ENTERPRISE RESOURCE PLANNING

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

7 December 2006

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION

This Enterprise Resource Planning (ERP) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements and implementation details for Commercial-Off-The Shelf (COTS) ERP application software. For this STIG, ERP software will refer to all commercially available software packages that supply one or more of the functions generally found within ERP packages. The functions include but are not limited to Human Resources, Financial processes, Customer Relations Management (CRM), sales, warehousing, inventory control, and manufacturing.

This STIG provides security configuration guidance for software products designed to deliver enterprise-class system ERP functionality. While the boundaries of the ERP discipline are such that there is no authoritative definition of an ERP product, Section 2, Enterprise Resource Planning Overview, provides a generic description of the elements characteristic of most ERP products. Section 3, ERP General Security Requirements, provides general guidance for ERP products.

This document is used in conjunction with the other STIGs developed by the Defense Information Systems Agency (DISA). The operating system (OS) STIGs provide crucial guidance for securing the platforms on which the ERP products run. The STIGs that cover database, networking, and web server products provide guidance to ensure those services used by ERP products also support a secure environment.

1.1 Background

ERP products are used by business to standardize and integrate their business processes. These products help to implement new regulatory compliance requirements, changes in business processing standards, and better leverage business information while freeing up organizational resources from the complexities of data processing so that they can focus on their core competencies.

The Department of Defense (DoD) is now deploying ERP systems to manage personnel processes and accounting/financial applications throughout its infrastructure. Though there are some aspects of ERP functionality that the DoD cannot use, the modularity of the available packages allows for the purchasing of only the functionality needed. As with commercial businesses, the use of ERP provides the DoD with better regulatory compliance and better use of current business “best practices”, while freeing up resources which can then be applied to mission critical projects.

ERP products evolved from mainframe based accounting and human resource applications, where they depended upon monolithic mainframe architecture and closed proprietary networks for security, into distributed server based applications on open networks, which lack the implied security imposed from the legacy architectures. While this transformation was taking place, little thought was given to adding security. As open networking grew into the Internet these applications were exposed to more threats from both inside and outside the organization deploying ERP. To combat these new threats security was grafted onto the ERP applications and vendors gave more guidance on isolating the ERP application, and its associated servers, from

the organizational network, allowing only restricted access into the network segment supporting ERP. Though these initiatives mitigate the external threat, the internal security controls within the application and its associated servers remained weak leaving the application vulnerable to exploitation if an attack succeeds in breaching the security perimeter. Additionally, because of the privileges granted the application in accessing system services, a compromised application leaves the enclave network vulnerable to an internal attack, if additional mitigating controls are not in place.

The goal of this document is to provide guidance that allows the power of ERP products to be utilized, while preventing that power from being exploited to degrade the confidentiality, integrity, or availability of the data under the control of the product. It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

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.

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

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

1.3 Scope

This document describes security requirements to be applied to ERP products used in DoD environments. The information is designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with the creation of more secure ERP configurations. As noted in the previous section, application of the requirements is intended to provide a certain level of assurance. Individual sites must determine if this level of assurance is appropriate to their environment.

This document provides general security guidance. Vendor implementation of ERP functionality does vary; and most commercial products provide only subsets of all the functions generally associated with ERP.
Future versions of this STIG will provide specific guidance for the following:

- SAP ERP
- PeopleSoft ERP (or the Oracle product that combines PeopleSoft with Oracle's ERP products)

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 provide an attacker immediate access into the ERP, provide access into system or functional configuration, or programming areas, or allow an attacker to gain access to the operating system or database via the ERP application.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1.1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these

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. ENTERPRISE RESOURCE PLANNING OVERVIEW

ERP is a term used to describe a class of software that implements and integrates the business processes normally found in a business environment. By optimizing business processes and encapsulating them into logical modules, ERP software allows an organization to leverage their data and integrate their business processes to better fulfill their primary function. Benefits include faster financial close (resulting in more timely knowledge of financial results), timelier billing and receivables processing, more efficient accounts payable, optimized operations, and improved forecasting and planning.

2.1 Introduction

ERP systems consist of functional modules that support business requirements such as Human Resources, Financials, or Inventory Control. The modules can be used individually or in conjunction with other modules as needed. The individual modules contain the business processes necessary to complete their intended function. These software processes need to be reconciled to the business processes used by the implementing organization. The organizational business processes may be modified to better fit with the ERP software (business process re-engineering), or the software may be tailored to the organization's processes. This tailoring is done by modifying the configuration of the module (by use of configuration tables) with little or no modification of the underlying code supplied by the vender. Additionally, the ERP packages all have a means of modifying the information displayed and stored within the system to match the requirements of the implementer. Though industry specific modules can be purchased some tailoring is always required.

ERP packages contain utilities to assist in the tailoring of the modules. Often the packages contain a development environment where the system is configured, and interfaces to other Automated Information Systems (AIS) used within the organization are developed.

If modifications are made to the underlying ERP source code to tailor the ERP to the business process of the organization, problems may arise when upgrading the ERP release level or applying vendor patches. This can lead to a loss of functionality in production or during upgrade preparation.

The data used by all modules is stored in a database. The database tables overlap where the module functionality overlaps to facilitate the process flow. Though this is useful for business process efficiency it does lead to security concerns in that a user must have access to parts of a table within the database without necessarily having a need to access the whole table. A simple example of this would be a warehouse shift supervisor would need-to-know the home phone number for an on call employee. The on call information can be retrieved in a shift scheduling table but the phone information can be retrieved from the personnel table stored in the HR modules. However, the personnel records also contain information that the supervisor does not need to access and this access should not be granted.

