar function is required.*

- *(DG0160: CAT III) The DBA will ensure database connection attempts are limited to a specific number of times within a specific time period as specified in the System Security Plan. The limit will not be set to unlimited.*

3.3.11 Least Privilege (ECLP)

3.3.11.1 Separation of Duties and Least Privilege

When an oversight responsibility is assigned to the same person performing the actions being overseen, the function of oversight is compromised. When the responsibility to manage or control one application or activity is assigned to one party yet another party is also assigned the privilege to the same actions, then neither party can logically be held responsible for those actions. These scenarios indicate a lack of separation of duties. Responsibility and accountability for actions is lost when privileges are not assigned following this principle.

Users granted privileges to perform unauthorized actions may do so either intentionally or unintentionally. This can lead to a number of problems including a compromise of the data or database and loss of accountability.

- *(DG0080: CAT II) The DBA will ensure privileges granted to application user database accounts are restricted to those required to perform the specific application functions.*

- *(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.*

- *(DG0120: CAT II) The DBA will ensure database application user roles are not granted unauthorized access to external database objects.*

- *(DG0121: CAT II) The DBA will ensure database privileges are assigned via roles and not directly assigned to database accounts. Privileges may be assigned directly to application owner accounts where the DBMS does not otherwise support access via roles.*

NOTE: *Any such exception must be supported by vendor documentation where not specifically addressed in a product-specific security compliance checklist.*

- *(DG0005: CAT II) The SA/DBA will ensure database administration OS accounts required for operation and maintenance of the DBMS are assigned the minimum OS privileges required by the specific DBMS to perform DBA functions.*

- *(DG0008: CAT II) The DBA will ensure database application objects are owned by an authorized application object owner account.*

- *(DG0085: CAT II) The DBA will ensure the minimum database administrative privileges are assigned to database administrative roles to perform the administrative job function.*

- *(DG0086: CAT II) The IAO will review monthly or more frequently the database privileges assigned to database administrative roles to ensure they are limited to the minimum required.*

- *(DG0063: CAT II) The DBA will restrict restore permissions on databases to DBAs and/or the database owners.*

- *(DG0077: CAT II) The DBA will ensure developers are not granted system privileges within a production database.*

3.3.11.2 Privileged accounts are accessible only by privileged users

DBA and other privileged administrative or application owner accounts are granted privileges that allow actions that can have a greater impact on database security and operation. It is especially important to grant access to privileged accounts to only those persons who are qualified and authorized to use them.

- *(DG0040: CAT II) The IAO will ensure access to the DBMS software installation account is restricted to IAO-authorized personnel only.*

- *(DG0041: CAT II) The IAO will ensure use of the DBMS software installation account is logged and/or audited to indicate the identity of the person who accessed the account.*

- *(DG0116: CAT II) The IAO will ensure database privileged role assignments are restricted to IAO-authorized accounts.*

- *(DG0124: CAT II) The IAO will ensure privileged database accounts are used only for privileged database job functions. The IAO will ensure non-privileged database accounts are used to perform non-privileged job functions.*

3.3.11.3 Use of privileged accounts is only for privileged functions

The use of privileged accounts for other than privileged functions can result in an unintentional action of high impact (e.g., deletion of all tables instead of a single table) usually as a result of the privilege to bypass protections to control or limit actions.

- *(DG0004: CAT II) The DBA will ensure custom application owner accounts are disabled or locked when not in use.*

- *(DG0042: CAT II) The IAO will ensure the DBMS software installation account is only used when performing software installation and upgrades or other DBMS maintenance. The IAO will ensure the DBMS software installation account is not used for DBA activities not related to DBMS file permission and ownership maintenance.*

- *(DG0051: CAT II) The DBA will monitor database batch and job queues to ensure no unauthorized jobs are accessing the database.*

3.3.12 Marking and Labeling (ECML)

A database user that does not know the sensitivity level of the data being accessed cannot be expected to protect it in accordance with requirements. While normally marking and labeling of the data is handled by the application displaying the data, many applications provided with the DBMS software may not provide this capability. Use or access to any application that cannot display sensitivity labels must be restricted to protect the data from inadvertent disclosure. Where the marking and labeling of the data can be configured by the DBMS, it must be assigned in accordance with the direction of the Information Owner.

- *(DG0087: CAT III) The DBA will configure DBMS marking and labeling of non-public data where required in accordance with the System Security Plan.*

3.3.13 Conformance Monitoring and Testing (ECMT)

The DBMS security configuration may be altered either intentionally or unintentionally over time.

