APPLICATION SECURITY and DEVELOPMENT CHECKLIST

Version 2, Release 1.5

26 June 2009

Developed by DISA for the DoD

TABLE OF CONTENTS

TABLE OF CONTENTS i
1. INTRODUCTION 1
1.1 The Scope of a Review 1
1.2 Pre-Review Activities 3
1.3 SRR Equipment 5
1.4 Recording Results 9
1.5 Severity Codes 9
1.6 Organization of the Checklist 10
2. SRR REPORT 12
2.1 Reviewer Information 13
2.2 Site / Organization Information 13
2.3 Application Information 14
2.4 Source Code Information 14
2.5 Server Overview 15
3. CHECKLIST INSTRUCTIONS – Generic Checks 16
APP2010 System Security Plan non existent or not adequate 19
APP2020 Application Configuration Guide does not exist 20
APP2030 No established IA budget 22
APP2040 Classification guide does not exist 23
APP2050 No MAC and CONF levels documented 25
APP2060 No coding standards exist 26
APP2070 Products are not NIAP/Common Criteria approved 27
APP2080 Products with no or unsuitable robustness profiles 29
APP2090 Public domain software in use 31
APP2100 Application violates Ports and Protocols Guidance 32
APP2110 Not registered with the DoD Ports and Protocols 33
APP2120 Security training not provided 34
APP2130 Maintenance does not exist or not sufficient 35
APP2140 An incident response process is not established 36
APP2150 Inadequate Workplace Security Procedures 37
APP2160 Approved Security Configuration Guidance not used 39
APP3010 Design document is not complete or does not exist 40
APP3020 Threat model not established or updated 41
APP3050 Inactive code and libraries not removed 43
APP3060 Application code and data are co-located 45

APP3070 Application components not separated from data storage 46
APP3080 Invalid URL or path references found 47
APP3090 Session hijacking prevention not supported 48
APP3100 Temporary objects not removed from system 49
APP3110 Unneeded functionality enabled 51
APP3120 Application has error handling vulnerabilities 52
APP3130 Secure design principle not followed 53
APP3140 Application failure results in an insecure state 54
APP3150 Application uses unapproved cryptographic modules 55
APP3170 Encryption for Key Exchange not used 56
APP3180 Encryption key permissions are not adequate 57
APP3190 Database connections use administrative accounts 58
APP3200 No support for roll-back and journaling 59
APP3210 Sensitive data not protected at rest 60
APP3220 Sensitive data is not encrypted in memory 61
APP3230 Application does not clear all memory blocks 62
APP3240 Actions not authorized before execution 63
APP3250 Sensitive data not protected in transit 64
APP3260 Integrity mechanisms on data files not supported 65
APP3270 Classification labels not appropriately displayed 66
APP3280 The application is not PK-enabled 68
APP3290 The application utilizes a PKI other than DOD PKI 70
APP3300 Server authentication is not PK-enabled 71
APP3305 Expired revoked untrusted certificates honored 72
APP3310 Clear text passwords displayed 74
APP3320 Userids have weak passwords 75
APP3330 Passwords not transmitted encrypted 77
APP3340 Passwords stored in an unapproved encrypted format 78
APP3350 Embedded authentication data stored in code 79
APP3360 Authentication data permissions not adequate 80
APP3370 Unneeded accounts active 81
APP3380 Application userids are not unique 82
APP3390 User accounts not locked after invalid logons 83
APP3400 User accounts unlocked by person other than admin 84
APP3410 Session limits do not exist for the application 85
APP3415 Sessions do not automatically terminate 86
APP3420 Explicit logout not available 87
APP3430 Authentication credentials not removed 88

APP3440 Logon warning not displayed 90
APP3450 Application resources has inappropriate permission 92
APP3460 Resource name used to control access 93
APP3470 Application functionality not role based 94
APP3480 Access control mechanism not in place 96
APP3500 Application runs with excessive privileges 97
APP3510 Insufficient input validation 99
APP3520 No Trust boundary data validation 101
APP3530 Application does not set character set 102
APP3540 Application is vulnerable to SQL Injection 103
APP3550 Application is vulnerable to integer overflows 105
APP3560 Application contains format string vulnerabilities 106
APP3570 Application vulnerable to Command Injection 107
APP3580 Application vulnerable to Cross Site Scripting 108
APP3590 Application is vulnerable to buffer overflows 109
APP3600 Vulnerable to canonical representation attacks 110
APP3610 Hidden fields used to control access privileges 111
APP3620 Application discloses unnecessary information 112
APP3630 Application vulnerable to race conditions 113
APP3640 No logs for data access and changes 114
APP3650 No warning when logs are near full 115
APP3660 Last Login information not displayed 116
APP3670 No notification of time of last change of data 117
APP3680 The application does not adequately log events 118
APP3690 Application audit logs have incorrect permissions 120
APP3700 Unsigned Cat 1A or 2 mobile code in use 121
APP3710 Mobile code executed without verifying signature 122
APP3720 Unsigned unconstrained mobile code used 123
APP3730 Uncategorized mobile code used 124
APP3740 Code sent in email 126
APP3750 New mobile development not compliant DoDI 5200.40 127
APP4010 Access rights to the CM repository not reviewed 128
APP4020 Flaws found during a code review are not tracked 129
APP4030 The SCM plan does not exist 130
APP4040 A Configuration Control Board does not exist 133
APP5010 No tester designated to test for security flaws 134
APP5030 Data files modified outside the application 135
APP5040 Changes to the application are not assessed for IA 136

APP5050 Tests plans not executed prior to release or patch 137
APP5060 System in insecure state during startup & shutdown 138
APP5070 Application has no code coverage statistics..... 139
APP5080 Code reviews not performed prior to release 140
APP5090 Flaws found during a code review are not tracked 141
APP5100 Fuzz testing is not performed..... 142
APP5110 Security flaws not addressed in project plan..... 143
APP6010 Critical application hosted on a multi-use server..... 144
APP6020 COTS products not configured to best practices 145
APP6030 Unnecessary services or software not removed 146
APP6040 Administrator has not registered to updates..... 147
APP6050 Current patches and configurations not installed..... 148
APP6060 App not decommissioned when maintenance is expired 149
APP6070 No procedures exist to decommission application..... 150
APP6080 Protections against DoS attacks not implemented 151
APP6090 No system alerts in a low resource condition 152
APP6100 Sensitive data not purged from production export..... 153
APP6110 Audit trail not periodically reviewed 154
APP6120 IAO has no process to report IA violations 155
APP6130 No automated audit trail monitoring..... 156
APP6140 Log files are not retained for at least one year..... 157
APP6160 Disaster recovery plan does not exist..... 158
APP6170 Application backups not in a fire rated container 159
APP6180 Backup and restoration device not protected 160
APP6190 Backups or backup procedures are incomplete..... 161
APP6200 Disaster plan does not exist or is incomplete..... 163
APP6210 No account management process in place 164
APP6220 Generated passwords do not comply with policy 165
APP6230 Access granted by group authenticator 166
APP6240 Inactive userids are not disabled 167
APP6250 Unnecessary built-in userids are not disabled..... 168
APP6260 Userids have default passwords 169
APP6270 DMZ not present between DoD and public networks 170
APPENDIX A: CHANGE LOG.....171
APPENDIX B: LIST OF ACRONYMS.....174
APPENDIX C: VMS 6.0 Instructions 177
C.1 : System Administrator..... 177
C.2: Reviewer..... 177

APPENDIX D: Additional Resource Information.....179
APPENDIX E: Cross Reference to Application Security and Development STIG 180

1. INTRODUCTION

This document contains procedures that enable qualified personnel to conduct an Application Security Readiness Review (SRR). The Application SRR assesses compliance, in part, with DISA's Application Security and Development Security Technical Implementation Guide (STIG) Version 2,R1.

DISA Field Security Operations (FSO) conducts Application SRRs to provide a minimum level of assurance to DISA, Joint Commands, and other Department of Defense (DoD) organizations that their applications are reasonably secure against attacks that would threaten their mission. The complexity of most mission critical applications precludes a comprehensive security review of all possible security functions and vulnerabilities in the time frame allotted for an Application SRR. Nonetheless, the SRR helps organizations address the most common application vulnerabilities and identify information assurance (IA) issues that pose an unacceptable risk to operations.

Ideally, IA controls are integrated throughout all phases of the development life cycle. Integrating the Application Review process into the development lifecycle will help to ensure the security, quality, and resilience of an application. Since the Application SRR is usually performed close to or after the applications release, many of the Application SRR findings must be fixed through patches or modifications to the application infrastructure. Some vulnerabilities may require significant application changes to correct. The earlier the Application Review process is integrated into the development lifecycle, the less disruptive the remediation process will be.

1.1 The Scope of a Review

An Application SRR encompasses all of the server-side components of an application including but not necessarily limited to, the following items supporting the application:

- Application code
- Web server(s)
- Database server(s)
- Directory and authentication device(s) (e.g., Windows domain controllers, RADIUS, etc.)
- Firewall(s)
- Network and enclave configuration required to support the application
- Operating system platforms for any of the above

During a full application review, a SRR is performed on each of the components listed above in addition to the Application itself. For example, if the application infrastructure consisted of a front-end web server running on Windows and a backend database running on UNIX, then the full review would consist of Web Server, Database, Windows, and UNIX SRRs in addition to the Application SRR. A vulnerability scan will also be performed as part of the review.

If this review is a full system baseline all components will be evaluated. If this review is an ST&E validation or a re-accreditation and current reviews exist for these components, only the

vulnerability scan needs to be completed at the time of the application review. A current review is defined as a review performed based upon the current STIG. A review is also deemed to not be current if the operating system or component has been reinstalled since the last SRR.

The Application Checklist is designed to be used with both Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) products. In some cases not all checks can be performed because access to the source code is required. As some of the checks become automated through the use of tools, more of the checks will be able to be used for GOTS products.

Some application elements are outside the scope of the Application SRR. These application elements include:

- Configuration and behavior of web browser clients
- Application development methodology

As security is only as strong as its weakest link, a complete security review should involve both the client and server components of the application, but in the case of web browsers, the reviewer does not have access to all the potential clients who may access the application. Therefore, it is not feasible to include these web browsers in the review. Fortunately, organizations that comply with the browser requirements listed in the Desktop Application STIG should be protected against known browser-based application attacks. Application developers should independently ensure their applications function properly with STIG-compliant browsers (which is not validated during the Application SRR).

The Application Checklist is not an appropriate evaluation for systems that perform multi-level classified processing. Only NSA approved devices in the approved configuration are appropriate in these environments. These types of checks are outside the scope of this review.

1.2 Pre-Review Activities

This document specifies duties to be completed by a team lead and a reviewer. In some cases, this may be the same person.

To make best use of time on-site, the team lead should perform the following activities prior to arrival. The following activities are listed in a suggested sequence order:

- Work with site to identify personnel to assist the reviewer with the Application SRR. One or more individuals need to be available to answer the reviewer's questions, provide access to source code, and provide access to privileged user interfaces as required.

- Work with site to coordinate the use of a client machine to be used for testing.

- Obtain signed SRR coordination memo in which site management accepts the review's scope and the operational risk associated with performing the review.

- Determine the scope of review incorporating what systems, software, and features will or will not be included.

- Obtain copies of the following documentation

  - System ID Profile (SIP) for DIACAP
  - System Security Authorization Agreement (SSAA) for DITSCAP
  - System Security Plan (SSP) for DIACAP and DITSCAP
  - Security Classification Guide for classified systems
  - Documented MAC and Confidentiality Levels
  - Threat Model
  - Design Document
  - Application Configuration Guide
  - Vulnerability Assessment Tool Output if automated assessment tools are used
  - Code review process and evidence
  - Test Procedures and Results
  - Coding standards
  - Code coverage statistics
  - Vulnerability Management Process
  - Incident Response Process
  - Workplace Security Procedures
  - Account Management Process
  - Organizational Password Policy
  - Software Configuration Management (SCM) Plan
  - CCB charter documentation
  - Unnecessary Code Removal Process
  - COTS Products List
  - COTS Product Vendor Security Recommendations if STIG not available

- Evidence of Security Training
- Disaster Recovery Plans & Procedures
- Backup and Recovery Procedures
- Maintenance Agreements
- Process for Log file Retention
- Project Plan with Security Flaws Identified
- Project Schedule with IA Resources and Budget

The reviewer should perform the following activities prior to arrival. These activities are listed in suggested sequence order:

- Obtain necessary approvals for physical and logical access to in-scope components. Submit appropriate DD Form 2875s for access to the site.

- Acquire a general knowledge of the application, including what it does and the user community it serves by reviewing the SSAA or SIP depending of the type of certification and accreditation process is used. Also review the SSP, Security Classification Guide, and the documented MAC and confidentiality levels.

- Determine which checks will be performed in lab environments versus production systems and the hours each system is available for observation and SRR testing.

- Submit change requests (if the site requires approvals for temporary changes during testing).

- Assist the Team Lead in determining the scope of the review and in identifying the necessary source files needed to perform the review.

Review copies of the following documentation

- Threat Model
- Design Document
- Application Configuration Guide
- Vulnerability Assessment Tool Output if automated assessment tools are used
- Code review process and evidence
- Test Procedures and Results
- Coding standards
- Code coverage statistics
- Vulnerability Management Process
- Incident Response Process
- Workplace Security Procedures
- Account Management Process
- Organizational Password Policy
- Software Configuration Management (SCM) Plan
- CCB charter documentation
- Unnecessary Code Removal Process
- COTS Products List

- COTS Product Vendor Security Recommendations if STIG not available
- Evidence of Security Training
- Disaster Recovery Plans & Procedures
- Backup and Recovery Procedures
- Maintenance Agreements
- Process for Log file Retention

The term "application representative" is used hereafter to denote personnel to assist the reviewer with the Application SRR. The application representative may be a program manager, application developer, systems administrator, or other individual with sufficient knowledge and access to the application to permit the reviewer to complete the review. In some cases, the application representative role may be split among two or more individuals.

1.3 SRR Equipment

To complete an SRR, the reviewer will require a site provided client machine to test client portion of the application. Browser checks are written for Windows clients. If the application uses a UNIX client, the team lead will work with the site to determine the client requirements.

If the application is web based, the machine must be configured with STIG-compliant configurations of the Microsoft Internet Explorer (IE) web browser. The following configuration tables will be used to configure the IE web browser.