2.2 ERP Processing Models

ERP systems are often deployed in either two-tier (client/server) or thee-tier (client/application server/database server) implementations.

2.2.1 Two-Tier Model

In a two-tier model the server holds the database and database software. The business processes, the programs, are downloaded to the client and executed on the client's system and the client system fetches the data from the database server. Access control is maintained by the business logic executing on the client system.

Some advantages of the two-tier model:

- The cost savings on server hardware.
- Expansion of the number of clients does not create a server bottleneck because the business process code is executing on the client systems.

Some disadvantages of the two-tier model:

- Increased network load.
- Data may be transferred to the client system that the user may not be authorized to view. Though the business logic will not allow the data to be displayed, the data is available on the client system and could be compromised.
- The database server must be visible to the client systems exposing it to additional vulnerabilities.
- Security auditing is difficult.

2.2.2 Three-Tier Model

In a three-tier model the client uses a browser or thick client (graphical user interface) to access the application server. The business processes, the programs, are executed on the application server and fetch the data from the database server. Access control is maintained by the business process logic executing on the application server.

Some advantages of the three-tier model:

- Decreased network load.
- Scalable.
- No data is transferred to the client system that the user is not authorized to access.
- The database server needs to be visible only to the application server decreasing its exposure to vulnerabilities.
- Security auditing is centralized and simpler.

Some disadvantages of the three-tier model:

- Increased server cost (additional server need for the application server).
- Increase in usage can create a server bottleneck at the application server. This may require additional hardware to be purchased for additional application servers and load balancing hardware/software to balance the load between the multiple parallel application servers.

2.3 ERP Security approach

ERP applications generally depend upon access controls enforced by the application code rather than operating system access controls or database access controls. Though they may have provisions for using third party or network authentication, in their native mode, they depend upon application code to authenticate the users via passwords. When evaluating whether to use the default authentication system, verification that the native system will support the DoD requirements for enforcing strong passwords is mandatory. To further enhance security, the ERP applications depend upon a strong perimeter defense between the ERP servers and rest of the enclave network.

These applications usually execute under the control of one or more system privileged accounts. All of their database accesses are made via a single database administrator account that owns all ERP objects within the database.

2.3.1 Development and Production Environments

Many ERP applications have a release control and management mechanism implemented within their design. This mechanism normally consists of a development environment, a Quality Assurance (QA) environment, and a production environment or some combination of these environments

The development environments are used during the initial implementation project, as well as for development of enhancements and follow up modules. It is also used to test patches and updates from the vendor and major new releases of the ERP application. Table configuration settings are made in the development system to custom tailor the ERP application to the needs of the organization. Programming for additional system functionality and reports takes place here, and custom interfaces to existing applications are created. The developer, prior to release for Quality Assurance testing, performs unit testing of new functionality and code.

The QA environment is used to perform functional integration testing to assure that the ERP configuration and code perform as designed, without injecting new vulnerabilities or instabilities into the base ERP application. QA should reflect the production environment as closely as possible. Dedicated QA personnel and subject matter experts, to avoid bias introduced into the process by the developers, normally perform the integration testing. This testing should be thorough and should be done without privileged access in order to verify that the correct access levels are being granted to the end users. All aspects should be tested including functionality, documentation, and security.

If the application does not pass QA testing, it is returned to the development environment for correction. No modifications are made to the configuration or code in the QA environment. When the corrections have been made, the application is returned to the QA environment for thorough testing. Unit testing is not normally performed in the QA system, although occasionally the lack of adequate data in the development system will require that the QA system be used. In any case, after unit testing of changes is completed, it must be followed by QA (integration) testing.

Because of the complexity of many ERP implementations a comprehensive change control process, including a Change Control Board (CCB), needs to be implemented. The CCB will review the change, its testing, and the implementation schedule to ensure that all necessary documentation and testing have been completed correctly and then approve the change for implementation.

Since the movement of an application from development to QA and finally to production can be a complex process, many ERP packages have a component to assist and control the process. These packages often require that the production environment be connected to the development and QA environments via a network connection. Care should be taken when designing and implementing these network connections to isolate the development environment from the production environment.

This isolation should ensure end users do not mistakenly access the test environment compromising test data with real data and processing test data as if it were real. Additionally, the production environment needs to be protected so that development, unit testing and QA integration testing do not occur in the production environment compromising production data.

2.4 Mobile code

Care needs to be taken when selecting and implementing an ERP solution to ensure that any mobile code used is compliant with DoD 8500.2 and the DoD memorandum,
Policy Guidance for the Use of Mobile Code Technologies in DoD Information Systems.

3. ERP GENERAL SECURITY REQUIREMENTS

This document takes into consideration the Sarbanes-Oxley Act of 2002 (SOX), specifically in the areas of segregation of duties and access to sensitive or powerful transactions, and the Health Insurance Portability and Accountability Act (HIPAA), particularly in the area of privacy. However, this document does not fully address these issues and is not intended to do so.

ERP User Roles and responsibilities within ERP systems are:

- Information Assurance Officer (IAO) – Responsible for implementing and maintaining user and access security on the ERP system.

- Information Assurance Manager (IAM) – Responsible for management and oversight of all ERP Information systems.

- ERP Administrator – Responsible for maintaining the ERP internal configuration and tables and to keep the systems operating at peak efficiency.