- *(DG0088: CAT III) The IAO will ensure the DBMS is included in the periodic testing of conformance with vulnerability management and IA configuration requirements.*

3.3.14 Privileged Account Control (ECPA)

DBA and other administrative level privileges pose a threat to the entire DBMS if not properly assigned. These privileges require extra vigilance to ensure they are not assigned to unauthorized users or accounts.

- *(DG0117: CAT II) The IAO will ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.*

- *(DG0118: CAT II) The IAM will review DBA role assignments whenever changes to the assignments occur.*

3.3.15 Production Code Change Controls (ECPC)

Developers play a unique role and represent a specific type of threat to the security of the DBMS. Where restricted resources prevent the required separation of production and development DBMS installations, developers granted elevated privileges to create and manage new database objects must also be prevented from actions that can threaten the production operation.

- *(DG0089: CAT III) The DBA will ensure application developer database accounts are assigned limited privileges in order to protect production application objects.*

- *(DG0194: CAT II) The IAO will review privileges granted to developers on shared production/development database systems that allow modification of application code or application objects every three months or more frequently.*

- *(DG0195: CAT II) The SA/DBA will ensure developer accounts on a shared production/development host system are not granted operating system privileges to production files, directories, or database components.*

3.3.16 Resource Control (ECRC)

Database storage locations may be reassigned to different objects during normal operations. If not cleared of residual data, sensitive data may be exposed to unauthorized access.

- *(DG0084: CAT III) The DBA will ensure DBMS resource controls are enabled to clear residual data from released object stores.*

3.3.17 Audit Reduction and Report Generation (ECRG)

Audit record collection may quickly overwhelm storage resources and an auditor’s ability to review it in a productive manner. Automated tools can provide the means to manage the audit data collected as well as present it to an auditor in an efficient way.

- *(DG0083: CAT II) The IAO will ensure automated tools are available and implemented for review and reporting of DBMS audit records.*

3.3.18 Audit Record Retention (ECRR)

Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures.

- *(DG0030: CAT II) The DBA will ensure the DBMS audit trail data is maintained for a minimum of one year.*

NOTE: It is recommended that the most recent thirty days of audit logs remain available online. After thirty days, the audit logs may be maintained offline. Online maintenance provides for a more timely capability and inclination to investigate suspicious activity.

3.3.19 Security Configuration Compliance (ECSC)

As mentioned earlier in this STIG, the security of the DBMS is also dependent on the security posture of the supporting host system, network, and other applications that access it or have a dependency on it. If not secured, an exploited vulnerability through one of them can lead to a compromise of the DBMS.

- *(DG0175: CAT II) The IAO will ensure the DBMS host and related applications and components comply with all applicable DoD STIGs.*

3.3.20 Software Development Change Controls (ECSD)

The creation or maintenance of database objects is considered a configuration change of the database. For example, when a data table is created, storage resources are specified and utilized and access privileges assigned to the owner. In addition, changes to objects in the database causes changes in the DBMS data definition system tables. These activities are not appropriate for application users to either perform or instigate. Application users by definition and job function require only the permissions to manipulate data within database objects and execute procedures within the database. The statements used to define objects in the database are referred to as DDL statements and include CREATE, DROP, and ALTER object statements. (DDL statements do not include CREATE USER, DROP USER, or ALTER USER actions.) This requirement is included here as a production system would by definition not support changes to the data definitions. Where object creation is an indirect result of DBMS operation or dynamic object structures are required by the application function as is found in some object-oriented DBMS applications, this restriction does not apply. Re-use of static data structures to recreate temporary data objects are not exempted.

On shared production and development DBMS systems access identifiers that do not clearly indicate whether the DBMS or DBMS object being accessed is part of the production or development objects can lead to unintentional modification of production objects.

- *(DG0015: CAT III) The IAO will ensure database applications do not use DDL statements except where dynamic object structures are required.*

- *(DG0017: CAT II) The DBA will ensure software development on a production system is separated through the use of separate and uniquely identified data and application file storage partitions and processes/services.*

3.3.21 Audit Trail Backup (ECTB)

As critical data that contributes to the DBMS security posture, the audit data requires verification that it is included with other DMBS backup procedures.