The following configuration changes should be made via selecting Tools then Internet Options from the IE menu:

IE INTERNET OPTIONS		
CATEGORY	**PARAMETER**	**REQUIRED SETTING**
General	*Home page – Address*	*about:blank* *[or]* *[A trusted site or the name of a local file]* *[Preferred]*

Security	*Security level for this zone [applies to all zones]*	*Custom level [See Security Zone Settings in the following section.]*
	Local intranet – Sites *- Include all local (intranet) sites not listed in other zones* *- Include all sites that bypass the proxy server* *- Include all network paths (UNCs)*	 *Disable* *Disable* *Disable*
Privacy [IE 6.0 only]	*Settings*	*Medium High* *[or]* *High* *[or]* *Block All Cookies*
Advanced	*Automatically check for Internet Explorer updates*	*Disable*
	Enable Install On Demand (Internet Explorer - [IE 6.0 only])	*Disable*
	Enable Install On Demand (Other) [IE 6.0 only]	*Disable*
	When searching	*Do not search from the Address bar* *[or]* *Just display the results in the main window* *[or]* *[No option selected]*
	Check for signatures on downloaded programs [IE 6.0 only]	*Enable*
	Do not save encrypted pages to disk	*Enable [Preferred] [see note following table]*
	Use Private Communication Technology (PCT) 1.0 [IE 5.5 only]	*Disable*
	Use SSL 2.0	*Enable [Preferred]*
	Use SSL 3.0	*Enable*
	Use TLS 1.0	*Enable*
	Warn about invalid site certificates	*Enable*
	Warn if changing between secure and not secure mode	*Enable*

	Warn if forms submittal is being redirected	*Enable*

The following configuration changes should be made via selecting Tools then Internet Options from the IE menu. Select the Security Tab. Select each of the zones (one at a time), and then select custom level. Ensure the parameters for each level match those listed in the following table:

SECURITY ZONE SETTINGS				
PARAMETER	**INTERNET ZONE**	**LOCAL INTRANET ZONE**	**TRUSTED SITES ZONE**	**RESTRICTED SITES ZONE**
Download signed ActiveX controls	*Disable*	*Prompt*		*Disable*
Download unsigned ActiveX controls	*Disable*	*Disable*		*Disable*
Initialize and script ActiveX controls not marked as safe	*Disable*	*Disable*		*Disable*
Run ActiveX controls and plug-ins	*Prompt*	*Prompt*		*Disable*
Script ActiveX controls marked safe for scripting	*Prompt*	*Prompt*		*Disable*
Allow cookies that are stored on your computer [IE 5.5 only]	*Prompt*	*Enable*		*Disable*
Allow per-session cookies (not stored) [IE 5.5 only]	*Prompt*	*Enable*		*Disable*
File download	*Enable*	*Enable*		*Disable*
Font download	*Prompt*	*Enable*		*Disable*
Java permissions [See notes on the Java VM in the following text.]	*Disable Java [Preferred] [or] Custom*	*Custom*		*Disable Java*
Access data sources across domains	*Disable*	*Prompt*		*Disable*
Allow META REFRESH [IE 6.0 only]	*Enable*	*Enable*		*Disable*
Display mixed content [IE 6.0 only]	*Prompt*	*Enable*		*Disable*

SECURITY ZONE SETTINGS				
PARAMETER	**INTERNET ZONE**	**LOCAL INTRANET ZONE**	**TRUSTED SITES ZONE**	**RESTRICTED SITES ZONE**
Don't prompt for client certificate selection when no certificate or only one certificate exists	*Disable*	*Disable*		*Disable*
Drag and drop or copy and paste files	*Prompt*	*Prompt*		*Disable*
Installation of desktop items	*Disable*	*Prompt*		*Disable*
Launching programs and files in an IFRAME	*Disable*	*Prompt*		*Disable*
Navigate sub-frames across different domains	*Prompt*	*Enable*		*Disable*
Software channel permissions	*High safety*	*High safety*		*High safety*
Submit non-encrypted form data	*Prompt*	*Enable*		*Disable*
Userdata persistence	*Disable*	*Enable*		*Disable*
Active scripting	*Enable*	*Enable*		*Disable*
Allow paste operations via script	*Disable*	*Prompt*		*Disable*
Scripting of Java applets	*Prompt*	*Enable*		*Disable*
User Authentication – Logon	*Prompt for user name and password*	*Prompt for user name and password*		*Anonymous logon*

Each browser must have four user profiles, each associated with one of the following:

- A valid DoD PKI Class 3 client certificate
- An expired DoD PKI Class 3 client certificate
- A revoked DoD PKI Class 3 client certificate
- A client certificate issued by a non-DoD certificate authority

SRR procedures use these various certificates to check whether the application recognizes improper authentication credentials.

Not all applications utilize browsers or certificates. In these cases, the reviewer must work with the application representative to determine the appropriate course of action for client configuration, which might involve the installation of additional client software on the client.

1.4 Recording Results

Once information is gathered and evaluated, the reviewer can record findings of vulnerabilities in the SRR Results Report included later in this document.

Results are also entered into the Vulnerability Management System (VMS). Create the asset as a unique entity in the Non-Computing branch and then add the proper target (Application – Pre-Production, Application - Production, Application – Additional Vulnerabilities) to the Asset Posture.

1.5 Severity Codes

Each vulnerability has an associated severity code. The severity codes range between I and III and are defined as follows:

- Category I Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges.

- Category II Assigned to findings that have a potential to lead to unauthorized system access or activity.

- Category III Assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.

1.6 Organization of the Checklist

The remainder of the document is divided into the following sections:

- Section 2 (SRR Report) provides a form on which reviewer will document the overall components of the applications.
- Section 3 (Checklist Procedures) provides a form and verification procedures for each of the vulnerabilities.
- Appendix A (Document Change Log) lists the changes made to this document.
- Appendix B (List of Acronyms) lists the acronyms used in this document.
- Appendix C VMS 6.0 Instructions
- Appendix D Additional Resource Information
- Appendix E Cross Reference to Application Security and Development STIG

This page is intentionally left blank

2. SRR REPORT

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

2.1 Reviewer Information

Reviewer Name	
Reviewer Phone number	Commercial: DSN:
Reviewer e-mail	
Reviewer SIPRNet e-mail	
Application Checklist version	
Date of review	
Date of report	

2.2 Site / Organization Information

Organization Name	
Primary Address Street Address City, State ZIP	
Application Representative Name	
Application Representative Phone number	Commercial: DSN:
Application Representative e-mail	
Application Representative SIPRNet e-mail	

2.3 Application Information

Application Name	
MAC Level	☐ I ☐ II ☐ III
Classification	☐ Unclassified ☐ Confidential ☐ Secret ☐ Top Secret
Environment	☐ Pre-Production ☐ Production

If the review is performed in a pre-production environment the Program Manager will have knowledge of the MAC and Classification Level. If the review is performed at a site or production environment, the IAO or information owner should provide the information.

Also interview the data owner to determine if sensitive data is being processed by the application.

2.4 Source Code Information

Application Language Used (C, C++, Java, PHP, ASP, etc.)	
Target Compiler (Visual C++, gcc, cc, etc.)	
Build Environment (Visual Studio, Eclipse, etc.)	

2.5 Server Overview

List all of the application servers, regardless of whether they are reviewed or not. If an OS SRR has been or will be performed on that server, place a "Y" in the "Reviewed?" column to the right of the "Operating System and Version" column. Otherwise, enter an "N." For each server, note what application software and version is installed (web, database, LDAP, etc.) and whether or not SRRs have been, or will be performed on those components.

Host Name	IP Address Subnet Mask	Operating System and Version	Reviewed?	Application Service Software and Version	Reviewed?	Physical Location

If previous reviews exist, list Trip Names: _____

_____

Vulnerability Scan Information

	Network Address	ISS Job ID	Function	Type of Scan
1				
2				
3				
4				
5				

3. CHECKLIST INSTRUCTIONS – Generic Checks

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The following checks in this section are the generic checks that may apply to pre-production and production environments.

To complete some of the following checks some investigation of source code, scripts, or web content depending on the application technology may be necessary. For applicable checks, source code, scripts, and web content may be required in order to satisfactorily determine the severity and complete the status instructions. If source code is needed for check completion and is unobserved during the review, appropriately note that the check is not complete because the necessary source code, scripts, or web content for check determination was not provided or observed.

For each vulnerability, check whether it is a finding or not a finding in the Status column. In cases in which the vulnerability is not applicable, check "Not Applicable" (e.g., guidance for marking N/A is included in the instructions). If a vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check "Not Reviewed". Reasons for not reviewing items should be included in the module text of the review.

Each check identifies the severity of the finding. If the severity of the finding is variable, the checklist gives instruction on determining the appropriate severity. The default severity in VMS is the highest possible severity code for the finding.

Each check is marked as pre-production and/or production. A pre-production environment includes development, acceptance, test, pilot systems, or other systems prior to production. Production environments are the application's final location where the resources and configuration have been thoroughly documented, stable, and formal reviews are performed before changes or upgrades are implemented.

For the first review of an application, if no pre-production environment exists, the pre-production environment checks must be performed in the production environment. If any check is not reviewed, the reasons the review was not performed should be included in the module text of the review.

Checks marked as Production are to be performed in a production environment because the resources and configurations may be significantly different than those in a pre-production environment. If a production environment does not exist and the application will be released for production before a final review, these checks can be performed in a pre-production environment. This should be noted in the module text.

Sections identified in the reference column refer to sections in the Application Security and Development STIG Version 2 Release 1, unless another document is referenced. References designated by a 4-digit code with a dash then a numeric are DoDI 8500.2 IA control references. If these IA controls are present, a Mac and Confidentiality level associated with the controls is also present. For example, IAIA-1 is listed as the control number, then 1-CS, 2-CS, and 3-CS is also listed. This means this control applies to Mac 1 systems that contain classified and sensitive

data, Mac 2 systems that contain classified and sensitive data, and Mac 3 systems that contain classified and sensitive data.

In addition to the checks listed in the following sections, there are ten additional vulnerabilities in VMS. These vulnerabilities are numbered APP7100-APP7190. They are to be used for additional checks identified in the application's test plan that are not covered by this checklist. If these additional vulnerabilities are needed, they can be added in VMS by the adding the "Application – Additional Vulnerabilities" to the asset posture. If used, the reviewer will need to update the severity code of the finding based upon the definition listed in Section 1.6.

Environment	Pre-Production & Production	**APP2010 System Security Plan non existent or not adequate**	**STIG Section**	2.1.1 System Security Plan 2.1.3 Information Assurance Budget
Finding Category	CAT II			
Vulnerability Key	V0006197		**IA Controls**	DCSD-1

Check

Instruction:
Interview the application representative and validate that the required IA roles are established in writing. These roles are DAA and IAM/IAO. This must include assigned duties and appointment criteria such as training, security clearance, and IT-designation.

If a traditional review is conducted at the same time as the application review, this check is not applicable.

Also validate a System Security Plan (SSP) exists and describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

Note: The SSP is "Appendix S" in legacy System Security Authorization Agreements.

1) if the SSP does not exist or is incomplete this is a finding.

2) if the IA Roles and assigned duties and appointment criteria are not made in writing this is a finding.

Ask site personnel which IAO or IAM for the systems/application is part of the application review.

3) If the IAO or IAM is unknown or not assigned this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2020 Application Configuration Guide does not exist**	**STIG Section**	2.1.2 Application Configuration Guide 2.1.4 Security Classification Guide 2.1.5 Mission Assurance Category and Confidentiality 2.2.1 NIAP Approved Products
Finding Category	CAT II			
Vulnerability Key	V0016773		**IA Controls**	DCSD-1 DCPB-1 DCSD-1

Check

Instruction:
The Application Configuration Guide is any document or collection of documents used to configure the application. These documents may be part of a User Guide, secure configuration guide, or any guidance that satisfies the requirements below:

The Application Configuration Guide must be made available to application hosting providers.

The Application Configuration Guide will contain a list of all potential hosting enclaves and connection rules and requirements.

Development systems, build systems, and test systems must operate in a standardized environment. These setting are to be documented in the Application Configuration Guide. Examples include:
- Versions of Compilers used
- Build options when creating application/components
- Versions of COTS Software Used as part of the application
- For web applications, which browsers and what versions are supported

All Known security assumptions, implications, system level protections, best practices, and required permissions are documented in the Application Configuration Guide.

All Deployment configuration settings are documented in the Application Configuration Guide. Examples include:
- Encryptions Settings
- PKI Certificate Configuration Settings
- Password Settings

All Deployment configuration settings from the Application Configuration Guide should be

implemented. Ask the application representative for Application Configuration Guide or other guidance where these requirements are documented. Verify the configuration settings have been implemented. 1) If any of the above information is missing or the application configuration guide does not exist this is a finding. 2) If the settings in the application configuration guide are not implemented this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2030 No established IA budget**	**STIG Section**	2.1.3 Information Assurance Budget
Finding Category	CAT III			
Vulnerability Key	V0016774		**IA Controls**	DCPB-1

Check

Instruction:
Obtain a copy of the most recent project schedule and interview the PM or IAM to determine if IA tasks and roles are allocated.

1) If there is no established IA tasks and roles on the schedule this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2040 Classification guide does not exist**	**STIG Section**	2.1.4 Security Classification Guide 2.1.5 Mission Assurance Category and Confidentiality
Finding Category	CAT II			
Vulnerability Key	V0006145		**IA Controls**	DCSD-1

Check

Instruction:
If the application does not process classified information, this check is not applicable.

The application may already be covered by a higher level program or other classification guide. If classification guide is not written specifically to the application, the sensitive application data should be reviewed to determine whether it is contained in the classification guide.

DoD 5200.1-R, January 1997 indentifies requirements for security classification and/or declassification guides.
http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf

Security classification guides shall provide the following information:
• Identify specific items, elements, or categories of information to be protected
• State the specific classification to be assigned to each item or element of information and, when useful, specify items of information that are unclassified
• Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from automatic declassification
• State a concise reason for classification for each item, element, or category of information that, at a minimum, cites the applicable classification categories in Section 1.5 of E.O. 12958
• Identify any special handling caveats that apply to items, elements, or categories of information
• Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of approval
• Provide a point-of-contact for questions about the guide and suggestions for improvement.
• For information exempted from automatic declassification because its disclosure would reveal foreign government information or violate a statute, treaty, or international agreement the security classification guide will identify the government or specify the applicable statute, treaty, or international agreement, as appropriate.

1) If the security classification guide does not exist or is incomplete this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2050 No MAC and CONF levels documented**	**STIG Section**	2.1.5 Mission Assurance Category and Confidentiality
Finding Category	CAT II			
Vulnerability Key	V0016775		**IA Controls**	DCSD-1

Check

Instruction:
Interview the application representative to determine if the system documentation has identified the Mission Assurance Category (MAC) and Confidentiality Levels of the application.