- System Administrator (SA) – Responsible for the operating system on which the ERP application resides.

- Developer – Programmer responsible for ERP system customization, developing reports and writing interfaces for ERP applications.

- User – Refers to functional users who have responsibility for a specific functional module within the ERP system such as finance, materials management, human resources, etc.

- Data Base Administrator (DBA) – Responsible for maintaining the database(s) for the ERP application.

Access and privileges are assigned to users based on a collection of transactions and authorization objects, which grant permissions to each field in the object. Examples of fields are activities (read only, write, execute, etc.), organizational units (plant, company code, organization), document type (purchase order, invoice, general ledger), and a plethora of other variables. An object might grant write access to factory 046 for warehousing receiving actions. Proper use of these security tools allows user access to be customized to their specific business needs. The permissions, needed to perform a specific task or job, are combined into security roles. Specific roles should be designed and granted to users on a need-to-know basis.

Some vendors use a security schema, which is based on “row level” security, but the principals involved are the same.

3.1 System Requirements

It is imperative that system security requirements are set up in such a way that the integrity of the application remains strong. ERP application integrity depends on properly managing the overall processing environment. The operating system should include all current OS patches, anti-

spyware and virus detection programs with the current definition files. The current version of the STIG will be applied to the ERP host system to ensure that all IAVM have been applied prior to loading any ERP application. Proper system management helps to protect system hardware, software and application data from unauthorized access and improper modification or disclosure of sensitive information.

- *(ERP000500: CAT II) The System Administrator will ensure the ERP systems are compliant with the OS STIG.*

3.2 Network Requirements

ERP systems applications depend on network security to prevent inappropriate exposure of resources, which could circumvent application controls. Based on the three tier model the network should be segmented with proper Access Control List (ACL) and/or firewalls should be utilized to ensure security for the entire ERP solution. Based on the three-tier approach the Web-front end should be separated from the Application backend. Further separation should occur between the application server and the backend database. Some ERP applications will not function properly if not configured to vendor specifications; therefore, consideration must be given to the ERP vendor's network security recommendations. All ERP application will comply with the Network Infrastructure STIG. Any network deviations are subject to the approval of the local Information Assurance Manager (ISM) and the final approval from the Designated Approving Authority (DAA).

- *(ERP000600: CAT II) The System Administrator will ensure the host network is compliant with the Network Infrastructure STIG.*

3.3 Database Requirements

A layered approach to overall application security provides the highest level of security. Therefore, the databases must be compliant with the Database STIG, to protect the ERP application as well as database accounts that are stored in the database. A single and independent instance of the database should be utilized for the ERP backend database. Ensure that only those accounts that are need for the database are defined. Remove or disable all other accounts.

- *(ERP000700: CAT II) The DBA will ensure the database(s) associated with ERP applications are compliant with the Database STIG.*

3.3.1 Database userids/Accounts

Because the ERP application requires elevated privileges for a single userid to perform all database access for the application, the database will not be shared with any other application. Isolating the ERP data in this manner will limit any unauthorized access solely to data within the ERP application should the ERP database userid be compromised. All user passwords should be encrypted using the FIPS-140-2 standards.

- *(ERP000720: CAT I) The DBA will ensure the ERP specific database is not shared with any other databases or applications.*

- *(ERP000730: CAT I) The DBA will ensure encryption is enabled on all passwords.*

- *(ERP000740: CAT II) The IAO will ensure DoD PKI certificates are used.*

3.4 Installation Requirements

Application integrity is most vulnerable to intrusion before applications have been completely configured for secure operation. Vendor delivered software has inherent vulnerabilities that need to be addressed during installation and prior to connection to the production network. Because of this vulnerability, the application will not be connected to the network before security requirements presented in this STIG are in place. The appropriate OS STIG will be applied before the ERP system is loaded onto the host system.

- *(ERP000800: CAT II) The IAO and ERP Administrator will ensure system parameters, which reside in operating system files, are correctly set before the ERP system is put into production.*

- *(ERP000810: CAT II) The IAO and ERP Administrator will ensure the appropriate OS STIG is applied.*

3.4.1 Default Application Userids and Accounts

Since applications are delivered containing userids and accounts that have well known default passwords, malicious users can make use of these accounts and userids unless action is taken prior to deployment. Vendor delivered userids will be removed or passwords changed to non-trivial passwords that conform to the DoD standards for passwords.

- *(ERP000820: CAT II) The IAO will ensure the removal of default user accounts, the changing of their passwords to generated passwords, before moving the application to production.*

- *(ERP000830: CAT II) The IAO will ensure system parameters, which govern the auto-regeneration of user accounts (for example, SAP*) are set so that the system does not regenerate the account automatically (with well-known password).*

3.4.2 Application File Protection

To protect the integrity of the application, all files to include: files installed within the application, files that are being used by the application, and/or files created by the application will be protected from operating system level access. This file protection will also extend to the ERP user to disallow modification by unauthorized system users.

If some level of file access is needed (for example, the uploading of spreadsheet data files), directory access will be limited solely to the needed data directory, and with minimal read/write

user access rights. Additional security transactions and objects may govern access to execute operating system commands

- *(ERP000850: CAT II) The IAO and ERP Administrator will ensure all files installed with the application, or created by the application, are protected from system level access or modification by unauthorized system users.*

3.4.3 Implementation Project Controls

ERP application modifications can change the security posture impacting the confidentiality, integrity, and availability of the application. A process of review mitigates potential vulnerabilities created by the changes.