- *(DG0176: CAT II) The DBA will ensure the DBMS audit logs are included in DBMS backup procedures.*

3.3.22 Audit Trail Protection (ECTP)

Audit data is frequently targeted by malicious users as it can provide a means to detect their activity. The protection of the audit trail data is of special concern and requires restrictions to allow only the auditor and DBMS backup, recovery, and maintenance users access to it.

- *(DG0032: CAT II) The DBA will ensure DBMS audit records are protected from unauthorized access.*

3.3.23 Warning Message (ECWM)

Without sufficient warning of monitoring and access restrictions of a system, legal prosecution to assign responsibility for unauthorized or malicious access may not succeed. A warning message provides legal support for such prosecution. Access to the DBMS or the applications used to access the DBMS require this warning to help assign responsibility for database activities.

- *(DG0179: CAT II) Where available, the DBA will ensure the DBMS is configured to display a warning message upon interactive user connection to the DBMS that complies with Chairman of the Joint Chiefs of Staff Memorandum (CJCSM) 6510.01 Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND), current as of 14 August 2006. This requirement may be fulfilled where the database user receives the warning message when authenticating or connecting to a front-end system that includes or covers the DBMS.*

3.3.24 Account Control (IAAC)

Database accounts that are not monitored for inactivity or removed when not longer authorized provide the potential for an unnoticed attack on or unauthorized access to the DBMS. The prompt removal or disabling of unused accounts helps to protect the DBMS from this basic form of unauthorized access.

- *(DG0070: CAT II) The DBA will ensure unauthorized database accounts are removed or disabled.*

- *(DG0074: CAT II) The DBA will monitor database account expiration and inactivity and remove expired accounts and accounts that are inactive for 35 days or longer or the site maximum limit.*

3.4 Enclave Boundary Defense

3.4.1 Boundary Defense (EBBD)

Network perimeter protections help restrict access to a DBMS to authorized users. When clients connect directly to a DBMS instead of accessing the DBMS through a mid-tier application system or architecture, then the DBMS must be configured to allow connection by a wider range of users. The ability to identify authorized users by their network location can protect the DBMS from a larger pool of potential malicious users.

- *(DG0186: CAT II) The IAO will ensure the DBMS is protected from direct client connections from public or unauthorized networks.*

3.4.2 Remote Access for Privileged Functions (EBRP)

Remote administration provides many conveniences that can assist in the maintenance of the designed security posture of the DBMS. On the other hand, remote administration of the database also provides malicious users the ability to access from the network a highly privileged function. Remote administration needs to be carefully considered and used only when sufficient protections against its abuse can be applied.

- *(DG0157: CAT II) The DBA will ensure remote administration of the database is not enabled or configured unless mission and/or operationally required and authorized by the IAO.*

- *(DG0158: CAT II) The DBA will configure auditing of all actions taken by database administrators during remote sessions.*

- *(DG0159: CAT II) The IAO or IAM will review daily audit trails of remote administrative sessions to discover any unauthorized access or actions.*

- *(DG0198: CAT II) The SA/DBA will ensure remote administration connections to the database are restricted to dedicated and encrypted network addresses and ports.*

3.5 Continuity

3.5.1 Protection of Backup and Restoration Assets (COBR)

Lost or compromised DBMS backup and restoration files may lead to not only the loss of data, but also the unauthorized access to sensitive data. Backup files need the same protections against unauthorized access when stored on backup media as when online and actively in use by the database system. Also, the backup media needs to be protected against physical loss. Most DBMSs maintain online copies of critical control files to provide transparent or easy recovery from hard disk loss or other interruptions to database operation.

- *(DG0114: CAT II) The DBA will ensure files critical to database recovery are protected by employment of database and OS high-availability options such as storage on RAID devices.*

- *(DG0064: CAT II) The DBA will ensure access to database backup and recovery files are restricted to the database and/or OS backup and recovery processes, DBAs, and database backup/recovery operators.*

3.5.2 Data Backup Procedures (CODB)

The DBMS and the data it stores can be lost as a result of a disaster or compromise. Backup of the DBMS and its data are critical to maintaining availability.

- *(DG0013: CAT II) The DBA/SA will ensure backups of database data, configuration, and other files critical to database operation are performed at intervals consistent with the database's assigned criticality level.*

3.5.3 Disaster and Recovery Planning (CODP)

Like other automated systems, the DBMS is vulnerable to loss. The identification of the threats that would cause a loss, the types of loss that may occur, the likelihood that the loss might occur and the value of the loss all need to be assessed to complete a disaster and recovery plan for the DBMS. The DBMS disaster and recovery plan should be included with the overall site plan. Testing of the disaster and recovery plan for the DBMS ensures that the plan is viable.