1) If no system documentation exists that identifies the MAC and Confidentiality levels this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2060 No coding standards exist**	**STIG Section**	2.1.6 Coding Standards 2.2.1 NIAP Approved Products
Finding Category	CAT II			
Vulnerability Key	V0016776		**IA Controls**	DCSQ-1

Check

Instruction:
If the application is a COTS product or is composed of only COTS products with no custom code, this check does not apply.

Interview the application representative to determine if a documented set of coding standards exists. Ask the application representative to demonstrate coding standards are being followed by reviewing a sample of code. Also check the coding standards for a list of unsafe functions or section documenting there are no unsafe functions.

1) If no coding standards exist at an organizational or project level this is a finding.

2) If documented coding standards are not being followed this is a finding.

3) If there is no documented list of unsafe functions or the coding standards do not document there are no unsafe functions for that particular language this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2070 Products are not NIAP/Common Criteria approved**	**STIG Section**	2.2.1 NIAP Approved Products
Finding Category	CAT III			
Vulnerability Key	V0006170		**IA Controls**	DCAS-1

Check

Instruction:
List all IA or IA enabled products that are part of the application. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) / Common Criteria Evaluated Products.

1) If the products have not been evaluated or in the process of being evaluated, this is a finding.

According to NSTISSP 11, an IA-enabled product is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. To meet the intent of NSTISSP 11, acquired IA-enabled products must be evaluated if the IA features are going to be used to perform one of the security services (availability, integrity, confidentiality, authentication, or non-repudiation). Therefore, the determination of whether an IA-enabled product must be evaluated will be dependent upon how that particular product will be used within the consumer's system architecture. Examples include such products as security-enabled web browsers, screening routers, and security-enabled messaging systems. Although NSTISSP #11 uses both terms, the policy as stated applies equally to both types of products.

A list of certified products is available on the common criteria website.
http://www.commoncriteriaportal.org/products.html

Below are definitions of IA and IA-Enabled products from DoD Instruction 8500.2.

IA Product - Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors,
firewalls, and intrusion detection devices.

IA-Enabled Product - Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Finding Results					
Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2080 Products with no or unsuitable robustness profiles**	**STIG Section**	2.2.2 Robustness Protection Profiles
Finding Category	CAT II			
Vulnerability Key	V0016777		**IA Controls**	DCSR-1 DCPD-1 DCPP-1

Check

Instruction:
Interview the application representative and determine the IA and IA-enabled COTS products used in the application. Also, review the confidentiality level for the application.
Public releasable data requires Basic robustness profile for IA and IA-enabled COTS products
Sensitive data requires Medium robustness profile for IA and IA-enabled COTS products
Classified data requires High robustness profile for IA and IA-enabled COTS products

Basic robustness security services and mechanisms are usually represented by good commercial practice.

Basic robustness technical solutions require, at a minimum:
• Authenticated access control
• NIST-approved key management algorithms
• NIST FIPS validated cryptography
• The assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness

Medium robustness security services and mechanisms provide for additional safeguards above Basic.

Medium robustness technical solutions require, at a minimum:
• Strong (e.g., crypto-based) authenticated access control
• NSA-approved key management
• NIST FIPS-validated cryptography
• The assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for Medium Robustness. The SSAA should list the products that are used.

High robustness security services and mechanisms provide, through rigorous analysis, the most confidence in those security mechanisms.

High robustness technical solutions require NSA-certified high robustness solutions for cryptography:
• NSA-certified access control
• NSA-certified key management
• High assurance security design as specified in NSA-endorsed high robustness protection profiles, where available.

The SSAA should list the products that are used.
A list of validated products and protection profiles is available on the common criteria website.
http://www.niap-ccevs.org/cc-scheme/pp/index.cfm

1) Compare that list against the approved products. If any of the third party products are not listed or is below the minimum robustness profile required by the application, this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2090 Public domain software in use**	**STIG Section**	2.2.3 Categories of Third Party Products
Finding Category	CAT II			
Vulnerability Key	V0016778		**IA Controls**	DCPD-1

Check

Instruction:
Software products and libraries with limited or no warranty will not be used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. If these products are required, they must be assessed for information assurance impacts, and must be approved for use by the DAA.

Review the DoD policy regarding Open Source software products.
http://www.defenselink.mil/cio-nii/docs/OpenSourceInDoD.pdf

Open Source Software: Copyrighted software distributed under a license that provides everyone the right to use, modify, and redistribute the source code of software.

Public Domain Software: Software not protected by any copyright laws providing the right to use, modify, and redistribute without permission or payment to the author.

Shareware: Copyrighted software distributed under a license that provides a trial right to use and redistribute the binaries. For continued usage users are required to pay a fee.

Freeware: Copyrighted software distributed under a license that provides a right to use and redistribute the binaries. Unlike shareware, there is no charge for continued use.

Commercial Software: Copyrighted software sold for profit by businesses also referred to as Commercial off-the-shelf (COTS) software.

1) If software products (e.g., Open Source Software, Public Domain Software, Shareware and Freeware) and libraries with limited or no warranty are used in DoD information systems except when they are necessary for mission accomplishment and there are no alternative IT solutions available, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2100 Application violates Ports and Protocols Guidance**	**STIG Section**	2.3 Ports and Protocols 2.3 Ports and Protocols 2.4.1 Management
Finding Category	CAT II			
Vulnerability Key	V0006169		**IA Controls**	DCPP-1

Check

Instruction:
Check that access control lists limit traffic to application servers. Check that all externally accessible servers are in a demilitarized zone.

Check all necessary ports and protocols needed for application operation that are needed to be accessed outside the local enclave against the DoD Ports and Protocols guidance to ensure compliance.

Establish the ports needed for the application
• Look at System Security Plan/SSAA
• Ask System Administrator
• Go to Network Administrator Retina Scanner
• Go to Network Reviewer
• If a network scan is available use it
• Use netstat/task manager
• Check /etc/services

All ports, protocols, and services needed for application operation need to be verified against the DoD Ports and Protocols guidance (http://iase.disa.mil/ports/index.html) to ensure the ports, protocols, and services are in compliance with the PPS Assurance Category Assignments List (CAL).

1) If the application is not in compliance with DoD Ports and Protocols guidance this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2110 Not registered with the DoD Ports and Protocols**	**STIG Section**	2.3 Ports and Protocols 2.4.1 Management 2.5.2 Vulnerability Management Process
Finding Category	CAT II			
Vulnerability Key	V0016779		**IA Controls**	DCPP-1

Check

Instruction:
Verify registration of the application and the ports in the Ports and Protocols database for a production site. https://pnp.cert.smil.mil

1) If the application is not registered or the all ports used have not been identified in the database this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP2120 Security training not provided**	**STIG Section**	2.4.1 Management 2.5.2 Vulnerability Management Process 2.5.1 Security Incident Response Process 2.6 Workplace Security Procedures
Finding Category	CAT II			
Vulnerability Key	V0016780		**IA Controls**	PRTN-1

Check

Instruction:
Interview the application representative and ask for evidence of security training for managers, designers, developers, and testers. Examples of evidence include course completion certificates and a class roster. At a minimum security training should include Security Awareness Training.

1) If there is no evidence of security training, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2130 Maintenance does not exist or not sufficient**	**STIG Section**	2.5.2 Vulnerability Management Process 2.7 Compliance with DoD Standards
Finding Category	CAT II			
Vulnerability Key	V0016781		**IA Controls**	DCCT-1 PESP-1 DCCS-1 DCCS-2 ECSC-1

Check

Instruction:
Interview the application representative to determine if users are provided with a means of obtaining updates for the application.

1) If users are not provided with a means of obtaining updates for the application, this is a finding.

Interview the application representative to determine if users are provided a mechanism to be notified of security flaws and the availability of patches.

2) If users are not provided security flaw and patch notifications for the application, this is a finding.

Interview the application representative and determine if a vulnerability management process exists.

3) If no vulnerability management process or policy exists, this is a finding.

Interview the application representative to determine maintenance is available for production applications.

4) If maintenance is not available for an application, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2140 An incident response process is not established**	**STIG Section**	2.5.1 Security Incident Response Process 2.6 Workplace Security Procedures
Finding Category	CAT II			
Vulnerability Key	V0016782		**IA Controls**	VIVM-1

Check

Instruction:
Interview the application representative to determine if a security incident response process for the application is established. The application's security incident response process may be part of the sites overall incident response process.

1) If a security incident response process for the application is not documented, this is a finding.

Interview the application representative to determine if a security incident response process for the application is followed.

2) If a security incident response process for the application is not followed, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2150 Inadequate Workplace Security Procedures**	**STIG Section**	2.6 Workplace Security Procedures 2.7 Compliance with DoD Standards
Finding Category	CAT II			
Vulnerability Key	V0016783		**IA Controls**	PESP-1

Check

Instruction:
Determine the sensitivity of the data of the application by reviewing the confidentiality levels for which the system was designed.

If a traditional review is being conducted at the same time as the application review, this check is not applicable.

For sensitive data, the following security guidelines must be followed.

• Verify the existence of policy and procedures to ensure the proper handling and storage of information at the site.
• Verify system media (e.g., tapes, printouts) is controlled and restricts the pickup, delivery, receipt, and transfer of system media to authorized personnel. (NIST MP-5).
• Verify there is a policy that addresses output handling and retention (NIST SI-12).
• Verify policy that addresses output handling and retention is being followed (NIST SI-12).

1) If sensitive data security guidelines do not exist or not followed, this is a finding.

For classified data, the following security guidelines must be followed.

• Verify the existence of policy and procedures to ensure the proper handling and storage of information at the site. (e.g., end-of-day, security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule).
• Verify the existence of a system of security checks at the close of each working day to ensure that the area is secure.
• An SF 701: Activity Security Checklist, is required to record such checks.
• An SF 702: Security Container Check Sheet, is requires to record the use of all vaults, secure rooms, and containers used for the storage of classified material.
• Verify system media (e.g. tapes, printouts) is controlled and restricts the pickup, delivery, receipt and transfer of system media to authorized personnel. (NIST MP-5).
• Verify there is a policy that addresses output handling and retention (NIST SI-12).
• Verify policy that addresses output handling and retention is being followed (NIST SI-12).

2) If classified data security guidelines do not exist or not followed, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP2160 Approved Security Configuration Guidance not used**	**STIG Section**	2.7 Compliance with DoD Standards 3.1.1 Design Document
Finding Category	CAT II			
Vulnerability Key	V0006198		**IA Controls**	DCCS-1 DCCS-2 ECSC-1

Check

Instruction:
The application client (e.g. Web Browser, C++ application) must be designed to work on a STIG compliant platform. Vulnerabilities are discovered frequently and security updates must be applied constantly and may not be reflected in the latest baseline of a secure image of the operating system. Any finding required to make the application client operate correctly will be documented in this check.

Conduct a review (using the SRR process) of an application client platform. The application client platform may not have been included in the overall application review. If the client is Windows based and the application uses either a browser interface or an MS Office Product, a Desktop Application review must also be conducted.

1) If the review of the application client platform produces findings required to make the application client operate correctly, this is a finding.

Ensure the application review includes test & build systems. All deployment, development, test & build systems should be included in the application review to ensure the applicable DoD approved or other acceptable security configuration documents have been applied.

2) If the application review does not include all deployment, development, test & build systems this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3010 Design document is not complete or does not exist**	**STIG Section**	3.1.1 Design Document
Finding Category	CAT II			
Vulnerability Key	V0007013		**IA Controls**	DCFA-1

Check

Instruction:
Ensure that all untrusted application interfaces to external systems are identified, protecting a user from unknowingly trusting an untrusted resource. Ask the application representative for a comprehensive list identifying all interfaces within the application that transmit information with, display content from, or link to an external untrusted resource.

Examine the list or the application itself (if no list is provided) for suspect interfaces. Determine which interfaces connect to trusted DoD systems (certified and installed on a DoD network), untrusted DoD systems (certification unknown, but installed on a DoD network), trusted non-DoD systems (outsourced DoD services where the vendor/provider has provided some level of assurance), and untrusted non-DoD systems.

All interfaces linking or transmitting data to or from untrusted systems are to be documented, labeled, and the users notified.

1) If any of the examined application interfaces are not properly documented, labeled, and the users notified of data transmitted with untrusted systems, this is a finding.

2) If any interface, such as a link or web hyperlink contained within the application, connects to an untrusted system and does not provide some disclaimer or notification to the users that they are leaving a trusted resource, this is a finding.

3) If there is any content displayed to the user from untrusted sources of origin that are not identified, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3020 Threat model not established or updated**	**STIG Section**	3.1.3 Threat Model 3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0006148		**IA Controls**	DCSQ-1

Check

Instruction:
Review the threat model and identify the following sections:
• Identified threats
• Potential mitigations
• Mitigations selected based on risk analysis

Detailed information on threat modeling can be found at the OWASP website.
http://www.owasp.org/index.php/Threat_Risk_Modeling

1) If the threat model does not exist or does not have sections in the document representing the sections this is a finding.

2) If the threat model has not been updated to reflect the application release being reviewed, this is a finding.

Verify the mitigations selected in the threat model have been implemented.

3) If the mitigations selected based on risk analysis have not been implemented, this is a finding.

Review the identified threats from the each of the application's networked components. For example, a backend server may accept SQL queries and SSH connections and also have an NFS share. Next, examine firewall rules and router ACLs that prevent clients from reaching these access points, effectively reducing the area of the threat surface. For example, if the backend database accepts queries but is in an enclave where there are no user workstations and firewall rules allow only web traffic, this is not a finding.

For each of the remaining access points, attempt to access these resources in a similar manner as the application would without utilizing the user interface (e.g., send SQL query using a tool outside of the application or attempt to access a share using command line utilities).

4) If a user can authenticate to any of these remaining access points outside of the intended user interface, this is a finding.

The finding details should note the application component accessed and the method or tool used to access it.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3050 Inactive code and libraries not removed**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0006149		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative if there is a documented process to remove code when it is no longer executed. Also ask if there is a documented process to ensure unnecessary code is not included into a release.

The process may include the following:
· Source Code Analysis Tools
· Development Environments that indicate unused source
· Compiler Options that detect unreachable code.