- *(ERP000860: CAT III) The IAO and ERP Administrator will ensure system changes are reviewed and approved by the Change Review Board (CBR) prior to implementation.*

ERP systems have separate environments for development, QA, and production. Each environment is configured with progressively restrictive controls. Only appropriate personnel will have access to each environment. During implementation, controls are put in place by correctly configuring the application to reflect the final production environment.

- *(ERP000870: CAT II) The IAO will ensure during deployment the ERP security controls reflect the intended production environment.*

3.5 Application Access Controls

This section identifies the discretionary access controls necessary to ensure that access to ERP resources are effectively managed and controlled within ERP systems.

- *(ERP001000: CAT II) The IAO will ensure security controls, requirements, responsibilities, and procedures are documented.*

Controls will be in place to support segregation of duties for security, application administration, development, and user access.

- *(ERP001100: CAT II) The IAO will ensure application role based access control enforces separation of duties.*

All available layers of security control will be utilized to form a layered “defense in depth”. This includes limiting both transaction and security object access for a given function. For example, loose control at the object level will not be permitted based on the assumption that the user will not have access to the transaction.

In addition, the following security authorization tools will be used:

Assignment of user ID into user groups
Authorization to run programs

Authorization to view/ update tables
Batch administrator authorizations

- *(ERP001150: CAT II) The IAO will ensure all available security control mechanisms are utilized in a layered defense.*

Controls will be in place to ensure that security administration access is only assigned to the authorized personnel. Access to the security software or access control mechanism of a system could allow security controls to be overridden. Access restricted to the SA ensures that the security controls remain as intended.

- *(ERP001200: CAT II) The authorized personnel will ensure access to the mechanism, which provides the system's access control, is restricted to those responsible for administering security for that system.*

- *(ERP001300: CAT II) The SA will ensure the ability to change a userids group membership is restricted to authorized security administrators.*

Access will be granted on a need-to-know basis and must be approved by the information owner or governing authority. Excessive access could allow a user to perform abusive or unauthorized acts, or commit errors that could result in unauthorized disclosure, modification or destruction of sensitive data. Excessive access also raises risk levels should a user's account and password be compromised.

ERP roles and responsibility guidelines will exist for the ERP application to further detail the sensitivity of data in each of the ERP application modules.

- *(ERP001400: CAT II) The IAO will ensure access to information; assets and resources are only granted to users to support only organization or module.*

- *(ERP001500: CAT III) The IAM will ensure an up-to-date classification guide exists for the application.*

There will be a documented procedure for unlocking users and changing passwords. Users must provide proof of identity before reactivation of the userid can occur.

- *(ERP001600: CAT III) The IAO will ensure there is a documented procedure that provides positive identification of the user prior to a password reset or an account being unlocked.*

Userids will not remain active on the system longer than necessary. This ensures that these userids are unusable and not available for unauthorized users to log on.

- *(ERP001700: CAT II) The IAO will ensure userids are disabled after 60 days of inactivity.*

- *(ERP001750: CAT II) The SA and the ERP Administrator will ensure userids are disabled after 60 days of inactivity.*

To protect the integrity of the application, authorizations will be modified from the installation defaults in order to tightly control access. All User Access Roles (authorizations) should be created and managed in accordance with security policy and with SOX and HIPAA Audit controls in mind.

- *(ERP001800: CAT III) The IAO will assist the SA in defining all roles and responsibilities to all user fields, taking into consideration SOX and HIPAA regulatory recommendations.*

Vendor delivered security roles, which are presented as models, are usually designed with ease/speed of implementation taking preference over best security practice. While these roles may be used as a reference, the authorizations must be reviewed and scaled down to least privilege. Over reliance on vendor models is a common mistake made in ERP implementations

- *(ERP001850: CAT II) The IAO will ensure unnecessary default roles are not being used and that required roles have the least privileged access.*

3.5.1 Developer Access

In typical ERP installations, there is usually a development, a QA test system, and the production system. The development system contains master copies of the ERP configuration and program source code. There is normally little or no data in the configuration master. Program development and new configuration take place in this system. The QA test environment is used for integration testing of code and configuration changes. This environment should be very similar (or identical) to the production environment.

ERP applications provide a control mechanism to move changes to QA test environment for end user testing and then to production after testing is completed and test cases are signed off. Access to the vehicle that moves these changes will be tightly controlled. Developers do not have the security permissions necessary to transport their own changes to production. The ERP production application is set so that configuration and program changes cannot be made directly there.

Developer access should be restricted to development and QA test environment areas only, if necessary, a developer may have read-only access to production in order to check their changes. A change control process is used to advance any changes to the production system and will include the approval for use. Developer's will access ERP Development and Test systems with a unique userid and password. This prevents an unauthorized user from writing code, promoting the code to production, and then executing the code without any approval, checks or balances.

Developers do not have authorization to run code in debug mode in production. Debug mode provides the capability to step through program code, potentially stepping over security authorization checks.

Additionally, advanced privileges granted to facilitate development present another avenue for the compromise of the application once development is complete. Failure to remove these privileges could result in unauthorized disclosure, modification or loss of production information by someone exploiting userids with these privileges.

- *(ERP002000: CAT I) The ERP Administrator will provide documented procedures for software updates.*

- *(ERP002100: CAT II) The ERP Administrator and IAO will review all system changes and customization prior to implementation in production to ensure they do not compromise the security of the system.*

- *(ERP002200: CAT II) The IAO will remove any advanced privileges granted to developers during installation before moving the application to production.*

- *(ERP002300: CAT II) The ERP Administrator will ensure testing of all software or services is completed in the QA environment before moving the application to production.*

- *(ERP002400: CAT II) The IAO will ensure programmers have only userids in development and QA areas of an ERP application.*

NOTE: If there is an emergency situation the IAO may need to provide read-only access in production.