- *(DG0020: CAT II) The DBA will ensure the DBMS backup and recovery strategy is documented, implemented, and tested at least semi-annually.*

3.5.4 Backup Copies of Critical Software (COSW)

The integrity of the DBMS is lost when the DBMS software is not reliably available. Loss or corruption of the software can occur during maintenance or update of the software, from hardware or host system loss or malfunction, or from unauthorized modifications.

- *(DG0187: CAT II) The DBA will ensure critical database software directories are backed up.*

3.5.5 Trusted Recovery (COTR)

A database startup is dependent on configuration files, data files, control files, and application files. Some DBMSs may provide additional means to verify or identify files are authorized or trusted versions. Where available, these additional protections should be employed.

- *(DG0115: CAT II) The DBA will configure the DBMS to use only authorized software, data files, or other critical files during recovery.*

3.6 Vulnerability and Incident Management

3.6.1 Vulnerability Management (VIVM)

DBMS software is upgraded and patched when supported by the vendor. When support is no longer provided, the DBMS version is not tested for newly discovered vulnerabilities nor provided with patches or updates. Unsupported DBMS software is more vulnerable to attack than supported versions. When security patches are not installed to protect against known vulnerabilities, the DBMS is easily compromised.

- *(DG0001: CAT I) The IAO will ensure unsupported DBMS software is removed or upgraded prior to a vendor dropping support.*

- *(DG0002: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading DBMS systems 6 months prior to the date the vendor drops security patch support.*

- *(DG0003: CAT II) The DBA will ensure all applicable vendor-provided security patches are installed.*

APPENDIX A. RELATED PUBLICATIONS

Government Publications:

Department of Defense Directive 8500.1, “Information Assurance”, 24 October 2002.

Department of Defense Instruction 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003.

Department of Defense, “Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance” 6 July 2006.

Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," 15 March 2002.

DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," 01 April 2004.

Department of Defense Instruction 8551.1, “Ports, Protocols, and Services Management (PPSM),” 13 August 2004

NSA Guide to the Secure Configuration and Administration of Oracle9i Database Server, 02 October 2003.

NSA Guide to Secure Configuration and Administration of Microsoft SQL Server 2000, 02 October 2003.

Defense Information Systems Agency, Enclave Security Technical Implementation Guide.

Defense Information Systems Agency, Network Infrastructure Security Technical Implementation Guide.

Defense Information Systems Agency, Windows 2000/XP/2003 Addendum.

Defense Information Systems Agency, UNIX Security Technical Implementation Guide.

Defense Information Systems Agency, OS/390 Security Technical Implementation Guide.

Defense Information Systems Agency, Web Server Security Technical Implementation Guide.

Defense Information Systems Agency, Desktop Application Security Technical Implementation Guide.

Defense Information Systems Agency, Application Security and Development Security Technical Implementation Guide.

This page is intentionally left blank.

APPENDIX B. LIST OF ACRONYMS

ACL	Access Control List
AIS	Automated Information Systems
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
CA	Certificate of Authority
CAC	Common Access Card
C&A	Certification and Accreditation
CIS	Center for Internet Security
COTS	Commercial-Off-The-Shelf
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DB	Database
DBA	Database Administrator
DBMS	Database Management System
DDL	Data Definition Language
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DML	Data Manipulation Language
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
FIPS	Federal Information Processing Standards
FSO	DISA Field Security Operations
GOTS	Government-Off-The-Shelf
HTTP	Hyper Text Transport Protocol
HTTPS	Secure Hyper Text Transport Protocol
I&A	Identification and Authentication
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
INFOCON	Information Operations Condition
IP	Internet Protocol
IT	Information Technology
MS	Microsoft
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
OS	Operating System
PKI	Public Key Infrastructure

RAID	Redundant Array of Inexpensive Disks
RBAC	Role-Based Access Control
SA	System Administrator
SAMI	Sources and Methods Intelligence
SANS	SysAdmin, Audit, Network, Security Institute
SIPRNet	Secret Internet Protocol Router Network
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRR	Security Readiness Review
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
WWW	World Wide Web

.GOV	World Wide Web Uniform Resource Locator Domain for the U.S. Government
.MIL	World Wide Web Uniform Resource Locator Domain for the U.S. Military