For a web-based application, conduct a spot check of the code directory (e.g., .html, .asp, .jsp, .php files), sampling at least four files, and ensure the code is executed for the application. If there is no documented process is not in place, check at least 10 pieces of code. Search for possible include files and scripts. Determine if the include files and scripts exist.
Examples of included files and script
jsp
<%@ include file="include.jsp" %>
php
<?php include("include.php"); ?>

asp
<!--#include file="include.html">
js
<script src="include.js" type="text/javascript"></script>
1) If include files and scripts do not exist, this is a finding.

2) If other code is found that is not being used, this is a finding.

Document the name of the file containing the offending code in the finding details.
For Visual Basic or C/C++ and other applications verify that a documented process is in place to prevent unused source code from being introduced into the application. Verify the process by source code analysis tools results, development environment tools, compiler options or the mechanism documented by process that enforces unused source from being introduced into the application.

3) If the application representative does not have a documented policy or there is no evidence that mechanisms are in place to prevent the introduction of unused code into the application, this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3060 Application code and data are co-located**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0006150		**IA Controls**	DCPA-1

Check

Instruction:
Ask the application representative or examine the application documentation to determine the location of the application code and data. Examine the directory where the application code is located.

1) If the application data is located in the same directory as the code, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3070 Application components not separated from data storage**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0016784		**IA Controls**	DCPA-1

Check

Instruction:
Interview the application representative a determine if logical separation exists between application components within the application. Review locations of the components of the application such as web server, database server, and application server. A separate machine is not required but is recommended.

Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, and combinations of these methods, or other methods, as appropriate.

1) If the application components are not separated in the application, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3080 Invalid URL or path references found**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0006157		**IA Controls**	DCSQ-1

Check

Instruction:
Search the source code for common URL prefixes and suffixes and to the extent feasible with available tools, NFS shares, NetBIOS shares and IP addresses.

All such resources should be captured from configuration files. (i.e., “http://”, ftp://, “.mil”, “.com”)

1) If any references are invalid, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3090 Session hijacking prevention not supported**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0016785		**IA Controls**	ECTM-2

Check

Instruction:
Ask the application representative to login and demonstrate the application supports detection and/or prevention of communication session hijacking.

If integrity checks (e.g., hash algorithms, checksums) are not used to detect errors in data streams there is no way to ensure the integrity of the application data as it traverses the network.

1) If the application representative can not demonstrate the above, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3100 Temporary objects not removed from system**	**STIG Section**	3.5 Best Practices
Finding Category	CAT II			
Vulnerability Key	V0006163		**IA Controls**	ECRC-1

Check

Instruction:
Check application to ensure that memory is being released. Also ensure database connections are closed, if applicable. Ask the application representative to demonstrate memory and database connections are released when the application is terminated.

1) If memory is not released and the application is not using garbage collection process for memory (e.g Java Applications), this is a finding.

2) If the application creates new database connections on entry to the application and does not release them on exit of the application, this is a finding.

Ask the application representative to access the application, perform selected actions and exit the application. Ask the application representative to search for files recently created.

For a Windows System:
Use Windows Explorer to search for all files (*.*) created today, and then examine the times to narrow the scope of the files to examine.

For a Unix System:
Enter: # touch -t 200301211020 /tmp/testdatefile

The -t flag represents the time option. The time format to be used with -t is {[CC]YYMMDDhhmm[ss]} where the century [CC] and the seconds [ss] are optional fields.

The resulting file is:
-rw-r--r-- 1 root root 0 Jan 21 10:20 /tmp/testdatefile

Enter a second command:
find / -newer /tmp/testdatefile --> This will produce all files on the system with a date later than that of 'testdatefile'
find ./* -newer /tmp/testdatefile --> This will produce all files, recursively, in the current directory with a date later than that of 'testdatefile'

3) If this list includes temporary files that are not being deleted by the application, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3110 Unneeded functionality enabled**	**STIG Section**	3.5.1 Secure Defaults
Finding Category	CAT II			
Vulnerability Key	V0016786		**IA Controls**	DCSD-1

Check

Instruction:
Ask the application representative to review the installation guide to determine what functionality is installed and enabled by default on installation of the application.

Examples may include the following:
Functions that send information back to the vendor.
Email functions enabled when not required for functionality.

1) If the application installs with functionality which is unnecessary and enabled by default this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3120 Application has error handling vulnerabilities**	**STIG Section**	3.5.2 Error Handling
Finding Category	CAT II-III			
Vulnerability Key	V0006166		**IA Controls**	DCSQ-1

Check

Instruction:
Use the error messages generated from APP3510 as input into this check. Ensure that the application provides error-handling processes. The application code should not rely on internal system generated error handling.

1) If the errors are not be handled by the application and are being processed by the underlying internal system, this is a CAT III finding.

Inspect the verbiage of the message. Ensure that the application does not provide information that can be used by an attacker.

2) If any of the following types of errors are displayed, this is a CAT II finding.

Error messages should not include variable names, variable types, SQL strings, or source code. Errors that contain field names from the screen and a description of what should be in the field should not be considered a finding.

Finding Results

Comments:					
Finding	CAT II ☐ CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3130 Secure design principle not followed**	**STIG Section**	3.5.3 Fail Closed
Finding Category	CAT I-II			
Vulnerability Key	V0016787		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application or the documented code review process.

If the results are provided from a manual code review, the application representative will need to demonstrate how secure design principle vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify secure design principle vulnerabilities, this is a CAT I finding.

2) If all code analysis tool was used to perform a code review and errors have not been fixed, this is a CAT II finding.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3140 Application failure results in an insecure state**	**STIG Section**	3.5.3 Fail Closed
Finding Category	CAT II			
Vulnerability Key	V0006167		**IA Controls**	DCSS-2

Check

Instruction:
Testing application failure will require taking down parts of the application. Examine application test plans and procedures to determine if this type of failure was tested. If test plans exist, validate the tests by performing a subset of the checks. If test plans do not exist, an application failure must be simulated. Simulate a failure. This can be accomplished by stopping the web server service and or the database service. Check to ensure that application data is still protected. Some examples of tests follow. Try to submit SQL queries to the database. Ensure that the database requires authentication before returning data. Try to read the application source files, access should not be granted to these files because the application is not operating. Try to open database files. Data should not be available because the application is not operational.

1) If any of these tests fail, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3150 Application uses unapproved cryptographic modules**	**STIG Section**	3.6.1 FIPS 140-2 3.6.4 Key Exchange
Finding Category	CAT II			
Vulnerability Key	V0006137		**IA Controls**	DCNR-1 ECCR-1 ECCR-2 ECCT-1 ECCT-2

Check

Instruction:
If the application does not utilize encryption, key exchange, digital signature, or hash, FIPS 140-2 cryptography is not required and this check is not applicable.

Identify all application or supporting infrastructure features that require cryptography (file encryption, VPN, SSH, etc.). Verify the application is using FIPS-140 validated cryptographic modules.

The National Institute of Standards and Technology's FIPS 140-1 and FIPS 140-2 Vendor List is located at: http://csrc.nist.gov/cryptval/.

1) If the application requiring encryption, key exchange, digital signature or hash is using an unapproved module or no module, this is a finding.

2) If the application utilizes unapproved modules for cryptographic random number generation, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐ CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3170 Encryption for Key Exchange not used**	**STIG Section**	3.6.4 Key Exchange
Finding Category	CAT II			
Vulnerability Key	V0016788		**IA Controls**	DCNR-1

Check

Instruction:
If the application does not implement key exchange this check is not applicable.

Identify all application or supporting infrastructure features use key exchange. Verify the application is using FIPS-140 validated cryptographic modules for encryption of key exchange algorithms.

1) If the application does not implement encryption for key exchange, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3180 Encryption key permissions are not adequate**	**STIG Section**	3.6.4 Key Exchange
Finding Category	CAT II			
Vulnerability Key	V0016789		**IA Controls**	ECCD-1

Check

Instruction:
Interview the application representative and determine the keys resident on application servers (including X.509 certificates). For the purposes of this checklist, no more than 20 keys need to be examined. Based on the number of keys in the inventory, determine if all of the keys will be examined or just a sample. If a sample will be selected, choose keys of a variety of types (certificate of a certificate authority, certificate of a user, private key of a user, etc.). No user or process should be able to write to any file containing keys. If keys need to be replaced or added, permissions can be changed temporarily for those events.

1) If any privileged or non-privileged user or application process has write permissions to a file containing cryptographic keys, this is a finding.

Determine whether when keys are read, that transaction occurs under the security context of a user account or of the application process (which would perform the transaction on behalf of the user). Ensure that read permissions are granted only to the account(s) that must know the key to make the application function. If any user groups are granted read permissions, check that the members of these groups contain only the users that require knowledge of the key.

2) If any user accounts have read (or greater) permissions to a private or secret key that do not require such permissions, this is a finding.

3) If any group with read permissions contains a user that does not require such permissions, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3190 Database connections use administrative accounts**	**STIG Section**	3.7.1 Database Management System
Finding Category	CAT II			
Vulnerability Key	V0016790		**IA Controls**	ECLP-1

Check

Instruction:
If the application does not use a database, this check is not applicable.

Ask the application representative how the application authenticates to the database.

1) If the application authenticates to the database by using a database account that has database administrator access, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3200 No support for roll-back and journaling**	**STIG Section**	3.7.1 Database Management System
Finding Category	CAT III			
Vulnerability Key	V0016791		**IA Controls**	ECDC-1

Check

Instruction:
If the application is not a transaction based application that stores and retrieves data, this finding is not applicable.

Ask the application representative if the application uses a database to store information. If the application utilizes Oracle, SYBASE, or Microsoft SQL Server then support for journaling and rollback is already present in the tools.

*Note: Microsoft Access does not support journaling and rollback. If Microsoft Access is used, ask the application representative to demonstrate the rollback and journaling features of the application.

1) If the application representative cannot demonstrate support for journaling and rollback, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3210 Sensitive data not protected at rest**	**STIG Section**	3.7.2 Data Storage
Finding Category	CAT II			
Vulnerability Key	V0006135		**IA Controls**	ECCR-1 ECCR-2

Check

Instruction:
Review the system security plan or interview the application representative to determine the classification of data in the application. Also review encryption mechanisms protecting the data.

NIST-certified cryptography should be used to protect stored sensitive information if required by the information owner.

NIST-certified cryptography should be used to protect stored classified non-SAMI (Sources and Methods Information) data if required by the information owner.

NSA-approved cryptography should be used to protect stored classified SAMI information.

1) If data at rest is not protected with the appropriate level of encryption this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3220 Sensitive data is not encrypted in memory**	**STIG Section**	3.7.3 In-Memory Data Handling
Finding Category	CAT II			
Vulnerability Key	V0016792		**IA Controls**	ECCR-1 ECCR-2

Check

Instruction:
If the application contains classified information, this check is not applicable.
If the application contains public information, this check is not applicable.

Ask the application representative to review global variables for the application. If the global variables contain sensitive information ask the application representative if they are required to be encrypted by the data owner. If the data is required to be encrypted by the data owner, ask the application representative to demonstrate they are encrypted. The .Net

The .Net Framework 2.0 and higher provides a SecureString class which can encrypt sensitive string values

1) If sensitive information is required to be encrypted by the data owner and global variables containing sensitive information are not encrypted, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3230 Application does not clear all memory blocks**	**STIG Section**	3.7.3 In-Memory Data Handling
Finding Category	CAT II			
Vulnerability Key	V0016793		**IA Controls**	ECCR-1 ECCR-2

Check

Instruction:
If the application does not contain sensitive or classified information, this check is not applicable

Ask the application representative to demonstrate how the application clears and releases memory blocks. Microsoft Visual C++ provides SecureZeroMemory that will not be optimized out of code for clearing sensitive and classified data.

1) If the application releases objects before clearing them, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3240 Actions not authorized before execution**	**STIG Section**	3.7.3 In-Memory Data Handling
Finding Category	CAT II			
Vulnerability Key	V0006142		**IA Controls**	ECRC-1

Check

Instruction:
Verify with the application representative how the application authorizes transactions. The authorization function may leverage file permissions enforced by the operating system or views enforced by the database software. Alternatively, authorization mechanisms may be built into the application code. If the latter is the case, ask the application developer to locate the modules in the code that perform the authorization function. Review these to assess their adequacy. The actual code review need not occur on a production system so long as it is equivalent to that code.

If the application leverages the access controls of the database or operating system software, identify cases in which permissions are granted to everyone, world, public or similar user or group for which all users would be authorized. Ask the application SA or developer if it is the stated intention that the resource be public such that everyone will be authorized to access the resource. OS or database access controls must be evaluated in the production environment because there is a significant probability these differ from those in the lab environment.

1) If neither the application code nor the access controls of supporting software provide appropriate controls preventing unauthorized users from performing transactions that require authorization, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3250 Sensitive data not protected in transit**	**STIG Section**	3.7.4 Data Transmission
Finding Category	CAT I-II			
Vulnerability Key	V0006136		**IA Controls**	ECCT-1 ECCT-2 ECNK-1

Check

Instruction:
Interview the application representative to determine if sensitive data is transmitted over a commercial circuit or wireless network (e.g., NIPRNet, ISP).

1) If any sensitive data is transferred over a commercial or wireless network and is not encrypted using NIST FIPS 140-2 validated encryption, this is a CAT I finding.

Interview the application representative to determine if classified data is transmitted over a network cleared to a lower level than the data. (e.g. TS over SIPRNet, Secret over NIPRNet).

2) If classified data is transmitted over a network cleared to a lower level than the data and NSA-approved type-1 encryption is not used to encrypt the data, this is a CAT I finding.

Interview the application representative and determine if the data in transit must be separated for need-to-know reasons.

3) If data in transit across a network at the same classification level is separated for need-to-know reasons and the data is not minimally encrypted using NIST FIPS 140-2 validated encryption this is a CAT II finding.

Interview the application representative and determine if SAMI data is transmitted.

4) If SAMI data in transit across a network at the same classification level is not separately encrypted using NSA Type 1 approved encryption this is a CAT II finding.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3260 Integrity mechanisms on data files not supported**	**STIG Section**	3.7.5 Data Integrity
Finding Category	CAT II			
Vulnerability Key	V0016794		**IA Controls**	ECTM-2 ECML-1

Check

Instruction:
Ask the application representative to demonstrate the application supports mechanisms assuring the integrity of all transmitted information to include labels and security parameters.

1) If the application does not support integrity mechanisms for any transmitted data, this is a finding.

Ask the application representative to login and demonstrate the application supports integrity mechanisms for transmission of both incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).