- *(ERP002500: CAT II) The IAO will review and approve all software changes before integration into the production system. All software changes need to have a back out plan before changes can occur on a production system.*

- *(ERP002600: CAT II) The IAO and ERP Administrator will ensure developers do not have the ability to run programs in debug mode in the production system.*

3.5.2 User Access

There will be unique identification in place for each system user. A user is either an individual or an executing process/service that accesses a computer resource. Actions performed by a user within the application will be traceable to an individual user account. Failure to implement this practice can compromise the integrity of data and eliminate the usefulness of audit trails.

- *(ERP003000: CAT I) The IAO will ensure all ERP accounts are protected by strong, non-default passwords.*

- *(ERP003100: CAT I) The IAO will ensure application userids are unique ID's.*

- *(ERP003200: CAT III) The IAO will ensure information such as name and related access information is associated with each userid.*

- *(ERP003300: CAT II) The IAO will ensure all user actions are audited to individual userids.*

- *(ERP003400: CAT II)The ERP Administrator will ensure the system accounts are disabled after three unsuccessful login attempts.*

- *(ERP003500: CAT II) The IAO, SA, and the ERP Administrator ensure userids are disabled after 30 days of inactivity.*

- *(ERP003600: CAT II) The IAO will ensure non-privileged users are not able to perform privileged functions.*

- *(ERP003650: CAT I) The ERP Administrator and the IAO will ensure an application client authenticates only to the appropriate application server.*

Password protection alone is not a strong enough mechanism, as it is too easy to break into applications where only passwords are used for authentication. The PKI certificates will not be test certificates. DoD will issue these certificates even in the development, and QA test environments. The ERP Application will utilize a Certificate Revocation List (CRL) to ensure proper certificates are used.

- *(ERP003700: CAT II) The IAO will ensure applications only accept DoD issued PKI certificates appropriate for the application's MAC level for all environments to include development, QA test and production.*

- *(ERP003750: CAT III) The IAO will ensure MAC I applications only accept DoD Class 4 certificates tokens. MAC II and MAC III applications may accept either DoD Class 3 or Class 4 certifications on tokens or on the local disk.*

- *(ERP003800: CAT II) The IAO will ensure the ERP Application does not honor non – DoD issued certificates.*

- *(ERP003850: CAT I) The ERP Administrator and the IAO will ensure the application users cannot circumvent the intended user interface to access resources in its supporting infrastructure.*

Users should only have access to an application for as long as they are actively using the application. Session limits will be in place to time out the session after a specified time of inactivity occurs. This must be done to ensure no person other than the assigned user is using the user's session.

- *(ERP003900: CAT II) The ERP Administrator and IAO will ensure session limits exist for the application. The session limit is 15 minutes.*

- *(ERP003950: CAT II) The IAO will ensure a process is in place for immediate notification when a user no longer has a need to access the ERP application their userid is disabled.*

3.6 Password Guidelines

Accounts must be protected from being accessed by unauthorized users. When an account is created for a user, that user must be given a temporary password. The IAO will brief the user on implementation of password protection. The IAO will utilize the DoD password policy for all user accounts.

- *(ERP004000: CAT III) The IAO will ensure user account passwords conform to DoD password policy and each user is instructed on the policy upon receiving a temporary password.*

All passwords will be stored in an encrypted format. The application account name and password will not be visible to the host or client operating system.

- *(ERP004100: CAT II) The IAO will ensure user account passwords are stored in an encrypted format using FIPS 140-2 compliant encryption; NIST validated cryptography or NSA approved cryptography.*

Application account logons should be limited to three failed logons before they become locked. This requirement reduces the ability for password cracking programs to be used successfully. The IAO will set the duration of the lock time to a specific length as approved by the IAO for the application or site or require a manual reset. The duration should be set appropriately for the environment; keeping in mind that the longer the duration, the more protected the accounts will be from password cracking programs. Passwords will be complex in nature to ensure they are not easily guessable.

- *(ERP004200: CAT II) The IAO and ERP administrator will ensure ERP passwords are a minimum of eight characters, have at least one non-alphanumeric character (special) character, one number, and system parameters is set to enforce same.*

- *(ERP004300: CAT III) The IAO will ensure users account passwords do not contain consecutively repeating characters and system parameters are set to enforce the same.*

- *(ERP004400: CAT III) The IAO will ensure users account passwords differ from the previous five passwords and system parameters are set to enforce the same.*

- *(ERP004500: CAT II) The IAO will ensure user account passwords expire every 60 days and will be a minimum of eight characters in length with a mix of upper and lower case, and also with special characters*

- *(ERP004600: CAT III) The IAO will ensure users are not allowed to change their user account passwords more than once every 24 hours without IAO approval.*

3.7 Special Considerations for Applications with Tightly Interconnected Production and Development Environments

The production, QA test, and development environments should all be separate. Development must take place in the development environment then moved to the QA test environment to be tested for functionality and user test. Changes should be approved prior to moving into the production environment. A strict change control process will be in place and followed without exception.

- *(ERP005000: CAT III) The IAO will ensure all changes to production software, hardware, and communication links are managed through a change control process.*

- *(ERP005100: CAT II) The IAO will ensure modifications to systems and networks are evaluated for impact to security controls.*

- *(ERP005200: CAT III) The ERP Administrator and IAO will ensure user acceptance testing is performed and user sign-offs are obtained before changes are moved into production.*

- *(ERP005300: CAT II) The ERP Administrator will ensure the application environment does not use unnecessary services or software within the environment.*

- *(ERP005400: CAT II) The ERP Administrator and the IAO will ensure a documented process is in place to ensure unnecessary custom code is not included in a release.*

- *(ERP005500: CAT II) The ERP Administrator will ensure application processes run with only privileges necessary for proper operation. This includes background user ID's needed by 3rd party "bolt on" products.*

- *(ERP005600: CAT II) The ERP Administrator will ensure the production environment is on its own server. The QA and development environment may reside on the same server.*

3.8 Application Design FeaturesRemote Access to ERP Applications

All remote connections to the ERP systems by administrative users will be encrypted in order to remove the possibility of using the credentials for an attack. These connections will be used to perform administrative functions including application account password resets and account management.

- *(ERP006000: CAT I) The IAO will ensure all administrative connections to the application are encrypted using FIPS 140-2 compliant encryption, NIST validated cryptograph, or NSA approved cryptography depending on the classification of the data residing within the application.*

- *(ERP006100: CAT II) The IAO will ensure all remote user access to the application is encrypted using FIPS 140-2 compliant encryption, NIST Certified cryptography or NSA*

approved cryptography depending on the classification of the data residing within the application.

- *(ERP006200: CAT I) The IAO will ensure all remote user audit trails are recorded.*

- *(ERP006300: CAT I) The IAO will ensure the application adequately validates user inputs before processing.*

3.8.1 Mobile Code

Application code will be compliant with the DoD mobile code policy if mobile code is used.

- *(ERP006400: CAT I) The ERP Administrator will ensure the application does not transmit unsigned CAT 1 or CAT 2 mobile code.*

- *(ERP006500: CAT II) The SA and ERP Administrator will ensure the application does not transmit mobile code that attempts to access local operating system resources or establish network connections to servers other than the application server.*

- *(ERP006600: CAT I) The SA and ERP Administrator will ensure the application does not execute mobile code without requiring and validating digital signatures.*

- *(ERP006700: CAT I) The SA and ERP Administrator will ensure the application does not utilize any type of mobile code for which there is no established policy.*

- *(ERP006800: CAT I) The SA and ERP Administrator will ensure the application does not send e-mail messages that include executable code.*

3.9 Logging

Reviews should be performed on application logs daily. The purpose of these reviews is to ensure no one is attempting to gain unauthorized access by guessing passwords and that any unauthorized transaction attempts are mistakes and not malicious.

- *(ERP007000: CAT II) The IAO and SA will ensure the application logs are reviewed daily.*

- *(ERP007100: CAT II) The IAO and SA will ensure the user audit logs are reviewed daily.*

3.10 Data Protection

Data is protected by strict controls of ERP userids and data access roles, which are assigned to each user. The roles are maintained at the field level and are granted levels such as read, write, delete, etc., for any particular modules in the application. Sensitive data at rest is encrypted at the data owners' discretion to protect from unauthorized viewing. Field level checks (user input) are performed to check for allowed input in order to protect the data integrity.

Both printed and application data should be protected in order to maintain confidentiality and integrity of the data. Procedures will be in place to mark printed material with sensitivity level if it does not appear on the report.

3.10.1 Data at Rest

Data at rest will reside inside the server's database in a protected manner. An encryption method will be used for protecting both the ERP user password and the data contained in the database. Only authenticated and specific authorization will be utilized along with file protection standards indicated previously. The ERP data owner has the rights to assign the sensitivity of the data and the ERP data owner may require encryption to protect against unauthorized viewing.

- *(ERP008000: CAT III) The IAO will ensure user procedures exist for manually marking printed documents if the printed report does not contain the same.*

- *(ERP008100: CAT II) The ERP Administrator will ensure the application displays an appropriate warning message upon user logon.*

- *(ERP008200: CAT II) The IAO will ensure an application user or client authentication is adequate.*

- *(ERP0008300: CAT I) The IAO and ERP Administrator will ensure sensitive data* is *encrypted using FIPS 140-2 validated encryption; NIST Certified cryptography or NSA approved cryptography depending on the classification of the data residing within the application.*

- *(ERP008400: CAT I) The System Administrator and ERP Administrator will ensure if a classified enclave contains Source and Materials Information (SAMI) and is accessed by unauthorized users, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.*

Sensitive application data will be adequately protected at rest in order to prevent compromised data.

- *(ERP008500: CAT I) The ERP Administrator will ensure no user or process has authorization to write to any file containing keys. If keys need to be replaced or added, permissions are changed temporarily for those events.*

3.10.2 In transit – Network connections to the application

When an ERP application connection is requested via the network, the client should provide an individual account name and authentication credentials to access the application. The ERP application account name and any password transmission from a client to a database server over a network must be encrypted. Encrypting information reduces the risk of unauthorized access to the data while being transmitted.