2) If the application does not support integrity mechanisms for file transmission, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3270 Classification labels not appropriately displayed**	**STIG Section**	3.7.6 Data Marking
Finding Category	CAT II			
Vulnerability Key	V0006146		**IA Controls**	ECML-1

Check

Instruction:
Before actual testing, determine which application functions to examine, giving preference to report generation capabilities and the most common user transactions that involve sensitive data (FOUO, secret or above). Ask the application representative for the application's classification guide. This guide should document the data elements and their classification. Logon to the application and perform these in sequence, printing output when applicable. The application representative's assistance may be required to perform these steps. For each function, note whether the appropriate markings appear on the displayed and printed output. If a classification document does not exist, data must be marked at the highest classification of the system.

Appropriate markings for an application are as follows: For classified data, markings are required at a minimum at the top and the bottom of screens and reports. For FOUO data, markings are required at a minimum of the bottom of the screen or report. In some cases technology may prohibit the appropriate markings on printed documents. For example, in some cases, this is not possible to mark all pages top and bottom when a user prints from a browser. If this is the case, ask the application representative if user procedures exist for manually marking printed documents. If procedures do exist, examine the procedures to ensure that if the users were to follow the procedures the data would be marked correctly. Also ask how these procedures are distributed to the users.

1) If appropriate markings are not present within the application and it is technically possible to have the markings present, this is a finding.

2) If it is not technically feasible to meet the minimum marking requirement and no user procedures exist or if followed the procedures will result in incorrect markings, or the procedures are not readily available to users, this is a finding.

In any case of a finding, the finding details should specify which functions failed to produce the desired results.

After completing the test, destroy all printed output using the site's preferred method for disposal. For example utlizing a shredder or disposal in burn bags.

Note: Physical markings on hardware do not meet this requirement.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3280 The application is not PK-enabled**	**STIG Section**	3.8.3.1 PKI User Authentication
Finding Category	CAT II			
Vulnerability Key	V0006127		**IA Controls**	DCBP-1 IATS-2 IAKM-2 DCNR-1

Check

Instruction:
This check is not applicable where application users are determined to have authorized access to the application and not eligible to receive a CAC/DoD PKI certificates. (e.g. Retirees, Dependents) as defined by DoDI 8520.2.

1) Ask the application representative if an application is PK-enabled. If the answer is no, this a finding.

If the application is in a production environment the application representative should be able to login to the application with a CAC.

If the application resides on the SIPRNet or in a test environment the application representative may only have test certificates and should be able to login to the application with a soft certificate.
Note: The certificates for this check do not need to be DoD approved certificates.

2) If the application representative cannot login the application with either soft certificates or certificates from a CAC, this is a finding.

Ask the application representative where the certificate store is for the application and verify there are the correct test or production certificates for user authentication. Make certain a certificate is required for user authentication. Ask the application representative to temporarily remove the certificate from the certificate store and authenticate to the application.

For web application using Internet Explorer from the Tools Menu Select “Internet Options”
Select “Content” Tab
Select “Certificates”
Select “Remove”
Other applications certificate stores will have similar features.

3) If the application representative can login to the application without either soft certificates or certificates stored on a CAC or another authentication mechanism, this is a CAT I finding for check APP3460. This finding should not be recorded for this check.

4) Ask the application representative to demonstrate encryption is being used for authentication if the application representative can’t demonstrate encryption is being used this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3290 The application utilizes a PKI other than DOD PKI**	**STIG Section**	3.8.3.1 PKI User Authentication 3.8.3.2 PKI Server Authentication
Finding Category	CAT II			
Vulnerability Key	V0006128		**IA Controls**	DCBP-1 IATS-2 IAKM-2 DCNR-1

Check

Instruction:
If the application is not PK-enabled this check is not applicable.

If the application resides on the SIPRNet and PKI infrastructure is unavailable this check is not applicable.

Ask whether the application utilizes PKI certificates other than DoD PKI and External Certification Authority (ECA) certificates. Verify the certificate used in authentication in APP3280.

Internet Explorer can be used to view certificate information.
Select “Tools”
Select “Internet Options”
Select “Content” Tab
Select “Certificates”
Select the certificate used for authentication
Click “View”
Select “Details” Tab
Select “Issuer”

1) If the application utilizes PKI certificates other than DoD PKI and ECA certificates, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3300 Server authentication is not PK-enabled**	**STIG Section**	3.8.3.2 PKI Server Authentication
Finding Category	CAT II			
Vulnerability Key	V0006168		**IA Controls**	IATS-1 IATS-2

Check

Instruction:
Ask the application SA or developer if the application enables clients to authenticate the server or the application it is communicating with. The most common example of this type of authentication is when a client validates a server's PKI certificate when initiating an SSL or IPSEC connection.

1) If the SA or developer answers that this capability is not present, this is a finding.

If the SA or developer states that the capability is present, validate this by logging on to each component that supports authentication of servers. For web applications, note cases in which the client browser issues a warning that the server's certificate is not valid. Reasons include:

• A trusted certificate authority did not issue the certificate
• The certificate has expired
• The name of the certificate does not match the URL of the page you are trying to view

The client application should provide a function to allow or disallow the server access to the client application. The server must be setup with a certificate for identification.

Determine if the application checks for server authentication before allowing the user to continue. The server's certificate should be checked by the user's web browser or client application.

2) If there is no server certificate or the client application does not validate the server certificate this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3305 Expired revoked untrusted certificates honored**	**STIG Section**	3.8.3.3 PKI Certificate Validation
Finding Category	CAT I			
Vulnerability Key	V0006129		**IA Controls**	DCBP-1 IATS-2 IAKM-2 DCNR-1

Check

Instruction:
If the application is not PK-enabled this check is not applicable.

If the application resides on the SIPRNet and PKI infrastructure is unavailable this check is not applicable.

This check is not applicable where system users are determined to be information privileged individuals, volunteers, or Reservists as in the DoDI 8520.2.

DoD Test Certificates can be obtained from the following website.
http://jitc.fhu.disa.mil/pki/lab2.html

Note: Before executing this check the following certificate types need to be obtained:
• Expired
• Revoked
• Improperly Signed

If the application is PK Enabled and is not using DoD PKI certificates, the application representative will need to provide these certificates.

If the application is a web-application that utilizes client certificates, validate the proper functioning of the PKI-functionality using a laptop configured for the Application SRR using an expired and revoked certificate. This laptop contains three user profiles: one with a revoked certificate, one with an expired certificate, and one with an improperly signed certificate. Log on each of the user accounts for which there is an associated “bad certificate” profile and perform selected functions in the application that require the use of a certificate (e.g., authentication).

1) If the expired, revoked or improperly signed certificate can be used for application functions, this is a finding.

Also review the web server’s configuration to ascertain whether appropriate certificate validity checks are occurring.

2) If the web server does not check for and deny expired, revoked or improperly signed certificates, this is a finding.

If the application is not a web-application, work with an application SA to identify PK enabled application functions and then sequentially install the invalid certificates, testing each of the functions against each of the certificates. 3) Any successful use of any of the invalid certificates is a finding. If a finding is found in any of the preceding steps document the details of the finding to include the following: • Which of the invalid certificates was accepted (potentially more than one). • The specific application functions that accepted the invalid certificate.					
Finding Results					
Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3310 Clear text passwords displayed**	**STIG Section**	3.8.4 Password Authentication
Finding Category	CAT I			
Vulnerability Key	V0016795		**IA Controls**	IAIA-1

Check

Instruction:
Ask the application representative to login to the application.

If the application uses password authentication, the password should not be displayed as clear text..

1) If the password is displayed as clear text, this is a finding.

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3320 Userids have weak passwords**	**STIG Section**	3.8.4.1 Password Complexity and Maintenance 3.8.6 User Accounts
Finding Category	CAT II			
Vulnerability Key	V0006130		**IA Controls**	IAIA-1

Check

Instruction:
If the entire authentication process for the application is performed by the operating system (such is the case for a Desktop Application), this check is Not Applicable.

First, inventory all the password based authentication processes present in the application. For example, a web server may effectively act as a client when authenticating with a backend database server. Peer-to-peer processes also are included because each peer still acts in the role of a client or server for particular transactions. Each process must be evaluated separately. If multiple processes must be used for a single authentication attempt, the combination of the processes should be evaluated to ensure this check is fully met.

In addition, the authentication may involve a user account database specific to the application or it may involve leveraging the authentication service of an operating system or directory service.

1) If the authentication process involves the presentation of a user account name only, this is a finding.

If the authentication is based on passwords, the passwords must have the following characteristics:

• A minimum of 15 characters
• Include at least one uppercase alphabetic character
• Include at least one lowercase alphabetic character
• Include at least one non-alphanumeric (special) character
• Expire after 60 days
• Be different from the previous 10 passwords used
• Be changeable by the administrator at any time
• Be changeable by the associated user only once in a 24 hour period (for human user accounts)
• Not be changeable by users other than the administrator or the user with which the password is associated

2) If the passwords do not have these characteristics this is a finding.

To verify compliance with these requirements, check the configuration of the software that manages the authentication process (e.g., OS, directory, and database or application software) and determine if each of the criteria listed are met. Also sample individual accounts to determine if any of the policy settings are overridden (e.g., password set to never expire). Focus on non-

human user accounts, as these are the most likely to violate the stated requirements. Non-human accounts, sometimes known as services accounts, may not be set to expire after 60 days.					
Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3330 Passwords not transmitted encrypted**	**STIG Section**	3.8.4.2 Password Transmission
Finding Category	CAT I			
Vulnerability Key	V0016796		**IA Controls**	ECCT-1

Check

Instruction:
Ask the application representative to demonstrate that passwords are encrypted before they are transmitted.

1) If the application does not use passwords for identification and authentication, this check is not applicable.

2) If the application does not encrypt passwords before transmitting them, this is a finding.

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3340 Passwords stored in an unapproved encrypted format**	**STIG Section**	3.8.4.3 Password Storage
Finding Category	CAT I-II			
Vulnerability Key	V0016797		**IA Controls**	IAIA-1 IAIA-2

Check

Instruction:
With respect to I&A information, only administrators and the application or OS process that access the information should have any permissions to these files. In many cases, local backups of the accounts database exist so these must be included in the scope of the review.

Authentication credentials such as passwords are required to be encrypted. Check the configuration of the application software to determine if encryption settings have been activated for the relevant data.

1) If these encryption settings have not been turned on, this is a CAT II finding.

If the data encryption functionality is not configurable and the I&A data are stored in ASCII or another readable format, examine the actual data to determine if they are in clear text.

2) If the authentication data is readable, this is a CAT I finding.

Record findings, regardless of whether or not the vulnerability has been captured in another SRR. For example, any weakness in OS authentication scheme that the application leverages applies both to the OS and the application.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3350 Embedded authentication data stored in code**	**STIG Section**	3.8.5 Authentication Credentials Protection
Finding Category	CAT I-II			
Vulnerability Key	V0006156		**IA Controls**	IAIA-1 IAIA-2

Check

Instruction:
Review source code (including global.asa, if present), configuration files, scripts, HTML file, and any ascii files to locate any instances in which a password, certificate, or sensitive data is included in code.

If credentials were found, check the file permissions on the offending file.

1) If the file permissions indicate that the file has no access control permissions (everyone can read or is world readable) this is a CAT I finding.

2) If there is a level of file protection that requires that at least authenticated users have read access, this is a CAT I finding.

3) If a level of protection exists that only administrators or those with a UID of 0 can read the file this is a CAT II finding.

The finding details should note specifically where the offending credentials or data were located and what resources they enabled.

Finding Results

Comments:					
Finding	CAT I ☐	CAT II ☐	CAT III ☐		
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3360 Authentication data permissions not adequate**	**STIG Section**	3.8.5 Authentication Credentials Protection
Finding Category	CAT II-III			
Vulnerability Key	V0016798		**IA Controls**	ECCD-1

Check

Instruction:
Identification and authentication information must be protected by appropriate file permissions. Only administrators and the application or OS process that access the information should have any permissions to access identification and authentication information. In many cases, local backups of the accounts database exist so these must be included in the scope of the review.

1) If non-privileged users have the permission to read or write password files other than resetting their own password, this is a CAT II finding.

2) If non-privileged users can read user information (e.g., list users but not passwords), this is a CAT III finding.

Finding Results

Comments:					
Finding	CAT II ☐ CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3370 Unneeded accounts active**	**STIG Section**	3.8.6 User Accounts
Finding Category	CAT II			
Vulnerability Key	V0016799		**IA Controls**	DCSD-1

Check
Instruction: Ask the application representative what accounts are enabled by default on installation of the application. 1) If the application installs with accounts unnecessary enabled by default this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3380 Application userids are not unique**	**STIG Section**	3.8.6 User Accounts
Finding Category	CAT II			
Vulnerability Key	V0006131		**IA Controls**	IAIA-1

Check

Instruction:
If the user accounts used in the application are only operating system or database accounts this check is Not Applicable.

Identify duplicate user IDs. If these are not available, sort the list by the user name and, if applicable, associated user ID number so that duplicates will be contiguous and thus easier to locate.

1) If any duplicates user accounts are discovered, this is a finding.

The finding details should specify the duplicates by name, unless they are too numerous to document, in which case a numerical count of the IDs is more appropriate.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3390 User accounts not locked after invalid logons**	**STIG Section**	3.8.6 User Accounts
Finding Category	CAT I			
Vulnerability Key	V0016800		**IA Controls**	ECLO-1

Check
Instruction: Ask the application representative to demonstrate the application locks a user account if a user enters a password incorrectly more than three times in a 60 minute period. 1) If the account is not disabled this is a finding.

Finding Results					
Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3400 User accounts unlocked by person other than admin**	**STIG Section**	3.8.6 User Accounts
Finding Category	CAT II			
Vulnerability Key	V0016801		**IA Controls**	ECLO-1

Check
Instruction: Ask the application representative to demonstrate only the administrator can unlock locked accounts. 1) If the application allows non-administrator to unlock their accounts, this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3410 Session limits do not exist for the application**	**STIG Section**	3.8.7 Sessions
Finding Category	CAT II			
Vulnerability Key	V0006144		**IA Controls**	ECLO-1

Check

Instruction:
Work with the application representative to identify application modules that involve user or process sessions (e.g., a user may initiate a session with a web server, which in turn maintains sessions with a backend database server). For each session type, ask the application representative the limits on:
• Number of sessions per user ID
• Number of sessions per application

1) If the application representative states the session limits are absent for any of the session types, this is a finding.

In many cases, session configuration parameters can be examined. If configuration parameters are embedded within the application they may not be available for review. Any configuration settings that are not configurable should be manually tested. The preferred method depends on the application environment.

2) If there is no evidence of a required session limit on one or more of the session types, this is a finding.

The finding details should note specifically which types of sessions are left unbounded and thus more vulnerable to denial of service attacks.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3415 Sessions do not automatically terminate**	**STIG Section**	3.8.7 Sessions
Finding Category	CAT II			
Vulnerability Key	V0016802		**IA Controls**	ECLO-1

Check

Instruction:
Interview application representative to identify the length of time a user can be idle before the application will time out and terminate the session and require reauthentication.

1) If the application representative states that one or all of the limits are absent for one or more session types, this is a finding.

In many cases, session configuration parameters can be examined. If configuration parameters are embedded within the application they may not be available for review. Any configuration settings that are not configurable should be manually tested. The preferred method depends on the application environment.

Manually validate session limits by empirical testing (logon on multiple times and leaving sessions idle). In some cases, testing session limits is not feasible because they may be set too high to properly simulate them during the review.

Even if the application does not provide time limits for idle sessions, such limits may exist at the transport layer (e.g., TCP timeouts). Consider all possible ways in which limits might be enforced before documenting a finding.

2) If there is no evidence of a required session timeout, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3420 Explicit logout not available**	**STIG Section**	3.8.7 Sessions
Finding Category	CAT II			
Vulnerability Key	V0006155		**IA Controls**	DCSQ-1

Check

Instruction:
Log on to the application and then attempt to log out. If this option is not available, ask the application representative to explain how this function is performed.

1) If the ability to log out is absent or is hidden to the extent most users cannot reasonably expect to easily find it, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3430 Authentication credentials not removed**	**STIG Section**	3.8.7 Sessions
Finding Category	CAT I-II			
Vulnerability Key	V0006153		**IA Controls**	IAIA-1 IAIA-2

Check

Instruction:
Persistent cookies are the primary means by which an application stores authentication information over more than one browser session. If the application is a web-based application, verify that Internet Explorer (IE) is set to warn the user before accepting a cookie. Logon to the application and perform several standard operations, noting if the application ever prompts the user to accept a cookie. Log out, close the browser and check the /Windows/cookies, /Windows/profiles/xyz/cookies, and the /documents and settings/xyz/cookies directories (where xyz is replaced by the Windows user profile name). If a cookie has been placed in either of these directories, open it (using Notepad or another text editor) and search for identification or authentication data that remain after to check for sensitive application data.

1) If authentication credentials exist (e.g., a password), this is a CAT I finding.

2) If identification information (e.g., user name, ID, or key properties) exists, but is not accompanied by authentication credentials such as a password, this is a CAT II finding.

The application may use means other than cookies to store user information. If the reviewer detects an alternative mechanism for storing I&A information locally, examine the credentials found.

3) If authentication data (e.g., a password), is found this is a CAT I finding.

4) If identification information is found (e.g., user name, ID or key properties) but is not accompanied by authentication credentials such as a password, this is a CAT II finding.

5) If the application will initiate additional sessions without requiring authentication after logging out of the application, this is a CAT I finding

Web applications using autocomplete can be setup to store passwords and sensitive data. Many operating systems centrally control the autocomplete feature and it is disabled in the Desktop Application STIG. Workstations that do not have this feature disabled by default have the risk of storage of password information and sensitive information. Examples include public kiosiks and home workstations connecting to the NIPRNet where this feature may be disabled.

View the html pages that contain password and sensitive information to determine if autocomplete feature has been turned off.

Example form html:
<FORM AUTOCOMPLETE = "off">

Autocomplete are explained further at the Microsoft website.
http://msdn.microsoft.com/en-us/library/ms533486(VS.85).aspx

6) If the application is configured to allow autocomplete for passwords,
this is a CAT I finding.

7) If the application is configured to allow for sensitive information fields,
this is a CAT II finding.

If URLs with embedded sessions ids can be forwarded and this URL could be used to gain access to a system without authentication.

Example URL with embedded sessionid.
https://10.55.3.2:8443/login.do;jsessionid=F2EE8C97B24635C9995A9D08E69D7B44

8) If URLs containing embedded session ids can be forwarded and used to gain access to the application without authentication, this is a CAT I finding.

Finding Results					
Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3440 Logon warning not displayed**	**STIG Section**	3.8.8 Logon Banner
Finding Category	CAT II			
Vulnerability Key	V0006152		**IA Controls**	ECWM-1

Check

Instruction:
Logon to the application. If a warning message appears compare it to the 2 following banners:

Use the following banner for desktops, laptops, and other devices accommodating banners of 1300 characters:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

For Blackberries and other PDAs/PEDs with severe character limitations use the following banner:

I've read & consent to terms in IS user agreem't.

These banners are mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance.

1) If the login banner is not one of the above banners or the login banner is missing this is a finding. If the only way to access the application is through the OS then an additional banner is not required at the application level. at the application level.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3450 Application resources has inappropriate permission**	**STIG Section**	3.9 Access Control 3.9.1 Name Resolution
Finding Category	CAT II			
Vulnerability Key	V0016803		**IA Controls**	ECCD-1

Check

Instruction:
Ask the application representative to demonstrate the application resources has appropriate access permissions.

1) If the application representative can not demonstrate all application resources has appropriate access permissions, this is a finding.

Review the locations of all format strings used by the application. Ask the application representative to demonstrate format strings used by the application are restricted to authorized users.

2) If access permissions to format string are not restricted to application administrators, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3460 Resource name used to control access**	**STIG Section**	3.9.1 Name Resolution
Finding Category	CAT I			
Vulnerability Key	V0016804		**IA Controls**	DCSQ-1

Check

Instruction:
Verify the application does not grant access solely based on a resource name. (e.g. username, IP address, machine name) Also verify a username with a blank password grants also does not grant access to the application.

1) If authentication is granted based on a resource name only this is a finding.

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3470 Application functionality not role based**	**STIG Section**	3.9.2 Role Based Access 3.9.2 Role Based Access
Finding Category	CAT II			
Vulnerability Key	V0006154		**IA Controls**	ECPA-1 ECCD-2

Check

Instruction:
If Oracle or SQL Server defined roles are being used, the Database SRR covers this check. Mark this check as Not Applicable.

Log on as an unprivileged user. Examine the user interfaces (graphical, web and command line) to determine if any administrative functions are available. Privileged functions include the following:

• Create, modify and delete user accounts and groups
• Grant, modify and remove file or database permissions
• Configure password and account lockout policy
• Configure policy regarding the number and length of sessions
• Change passwords or certificates of users other than oneself
• Determine how the application will respond to error conditions
• Determine auditable events and related parameters
• Establish log sizes, fill thresholds and fill behavior (i.e., what happens when the log is full)

1) If non-privileged users have the ability to perform any of the functions listed above, this is a finding.

Finding details should specify which of the functions are not restricted to privileged users.

Work closely with the application SA before testing any administrative changes to ensure local change management procedures are followed. Immediately back out of any changes that occur during testing.

Review administrative rights assignments in all application components, including the database software and operating system.

On Windows systems, review each of the User Rights to determine which users and groups are given more than default capabilities. User Rights can be viewed by using DumpSec then selecting Reports, Dump Rights.

2) If privileged rights are granted to non-privileged users, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3480 Access control mechanism not in place**	**STIG Section**	3.9.2 Role Based Access 3.1 Input Validation
Finding Category	CAT II			
Vulnerability Key	V0006141		**IA Controls**	ECCD-2 ECLP-1 DCSQ-1

Check

Instruction:
Ask the application representative if particular administrative and user functions can be restricted to certain roles. The objective is to ensure that the application prohibits combination of roles that represent an IA risk. In particular, inquire about separation of duties between the following:

• Personnel that review and clear audit logs and personnel that perform non-audit administration.
• Personnel that create, modify, and delete access control rules and personnel that perform either data entry or application programming.

1) If the application representative states that the application does not enforce separation of duties between the roles listed above, this is a finding.

If the representative claims that the required separation exists, identify which software component is enforcing it. Evidence of enforcement can either involve the display of relevant security configuration settings or a demonstration using different user accounts, each assigned to a different role.

2) If the application representative cannot provide evidence of separation of duties, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3500 Application runs with excessive privileges**	**STIG Section**	3.9.3 Excessive Privileges
Finding Category	CAT II			
Vulnerability Key	V0006143		**IA Controls**	ECLP-1

Check

Instruction:
Identify the application user account(s) that the application uses to run. These accounts include the application processes (defined by Control Panel Services (Windows) or ps –ef (UNIX). Also for an n-tier application, the account that connects from one service (such as a web server) to another (such as a database server).

Determine the user groups in which each account is a member. List the user rights assigned to these users and groups and evaluate whether any of them are unnecessary.

1) If the rights are unnecessary, this is a finding.

2) If the account is a member of the Administrators group (Windows) or has a User Identification (UID) of 0 (i.e., is equivalent to root) (UNIX) this is a finding.

3) If this account is a member of the SYSAdmin fixed server role in SQL Server, this is a finding.

4) If the account has DDL (Data Definition Language) privileges, (create, drop, alter) or other system privileges this is a finding.

Search the file system to determine if these users or groups have ownership or permissions to any files or directories.

Review the list of files and identify any that are outside the scope of the application.

5) If there are such files outside the scope of the application, this is a finding.

Check ownership and permissions and identify permissions beyond the minimum necessary to support the application.

6) If there are instances of unnecessary ownership or permissions, this is finding.

The finding details should note the full path of the file(s) and the associated issue (i.e., outside scope, permissions improperly granted to user X, etc.).

7) If the target is a .NET application that executes with least privileges using code access security (CAS), this is not a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3510 Insufficient input validation**	**STIG Section**	3.1 Input Validation
Finding Category	CAT I-II			
Vulnerability Key	V0006164		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for the test plans for the application, which should be included in SSAA documentation. Examine the test plan to determine if testing was performed for invalid input. Invalid input includes presence of scripting tags within text fields, query string manipulation, and invalid data types and sizes. If the test plans indicate these types of tests were performed, only a small sampling of testing is required. If the test plans do not exist or do not indicate that these types of tests were performed more detailed testing is required. Testing should include logging on to the application and entering invalid data. If there are various user types defined within the system, this test should be repeated for all user types.

Test the application for invalid sizes and types. Test input fields on all pages/screens of the application. Try to exceed buffer limits on the input fields. Try to put wrong types of data in the input fields. For example put character data in numeric field.

1) If invalid input can be used to bypass the login screen, this is a CAT I finding.

2) If invalid input can be used to bypass access control functions to allow an authenticated user access to data that should be restricted this is a CAT II finding.

For query string manipulation testing, determine if the user bypasses access control functions to gain to data that should be restricted based on the users security level or role. For example, if a query string such www.testweb.mil/apppage.asp?xyz=113&asd=185 gives the user access to data for data identifier number 185. Try to resubmit the query string with another three digit number say 186 to see if that data is displayed. If this data would can be displayed through reports or other access points in the application this would not be considered a finding.

3) If data displayed in the query manipulation testing is above the users security level or role, this is a CAT II finding.

For script tag embedding, select a text field of the application that accepts at least 15 characters. Try to input a script tag (script) into the field. If the data is accepted without an error, access the data entered via the application (this process will vary depending upon the application).

4) If the script tag in its entirety is displayed within the application this is a CAT II finding.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3520 No Trust boundary data validation**	**STIG Section**	3.1 Input Validation
Finding Category	CAT II			
Vulnerability Key	V0016805		**IA Controls**	DCSQ-1

Check

Instruction:
Review the threat model and analyze the trust boundaries. Ask the application representative for evidence that all trust boundaries validates input. Ask the application representative to provide documented interfaces with ranges of expected values for input parameters. Also review the interface for handling of unexpected input such as special characters.

1) If the boundary interface does not filter or validate input, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3530 Application does not set character set**	**STIG Section**	3.1 Input Validation
Finding Category	CAT II			
Vulnerability Key	V0016806		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to review web pages and determine the application sets the character set.

Perl
After the last header look for
print "Content-Type: text/html; charset=utf-8\n\n";

PHP.
Look for the header() function before any content is generated
header('Content-type: text/html; charset=utf-8');

Java Servlets.
Look for the setContentType method on the ServletResponse object
Objectname.setContentType ("text/html;charset=utf-8");

JSP.
Look for a page directives
<%@ page contentType="text/html; charset=UTF-8" %>

ASP
Look for Response.charset
<%Response.charset="utf-8"%>

ASP.Net
Look for Response.ContentEncoding
Response.ContentEncoding = Encoding.UTF8;

1) If the application representative can not demonstrate the above, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3540 Application is vulnerable to SQL Injection**	**STIG Section**	3.10.1 SQL Injection Vulnerabilities
Finding Category	CAT I-II			
Vulnerability Key	V0016807		**IA Controls**	DCSQ-1 DCSQ-1

Check

Instruction:
SQL Injections attacks can be used to bypass the login to the application or provide authenticated user access to data that should not normally be provided by the application.

Test applications using Oracle, Microsoft SQL Server and other backend databases by putting a single ' in any of the fields used to login. Submit the form and check for a server error 400. If the error occurs the application is not properly validating input fields. If an invalid user or password message is returned upon submitting the web form, the application is at least minimally protected.

Fill in login fields with potentially valid user names (e.g. admin, system, root, adminstrator) with a comment field to ignore the rest of the SQL query. Fill in the password fields with any values and submit the form.

username' --
username' #
username'/*

1) If the application provides a valid login to these inputs, this is a CAT 1 finding.

Try to append the "or" operator with a true value "1=1" and comment field. This will test if a SQl query could be passed into the application for execution.

Fill in the login and password fields one at a time with the inputs below and submit the form.

' or 1=1--
' or 1=1#
' or 1=1/*
') or 1=1--
') or 1=1#
') or 1=1/*

2) If the application provides a valid login to these inputs, this is a CAT 1 finding.

Also other fields not associated with the login fields should be tested.

Fill in the each of the inputs one at a time with the inputs below and submit the form.

' or 1=1--
' or 1=1#
' or 1=1/*
') or 1=1--
') or 1=1#
') or 1=1/*

3) If the application provides an authenticated user access to data that should be restricted this is a CAT 2 finding.

Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool. If the application representive can not provide results from a code review, then ask the application representive to demonstrate how the applications meets the requirements below.