- *(ERP008600: CAT I) The System Administrator and ERP Administrator will ensure the transmission of an ERP account name and password from a client to an ERP Application server over a network is encrypted using NIST-certified cryptography.*

- *(ERP008700: CAT I) The System Administrator and ERP Administrator will ensure all network connections to an ERP application require an individual ERP application account and authentication credentials.*

- *(ERP008900: CAT II) The System Administrator and ERP Administrator will ensure file encryption, VPN, SSH and other entities to be encrypted are FIPS 140-2 compliant.*

3.11 Application Access to System Services

Accounts created for and used by non-interactive automated processing are subject to special consideration. These accounts may be used for a variety of functions such as maintenance batch jobs, etc. These accounts will not be shared with interactive application users. The primary vulnerability with non-interactive accounts is a frequent requirement to store the account name and password within application code, external files, or even on a remote server (example- 3rd party business warehouse application) and the possibility of exposure of this information during the logon process. Assignment of the minimal level of authorization access is critical for this reason. Accounts used for automated processing should be restricted to appropriate hours of access where possible.

- *(ERP009000: CAT II) The IAO and ERP Administrator will ensure non-interactive automated processing accounts meet the same security requirements as application dialog userids with the exception of password lifetime.*

- *(ERP009100: CAT III) The ERP Administrator will ensure the use of non-interactive automated processing accounts is documented and authorized by the IAO.*

- *(ERP009200: CAT I) The ERP Administrator will ensure application utilities and batch submissions do not contain or store unencrypted database account names and passwords.*

- *(ERP009300: CAT II) The IAO and ERP Administrator will ensure the application process removes temporary objects from memory or disk before the application terminates.*

3.12 Application Access to Database Services

A wide range of application languages and interfaces are supported for application and database services. For security reasons, it is important to only use one instance of a database for each ERP application. Multiple instances of a database can cause unauthorized users ability to compromised data elements or data tables. This also can lead to complex audit review of an application.

- *(ERP0010000: CAT III) The IAO and ERP Administrator will ensure the application does not modify data files outside the scope of the application.*

3.12.1 Separation of user interface from data storage

User data will be stored in a different directory than the application code to prevent any compromise of information. User credentials will be deleted from a client computer immediately upon session termination in order to prevent an unauthorized individual from gaining access to the ERP application on a recently used client computer.

- *(ERP010100: CAT II) The ERP Administrator will ensure the application code and application data is not located in the same directory.*

- *(ERP010200: CAT II) The ERP Administrator will ensure the application does not store authentication credentials on client computers after a session terminates.*

3.13 Application Configuration and Customization Requirements

Delivered application and security should be customized to comply with governing policies and standards. Management, data owners, IAO, ERP Administrator, SA and other stakeholders will all work together to customize the system to match said governing policies and standards.

- *(ERP011000: CAT II) The ERP Administrator and developers will ensure the application does not include an explicit error and exception handling capability.*

- *(ERP011100: CAT III) The ERP Administrator and SA will ensure the application interfaces are identified and protected.*

- *(ERP011200: CAT II) The developers will ensure the application code does not contain invalid references to network resources (pathnames, URLs, etc.).*

All files, ERP application accounts, application objects and application code that are solely associated with an unused module or area of the ERP application will be removed from the ERP application. In ERPs, the application access usually includes a shell interface to the OS and an "ad hoc query" interface that can sometimes punch through to the file system.

- *(ERP011300: CAT II) The ERP application administrator will ensure that any shell access privileges the users can get through the application client are removed.*

- *(ERP011400: CAT II) The ERP application administrator will ensure the removal of ad hoc query privileges from users through the application client.*

- *(ERP011500: CAT II) The IAO will not grant access to transactions or authorization objects not being used for a defined purpose.*

3.14 Patching and Maintenance Requirements

ERP patches are identified and sent out by the vendor. At that point in time the ERP Administrator should plan a system outage in order to apply the patch to the ERP application.

Maintenance includes upgrades, and test system refreshes with production data. Upgrades should be performed in a timely manner in order to maintain support from the vendor. This task should be performed as a project plan and executed by IAO, ERP Administrators, Developers and any necessary Application Users. Testing should take place by all groups in order to assure integrity of the system after the upgrade. Sign off should occur by the governing body indicating that they agree that the integrity of the system is intact and ready to be moved to production.

The QA system refreshes should be scheduled on a quarterly basis. Code must be moved from Development, to QA before it can be utilized in the production environment. Code review and tracking should be utilized in all working environments. The proper STIGs (Operating system, Network, application, etc.) will be used as part of a security review prior to the code going to the production environment. The SA will schedule downtime for the refresh and works together with the IAO and users to accomplish this task. Even though this only affects the test system, testing should be performed after the refresh in order to assure system integrity is intact.

- *(ERP012000: CAT III) The ERP Administrator will ensure the ERP application code changes are tracked and documented.*

- *(ERP012100: CAT II) The IAO will ensure the ERP application document all security changes to ensure the SSAA is updated to reflect the changes.*

3.15 Audit

Audit reviews are to ensure no one is attempting to gain unauthorized access by guessing passwords and that any unauthorized transaction attempts are mistakes and not malicious. Auditing will be configured and implemented on all systems. Auditing is capable of capturing all ERP Application operations, including application events, modification to database parameters and resources as well as modification to the data. Auditing can result in a great deal of information being collected on ERP Application activities. There should be a determination made of critical events/data to audit to allow enough granularity to allow for the monitoring of intrusive activity.

Logging and monitoring should exist for tables, which are deemed critical, and for powerful transactions and authorization objects. Controls should be in place to ensure audit log data is not deliberately or accidentally disabled. If this is not done, there is a risk that logging would not be done and an attack could remain undetected.

Documentation is key to consistent security measures being applied across an environment or an enterprise. Roles, responsibilities and security access authorizations will be clearly documented. Each user group should be aware of their specific roles and their responsibilities to protect data. Audit will be enabled for all user accounts to ensure data integrity.