Identify from the code review results or the application reprsentative demonstration how the application
- uses prepared statements for SQL queries
- does not provide direct access to tables (e.g. access is provided by views and stored procedures)
- does not use concatenation or use replacement to build SQL queries

4) If the results are not provided from a manual code review or automated tool or the application representative can not demonstrate the application uses prepared statements for SQL queries, this is a CAT II finding

5) If the results are not provided from a manual code review or automated tool or the application representative can not demonstrate the application does not use concatenation or use replacement to build SQL queries, this is a CAT II finding

6) If the results are not provided from a manual code review or automated tool or the application representative can not demonstrate the application does not directly accesses tables in adatabase, this is a CAT II finding.

7) If APP3500 is a finding due to the application account being a member of the Administrators group (Windows), has a UID of 0 (i.e., is equivalent to root) (UNIX), is a member of the SYSAdmin fixed server role in SQL Server or has DDL (Data Definition Language) privileges, any findings found in this check should be upgraded to a CAT I finding.mber of the SYSAdmin fixed server role in SQL Server or has DDL (Data Definition Language) privileges, any findings found in this check should be upgraded to a CAT I finding.

Finding Results					
Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3550 Application is vulnerable to integer overflows**	**STIG Section**	3.10.2 Integer Arithmetic Vulnerabilities
Finding Category	CAT I			
Vulnerability Key	V0016808		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review, the application representative will need to demonstrate how integer overflow vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify integer overflow vulnerabilities, this is a finding.

Examples of Integer Overflow vulnerabilities can be obtained from the OWASP website.
http://www.owasp.org/index.php/Integer_overflow

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3560 Application contains format string vulnerabilities**	**STIG Section**	3.10.3 Format String Vulnerabilities
Finding Category	CAT I			
Vulnerability Key	V0016809		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review, the application representative will need to demonstrate how format string vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify format string vulnerabilities, this is a finding.

Examples of Format String vulnerabilities can be obtained from the OWASP website.
http://www.owasp.org/index.php/Format_string_problem

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3570 Application vulnerable to Command Injection**	**STIG Section**	3.10.4 Command Injection Vulnerabilities
Finding Category	CAT I			
Vulnerability Key	V0016810		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review, the application representative will need to demonstrate how command injection vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify command injection vulnerabilities, this is a finding.

Examples of Command Injection vulnerabilities can be obtained from the OWASP website.
http://www.owasp.org/index.php/Command_Injection

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3580 Application vulnerable to Cross Site Scripting**	**STIG Section**	3.10.5 Cross Site Scripting (XSS) Vulnerabilities
Finding Category	CAT I			
Vulnerability Key	V0016811		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review the application representative will need to demonstrate how cross site scripting vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify cross site scripting vulnerabilities, this is a finding.

Examples of Cross Site Scripting vulnerabilities can be obtained from the OWASP website.
http://www.owasp.org/index.php/Cross_Site_Scripting

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3590 Application is vulnerable to buffer overflows**	**STIG Section**	3.10.6 Buffer Overflow Vulnerabilities
Finding Category	CAT I			
Vulnerability Key	V0006165		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for the test plans for the application. Examine the test plan to determine testing was performed for buffer overflows. If the test plans indicate that buffer overflow was performed, only a small sampling of testing is required. If the test plans do not exist or do not indicate that buffer overflow was performed more detailed testing is required. Testing should include logging on the application and entering data larger than the application is expecting

This testing should include the following:

• Very large number including large precision decimal numbers in numeric data fields
• Both negative and positive numbers should be included in numeric data fields
• Large amounts of data (at least 1024K) into the text fields
• If the application is a web-based application that utilizes query strings, testing should include passing at least 500 characters of data into the query string parameter.

1) If the application gives an error that indicates that the error condition is not being checked, this is a finding.

Ask the application representative for code review results from the entire application. This can be provided in the form of results from an automated code review tool. If an automated tool is used and checks for buffer overflows this is not a finding.

If the results are provided from a manual code review, the application representative will need to demonstrate how buffer overflow vulnerabilities and functions vulnerable to buffer overflows are identified during code reviews.

2) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify buffer overflow vulnerabilities, this is a finding.

Finding Results

Comments:					
Finding	CAT I ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3600 Vulnerable to canonical representation attacks**	**STIG Section**	3.11 Canonical Representation
Finding Category	CAT II			
Vulnerability Key	V0016812		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided in the form of results from an automated code review tool.

If the results are provided from a manual code review the application representative will need to demonstrate how canonical representation vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify canonical representation vulnerabilities, this is a finding.

Examples of Canonical Representation vulnerabilities can be obtained from the OWASP website. http://www.owasp.org/index.php/Canonicalization,_locale_and_Unicode

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3610 Hidden fields used to control access privileges**	**STIG Section**	3.12 Hidden Fields in Web Pages
Finding Category	CAT I-II			
Vulnerability Key	V0016813		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review, the application representative will need to demonstrate how hidden field vulnerabilities are identified during code reviews.

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify hidden field vulnerabilities, this is a CAT I finding.

2) If the code review results are provided and hidden field vulnerabilities exist for user authentication this is a CAT I finding.

3) If the code review results are provided and hidden field vulnerabilities exist allowing users to access unauthorized information, this is a CAT II finding.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3620 Application discloses unnecessary information**	**STIG Section**	3.13 Application Information Disclosure
Finding Category	CAT II			
Vulnerability Key	V0016814		**IA Controls**	ECCD-1

Check

Instruction:
Ask the application representative to demonstrate the application does not disclose application or other unnecessary information to unauthorized users.

Ask the application representative to login as a non-privileged user and review all screens of the application to identify any potential data that should not be disclosed to the user.

1) If the application displays any data that should not be disclosed, this is a finding.

Mitigate information disclosure vulnerabilities, by using HTTP-only cookies to prevent potential cross-site scripting vulnerabilities. Examine the any cookies used while application is being executed. Verify then HttpOnly flag has been set for all cookies

2) If the the HttpOnly flag has not been set for all cookies, this is a finding.

HttpOnly cookies are explained further at the Microsoft website.
http://msdn.microsoft.com/en-us/library/ms533046.aspx

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3630 Application vulnerable to race conditions**	**STIG Section**	3.14 Race Conditions
Finding Category	CAT II			
Vulnerability Key	V0016815		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool.

If the results are provided from a manual code review, the application representative will need to demonstrate how the following vulnerabilities are identified during code reviews.

• Race conditions
• Using global variables when local variables could be used
• Multi-threaded application uses thread safe functions
• Global resources are locked before being accessed by the application

1) If the results are not provided or the application representative can not demonstrate how manual code reviews are performed to identify these vulnerabilities, this is a finding.

Examples of Race Conditions vulnerabilities can be obtained from the OWASP website.
https://www.owasp.org/index.php/Reviewing_Code_for_Race_Conditions

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3640 No logs for data access and changes**	**STIG Section**	3.15 Auditing
Finding Category	CAT II			
Vulnerability Key	V0016816		**IA Controls**	ECCD-2

Check

Instruction:
Ask the application representative to login as an unprivileged user and demonstrate the application creates transaction logs for access and changes to the data. Verify transaction logs exist that record access and changes to the data. This check is in addition to the ECAR auditing requirements.

1) If the application representative cannot demonstrate the above, this is a finding

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3650 No warning when logs are near full**	**STIG Section**	3.15.1 Audit Notifications
Finding Category	CAT III			
Vulnerability Key	V0006139		**IA Controls**	ECAT-2

Check

Instruction:
Examine the application documentation and ask the application representative what automated mechanism is in place to ensure the administrator is notified when the application logs are near capacity.

1) If an automated mechanism is not in place to warn the administrator, this is a finding.

If the application representative or the documentation indicates a mechanism is in place, examine the configuration of the mechanism to ensure the process is present and executing.

2) If an automated mechanism is not executing, this is a finding.

Note: This may be automated by the operating system of the application servers.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3660 Last Login information not displayed**	**STIG Section**	3.15.1 Audit Notifications
Finding Category	CAT III			
Vulnerability Key	V0016817		**IA Controls**	ECLO-2

Check

Instruction:
If the application uses password authentication, try to login to the system using an incorrect password.
Restart the application and login again using the correct password. After a successful login to the application logout of the application and note the date and times for the last success and unsuccessful logons. Again login to the application and determine whether the application correct displays the following information:

Unsuccessful Logon
Date
Time
IP Address

Successful Logon
Date
Time
IP Address

If the application does not correctly display the last unsuccessful and successful logon information, this is a finding

For CAC and NSA approved token authentication logons, remove the CAC or mistype the pin to simulate an unsuccessful login.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3670 No notification of time of last change of data**	**STIG Section**	3.15.1 Audit Notifications
Finding Category	CAT II			
Vulnerability Key	V0016818		**IA Controls**	ECCD-2

Check

Instruction:
Ask the application representative to demonstrate the application provides the users of time and date of the last change in data content. This may be demonstrated in application logs, audit logs, or database tables and logs.

1) If the application representative cannot demonstrate the above, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3680 The application does not adequately log events**	**STIG Section**	3.15.2 Access for Need-to-Know 3.16.1.1 Category 1A Mobile Code 3.16.1.1 Category 1A Mobile Code 3.16.2.1 Category 2 Mobile Code in Constrained Environment 3.16.4 Emerging Mobile Code
Finding Category	CAT II			
Vulnerability Key	V0006138		**IA Controls**	ECAR-1 ECAR-2 ECAR-3

Check

Instruction:
If one or more of the following events are not found in the log, do one of the following:

• Check the configuration of the audit facility to see if the configured policy calls for logging such an event.
• Perform a transaction that would generate such an event and verify that it appears in the audit log.
• Review source code to identify appropriate event handling routines.

For each of these events, the items required to be included in the log files vary depending upon classification or MAC level.

For Classified or MAC I systems the following items are required to be in the audit log:

• UserID of user or process ID of process causing the event
• Success or failure of attempt to access a security file
• Date and time of the event
• Type of event
• Success or failure of event
• Severity of event violation
• Success or failure of login attempt
• Denial of access resulting from excessive number of login attempts
• Blocking or blacklisting a UserID, terminal, or access port, and the reason for the action
• Data required to audit the possible use of covert channel mechanisms
• Privileged activities and other system level access
• Starting and ending time for access to the application

• Activities that might modify, bypass, or negate safeguards controlled by the system
• Security-relevant actions associated with periods processing, or the changing of security labels or categories of information
• For I&A events: origin of request (e.g., originating host's IP address)
• For write or delete events: name of data object written or deleted.

For Sensitive, private or Mac II systems the following items are required to be in the audit log:

• UserID of user or process ID of process causing the event
• Success or failure of attempt to access security file
• Date/time of event
• Type of event
• Success or failure of event
• Seriousness of event violation
• Success or failure of login attempt
• Denial of access resulting from excessive number of login attempts
• Blocking or blacklisting of UserID, terminal, or access port, and reason for the action
• Activities that might modify, bypass, or negate security safeguards controlled by the application,
• For I&A events: origin of request (e.g., originating host's IP address)
For write or delete events: name of data object written or deleted

For Public or Mac III the following items are required to be in the audit log:

• UserID of user or process ID of process causing the event
• Success or failure of attempt to access security file
• Date/time of event
• Type of event
• Success or failure of event
• Seriousness of event violation
• For I&A events: origin of request (e.g., originating host's IP address)
• For write or delete events: name of data object written or deleted

1) If all the required events and associated details are not included in the log or there is not logging mechanism, this is a finding.

The mechanism that performs auditing may be a combination of the operating system, web server, database, application, etc.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production & Production	**APP3690 Application audit logs have incorrect permissions**	**STIG Section**	3.15.5 Audit Trail Protection 3.16.2.1 Category 2 Mobile Code in Constrained Environment
Finding Category	CAT II			
Vulnerability Key	V0006140		**IA Controls**	ECTP-1

Check

Instruction:
Locate the application audit log location. Examine the properties of the log files.

For a Windows system, the NTFS file permissions should be System – Full control, Administrators and Application Administrators - Read, and Auditors - Full Control.

1) If the log files have permissions more permissive than what is listed, this is a finding.

For UNIX systems, use the ls –la (or equivalent) command to check the permissions of the audit log files.

2) If excessive permissions exist, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3700 Unsigned Cat 1A or 2 mobile code in use**	**STIG Section**	3.16.1.1 Category 1A Mobile Code 3.16.4 Emerging Mobile Code 3.16.4 Emerging Mobile Code 3.16.5 New Procurement and Development Efforts
Finding Category	CAT II			
Vulnerability Key	V0006159		**IA Controls**	DCMC-1

Check

Instruction:
Interview application representative and examine application documentation to determine if Category 1A or 2 mobile code is used.

The URL of the application must be added to the Trusted Sites zone. This is accomplished via the Tools, Internet Options, and Security Tab. Select the trusted sites zone.
Click the sites button. Enter the URL into the text box below the Add this site to this zone message. Click Add. Click OK.

Note: This requires administrator privileges to add URL to sites on a STIG compliant workstation.

Next test the application. This testing should include functional testing from all major components of the application. If mobile code is in use, the browser will prompt to download the control. At the download prompt, the browser will indicate that code has been digitally signed.

1) If the code has not been signed or the application warns that a control cannot be invoked due to security settings, this is a finding.

2) If the code has not been signed with a DoD approved PKI certificate, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3710 Mobile code executed without verifying signature**	**STIG Section**	3.16.1.1 Category 1A Mobile Code 3.16.2.1 Category 2 Mobile Code in Constrained Environment
Finding Category	CAT II			
Vulnerability Key	V0006161		**IA Controls**	DCMC-1

Check

Instruction:
Ask the application representative and examine the documentation to determine if the application accepts file inputs via email, ftp, file uploads or other automated mechanisms.

If the application does not accept file uploads this check is not applicable.

If the application accepts inputs, investigate the process that is used to process the request. If the process could contain mobile code, a mechanism must exist to ensure that before mobile code is executed, its signature must be validated.

The following examples are intended to show determination of the finding:

Non-finding example: The application allows upload of data. The data file is parsed looking for specific pieces of information in an expected format. An application program in accordance with established business rules then processes the data. This situation would be not a finding.

Finding example: The application allows upload of data. The data file is sent directly to an execution module for processing. This example could include a .doc file that is sent directly to MS Word for processing. Using this example, if there was a process in place to ensure that the document was digitally signed and validated to be a DOD approved PKI certificate before processing, this would be not a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3720 Unsigned unconstrained mobile code used**	**STIG Section**	3.16.2.1 Category 2 Mobile Code in Constrained Environment
Finding Category	CAT II			
Vulnerability Key	V0006160		**IA Controls**	DCMC-1

Check

Instruction:
If the application does not contain mobile code, this is not applicable.