- *(ERP013000: CAT II) The ERP Administrator and IAO will ensure all updates to security software or security functionality of software and applications are logged.*

- *(ERP013100: CAT II) The ERP Administrator will ensure the IAO is notified when the application logs are near capacity.*

- *(ERP013200: CAT II) The ERP Administrator and IAO will ensure the activities of administrators are monitored for evidence of misuse of privileges.*

Controls will be in place to ensure audit log data is protected from corruption or deletion. This control is necessary to ensure audit log data is protected. Without protection, the data could be changed or deleted intentionally or unintentionally, rendering the data inaccurate or unavailable for investigative purposes.

- *(ERP0133250: CAT I) The ERP Administrator will ensure logs maintained for audit purposes are stored securely.*

- *(ERP013300: CAT II) The IAO will ensure the use of system audit tools is restricted to authorized users.*

- *(ERP013350: CAT I) The IAO will ensure ERP Application audit data is captured and maintained for one year.*

Controls should be in place to obtain a list of the "administrative user" userids and then ensure the appropriate logging of these userids is taking place. Monitoring for evidence of misuse helps to protect the integrity and availability of the system.

- *(ERP013400: CAT II) The IAO will review authorization to maintain security audit logs once a week to ensure no one other than the IAO has access to modify security.*

- *(ERP013450: CAT I) The IAO will ensure changes to identifiers and role privileges or attributes are logged.*

The security audit log will be reviewed on a regular basis. Failure to monitor the system to detect unauthorized activities and reconciliation of abnormalities could result in unauthorized disclosure, modification or destruction of sensitive data.

- *(ERP013500: CAT II) The IAO will ensure security violations are reviewed and reconciled based on the access requirements and security needs of each individual.*

- *(ERP013550: CAT II) The IAO and ERP administrator will review the ERP application logs periodically to ensure compliance with security controls*

The IAO will conduct security audit reviews on all production systems and document the results. The IAO should become familiar with Sarbanes-Oxley Act (SOX) and Health Insurance

Portability and Accountability Act (HIPAA) audit requirements in order to monitor and review activity to ensure users are set up appropriately to satisfy these requirements.

- *(ERP013600: CAT II)The IAO will review changes to access in production systems once a month to ensure no roles change in a production system.*

- *(ERP013650: CAT II) The IAO will review access to view system logs once a month to ensure no one other than the users with batch submit access can display the system log.*

- *ERP013700: CAT II)The IAO will review authorization to process batch input sessions once a monthly to ensure only authorized userids have access to delete, release and lock sessions.*

- *(ERP013750: CAT II) The IAO will review batch and generic userids once a month in order to ensure all such userids are valid and that no new userids are created without approval. All anomalies are reviewed and appropriate action taken to secure the system.*

- *(ERP013800: CAT II) The IAO will review access to the background administrator function once a month to ensure only appropriate userids have this ability.*

- *(ERP013850: CAT II) The IAO will review access to system administration functions (ERP Administrator) once a month in order to ensure only appropriate userids and file permissions.*

- *(ERP013900: CAT II) The IAO will review data dictionary functions once a month to ensure only appropriate userids have this function.*

- *(ERP013910: CAT II) The IAO will review administrator access to the transport and change system once a month in order to ensure all such userids are valid.*

- *(ERP013920: CAT II) The IAO will review developer access once a month in order to ensure only authorized userids have this access.*

- *(ERP013950: CAT II) The ERP Administrator will review system parameters once a month to ensure applicable system parameters comply with standards and that changes to system parameters are documented and appear appropriate. This includes auditing of creating, alteration or deletion of application objects, granting and revoking of roles/privileges, connection failures, changes to classified data, unusual patterns of activity, configuration changes, and critical table changes.*

- *(ERP013960: CAT II) IAO will review a list of conflicting access once a month in order to ensure all such userids have a valid approval by the appropriate approver(s) and segregation of duties is intact for SOX audit information.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

Chairman Of The Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) And Computer Network Defense (CND)," March 25, 2003

DoD Memorandum, "Policy Guidance for the Use of Mobile Code Technologies in DoD Information Systems," November 7, 2000

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements For Cryptographic Modules" May 25, 2001 as modified December 3, 2002. This publication may be found on the NIST website http://www.nist.gov/.

Carter, Jason D. (2004). *The Expert Guide to PeopleSoft Security*. Lincoln, NE: iUniverse, Inc.

Security, Audit and Control Features- SAP R3- A Technical and Risk Management Reference Guide, 2002, IT Governance Institute

This page is intentionally left blank.

APPENDIX B. LIST OF ACRONYMS

ACRONYM	PLAIN TEXT
AIS	Automated Information Systems
CCB	Configuration Control Board
COTS	Commercial Off the Shelf
CRM	Customer Relations Management
DAA	Designated Approving Authority
DBA	Database Administrator
DoD	Department of Defense
ERP	Enterprise Resource Planning
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resource
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
IT	Information Technology
JTF-GNO	Joint Task Force-Global Network Operations
MAC	Mandatory Access Control
NIST	National Institute for Standards and Technology
NSO	Network Security Officer
PKI	Public Key Infrastructure
QA	Quality Assurance
SOX	Sarbanes-Oxley Act
SA	System Administrator
SAMI	Source and Materials Information
SDID	Short Description Identifier
SSH	Secure Shell
STIG	Security Technical Implementation Guide
VPN	Virtual Private Network

This page is intentionally left blank.