If any other mobile code is being transmitted by the application, examine the configuration of the test machine to ensure that no network connections exist. This can be accomplished by typing the netstat command from the command prompt on a Windows client. Ensure that after the mobile code is executed that network connections do not exist.

1) If the application transmits mobile code that attempts to access local operating system resources or establish network connections to servers other than the application server, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3730 Uncategorized mobile code used**	**STIG Section**	3.16.4 Emerging Mobile Code
Finding Category	CAT II			
Vulnerability Key	V0006162		**IA Controls**	DCMC-1

Check

Instruction:
Ask the application representative and examine the documentation to determine if additional mobile code types are being used that have not been defined in the mobile code policy.

By definition, mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

In order to determine if an emerging technology is not covered by the current policy, excerpts of the DoD Mobile Code Policy dated 7 November 2000 are included so the reviewer knows what types of technologies are included, which he or she must know to determine what is outside the scope of the policy.

Items covered by the policy include:

• ActiveX
• Windows Scripting Host when used as mobile code
• Unix Shell Scripts when used as mobile code
• DOS batch scripts when used as mobile code
• Java applets and other Java mobile code
• Visual Basic for Applications (VBA)
• LotusScript
• PerfectScript
• Postscript
• JavaScript (including Jscript and ECMAScript variants)
• VBScript
• Portable Document Format (PDF)
• Shockwave/Flash

Currently the following are not designated as mobile code by the policy:

• XML
• SMIL
• QuickTime
• VRML (exclusive of any associated Java applets or JavaScript scripts)

The following are outside the scope of the DoD mobile code policy:

• Scripts and applets embedded in or linked to web pages and executed in the context of the web server. Examples of this are Java servlets, Java Server pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side LotusScript.
• Local programs and command scripts
• Distributed object-oriented programming systems (e.g. CORBA, DCOM)
• Software patches, updates, including self-extracting updates - software updates that must be invoked explicitly by the user are outside the mobile code policy. Examples of technologies in this area include: Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins and Linux.

If other types of mobile code technologies are present that are not covered by the policy, a written waiver must been granted by the CIO (allowing use of emerging mobile code technology). Also uncategorized mobile code must be submitted for approval.

1) If the application representative is unable to present the written waiver granted by the CIO, this is finding.

2) If application representative provides acceptable written waiver granted by the CIO, this is not a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3740 Code sent in email**	**STIG Section**	3.16.4 Emerging Mobile Code
Finding Category	CAT II			
Vulnerability Key	V0006158		**IA Controls**	DCMC-1

Check

Instruction:
If the application does not send email, this check is not applicable.

If the application sends email, ask for user documentation and test results of email portion of application. Additionally execute the email portion of the application. If possible, configure mail to send to an established email account. If network configurations prevent actual mail delivery, perform the check by examining the mail in the mail queue. Examine documentation and email output.

1) If any email message contains files with the following extensions (.exe, .bat, .vbs, .reg, .jse, .js, .shs, .vbe, .wsc, .sct, .wsf, .wsh), this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP3750 New mobile development not compliant DoDI 5200.40**	**STIG Section**	3.16.5 New Procurement and Development Efforts
Finding Category	CAT II			
Vulnerability Key	V0016819		**IA Controls**	DCMC-1

Check

Instruction:
Interview the designer and determine if new mobile code is in development.

If no new mobile code is in development, this check is not applicable.

1) If new code is being developed determine and a risk assessment has not been performed, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP4010 Access rights to the CM repository not reviewed**	**STIG Section**	4 Software Configuration Management
Finding Category	CAT III			
Vulnerability Key	V0016820		**IA Controls**	ECPC-1 ECPC-2

Check

Instruction:
The configuration management repository access permissions are not reviewed at least every three months.

Ask the application representative when the last time the access privileges were reviewed.

1) If access privileges were not reviewed within the last three months, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP4020 Flaws found during a code review are not tracked**	**STIG Section**	4 Software Configuration Management
Finding Category	CAT III			
Vulnerability Key	V0016821		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to demonstrate that the bug tracking system captures flaws in the code review process.

1) If there is no bug tracking system or the code review flaws are not captured in the bug tracking system, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP4030 The SCM plan does not exist**	**STIG Section**	4.1 Software Configuration Management Plan
Finding Category	CAT II-III			
Vulnerability Key	V0016822		**IA Controls**	DCCS-2

Check

Instruction:
Ask the application representative to review the applications SCM Plan.

The SCM plan should contain the following:
• Description the configuration control and change management process
• Types of objects developed
• Roles and responsibilities of the organization

1) If the SCM plan does not include the above, this is a CAT II finding.

The SCM plan should also contain the following:
• Defines responsibilities
• Actions to be performed
• Tools used in the process
• Techniques and methodologies
• Defines an initial set of baselined software components

2) If the SCM plan does not include the above, this is a CAT III finding.

The SCM plan should identify all objects that are under configuration management control. Ask the application representative to provide access to the configuration management repository and identify the objects shown in the SCM Plan.

3) If the application representative cannot display all types of objects under CM control, this is a CAT III finding.

The SCM plan should identify third party tools and their respective version numbers.

4) If the SCM plan does not identify third party tools, this is a CAT II finding.

The SCM plan should identify mechanisms for controlled access of individuals simultaneously updating the same application component.

5) If the SCM plan does not identify mechanisms for controlled access, this is a CAT III finding.

The SCM plan assures only authorized changes by authorized persons are allowed.

6) If the SCM plan does not assure only authorized changes are made, this is a CAT II finding.

The SCM plan should identify mechanisms to control access and audit changes between different versions of objects subject to configuration control.

7) If the SCM plan does not identify mechanisms to control access and audit changes between different versions of objects subject to configuration control, this is a CAT III finding.

The SCM plan should have procedures for label versions of application components and application builds under configuration management control. Ask the application representative to show you the configuration management repository and identify versions and releases of the application. Ask the application representative to create a build or show how a current release of the application would be recreated.

8) If the application representative cannot display releases and application component versions, this is a CAT II finding.

The configuration management repository should track change requests from beginning to end. Ask the application representative to display a completed or in process change request.

9) If the configuration management repository cannot tracks change requests, this is a CAT III finding.

If the application has just completed its first release there may not be any change requests logged in the configuration management repository. In this case, this finding is not applicable.

The configuration management repository should authorize change requests to the application. Ask the application representative to display an authorized change request and identify who is responsible for authorizing change requests.

10) If the configuration management repository does not track authorized change requests, this is a CAT III finding.

If the application has just completed its first release there may not be any change requests logged in the configuration management repository. In this case, this finding is not applicable.

The configuration management repository should contain security classification labels for code and documentation in the repository. Classification labels are not applicable to unclassified systems.

11) If there are no classification labels of code and documentation in the configuration management repository, this is a CAT III finding.

The configuration management repository should monitor all objects under CM control for auditing.

12) If the configuration management repository does not audit for modifications, this is a CAT II

finding.					
Finding Results					
Comments:					
Finding	CAT II ☐ CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP4040 A Configuration Control Board does not exist**	**STIG Section**	4.2 Configuration Control Board
Finding Category	CAT II-III			
Vulnerability Key	V0016823		**IA Controls**	DCCB-1 ECRC-1

Check

Instruction:
Interview the application representative and determine if a configuration control board exists. Ask about the membership of the Configuration Control Board (CCB) and identify the primary members. Ask if there is a CCB charter documentation.

1) If there is no evidence of CCB, this is a CAT II Finding.

2) If the IAM is not part of the CCB, this is a CAT II Finding.

Interview the application representative and determine how often the configuration control board meets. Ask if there is CCB charter documentation. The CCB charter documentation should indicate how often the CCB meets. If there is no charter documentation, ask when the last time the CCB met and when was last release of the application. CCB's do not have to physically meet and the CCB chair may authorize a release based on phone and/or email conversations.

3) If there is not evidence of a CCB meeting during every release cycle, this a CAT III finding.

Finding Results

Comments:					
Finding	CAT II ☐ CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5010 No tester designated to test for security flaws**	**STIG Section**	5 Testing
Finding Category	CAT III			
Vulnerability Key	V0016824		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative if any testers have been designated to test for security flaws.

1) If no testers have been designated to test for security flaws, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5030 Data files modified outside the application**	**STIG Section**	5 Testing
Finding Category	CAT II			
Vulnerability Key	V0006147		**IA Controls**	ECRC-1

Check

Instruction:
On each computer in the application infrastructure, search the file system for files created or modified in the past week. If the response is too voluminous (more than 200 files), find the files created or modified in the past day. Search through the list for files and identify those that appear to be outside the scope of the application. Ask the application representative how the file relates to the application.

1) If the creation or modification of the file does not have a clear purpose this is a finding.

The finding details should include the full path of the file.

The method described above may not catch all instances of out-of-scope modifications because the file(s) may have been modified prior to the threshold date or because the files may be resident on a system other than those examined. If additional information is obtained later in the review regarding improper modification of files, revisit this check. This information may be uncovered when the reviewer obtains more detailed knowledge of how the application works during subsequent checks.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5040 Changes to the application are not assessed for IA**	**STIG Section**	5 Testing
Finding Category	CAT II			
Vulnerability Key	V0016825		**IA Controls**	DCII-1

Check

Instruction:
Interview the application representative and determine if changes to the application are assessed for IA impact prior to implementation. Review the CCB process documentation to ensure potential changes to the application are evaluated to determine impact. An informal group may be tasked with impact assessment of upcoming version changes.

1) If impact analysis is not performed, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5050 Tests plans not executed prior to release or patch**	**STIG Section**	5.1 Test Plans and Procedures
Finding Category	CAT II			
Vulnerability Key	V0016826		**IA Controls**	DCCS-2

Check

Instruction:
Ask the application representative to provide tests plans, procedures and results to ensure they are updated for each application release or updates to system patches.

1) If test plans, procedures and results do not exist or are not updated for each application release or updates to system patches, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5060 System in insecure state during startup & shutdown**	**STIG Section**	5.1 Test Plans and Procedures
Finding Category	CAT II			
Vulnerability Key	V0016827		**IA Controls**	DCCS-2

Check

Instruction:
Ask the application representative to provide tests plans, procedures and results to ensure system initialization, shutdown, and aborts keep the system in a secure state.

1) If test plans, procedures and results do not exist or at least executed annually, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5070 Application has no code coverage statistics**	**STIG Section**	5.3 Code Coverage
Finding Category	CAT III			
Vulnerability Key	V0016828		**IA Controls**	DCSQ-1

Check
Instruction: Ask the application representative to provide code coverage statistics maintained for the application. 1) If these code coverage statistics do not exist, this is a finding.

Finding Results					
Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5080 Code reviews not performed prior to release**	**STIG Section**	5.4 Code Reviews
Finding Category	CAT II			
Vulnerability Key	V0016829		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to provide evidence of code reviews.

1) If code is not being reviewed or only some application components are being reviewed, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5090 Flaws found during a code review are not tracked**	**STIG Section**	5.4 Code Reviews
Finding Category	CAT II			
Vulnerability Key	V0016830		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to demonstrate that the configuration management repository captures flaws in the code review process. The configuration management repository may consist of a separate application for capturing code defects.

1) If there is no configuration management repository or the code review flaws are not captured in the configuration management repository, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5100 Fuzz testing is not performed**	**STIG Section**	5.2 Fuzz Testing
Finding Category	CAT III			
Vulnerability Key	V0016831		**IA Controls**	DCSQ-1

Check

Instruction:
Fuzz testing or fuzzing is a software testing technique that provides unexpected or random data called fuzz to the inputs of an application to discover vulnerabilites.

Automated fuzz testing tools or fuzzers indentify vulnerabilities and indicate potential causes. This information is often used by malicious hackers to help in deterimining methods to attack a target system.

Fuzzers can sometimes help identify buffer overflows, cross-site scripting, denial of service attacks, format bugs and SQL injection.

The following website provides an overview of fuzz testing and examples:
http://www.owasp.org/index.php/Fuzzing

Ask the application representative to provide tests procedures and results to ensure they are updated to include fuzz testing procedures.

1) If these test procedures and results do not include fuzz testing, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Pre-Production	**APP5110 Security flaws not addressed in project plan**	**STIG Section**	5.2 Fuzz Testing
Finding Category	CAT II			
Vulnerability Key	V0016832		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to demonstrate how security flaws are integrated into the project plan.

1) If security flaws are not addressed in the project plan or there is no process to introduce security flaws into the project plan this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6010 Critical application hosted on a multi-use server**	**STIG Section**	6.1.3 Application Configuration Guide
Finding Category	CAT II			
Vulnerability Key	V0016833		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to review the servers where the application is deployed. Also ask what other applications are deployed on those servers.

1) If a mission critical (MAC I) application is deployed on the same server as other applications, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6020 COTS products not configured to best practices**	**STIG Section**	6.2 Third Party Software
Finding Category	CAT II			
Vulnerability Key	V0016834		**IA Controls**	DCCS-1

Check

Instruction:
If a DoD STIG or NSA guide is not available, application and application components will be configured by the following in descending order as available: (1) commercially accepted practices, (2) independent testing results, or (3) vendor literature.

1) If the application and application components do not have DoD STIG or NSA guidiance available and not configured by (1) commercially accepted practices, (2) independent testing results, or (3) vendor literature, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6030 Unnecessary services or software not removed**	**STIG Section**	6.5 Unnecessary Services
Finding Category	CAT II			
Vulnerability Key	V0006151		**IA Controls**	DCSD-1

Check

Instruction:
Examine the configuration of the servers. Determine what software is installed on the servers. Determine which services are needed for the application by examining the SSAA documentation and interviewing the application representative. For example if a two web servers (IIS and Apache) are installed and only one is being used.

1) If there are services or software present not needed for the application, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6040 Administrator has not registered to updates**	**STIG Section**	6.6.1 Vulnerability Management
Finding Category	CAT II			
Vulnerability Key	V0016835		**IA Controls**	DCCT-1

Check

Instruction:
Review the components of the application. Deployment personnel should be registered to receive updates to all components of the application. (e.g. Web Server, Application Servers, Database Servers) Also if update notifications are provided to any custom developed software, deployment personnel should also register for these updates. Customed developed software could include updates for the individual application components requiring only one locations to register to receive updates and security patches. Ask the application representative to demonstrate deployment personnel are registered to receive notifications for updates to all the application components including and custom developed software.

*Note: Subscribing to IAVA distribution, does not satisfy this requirement.

1) If the application provides automated alerts for update notifications, and no deployment personnel are registered to receive the alerts, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6050 Current patches and configurations not installed**	**STIG Section**	6.6.1 Vulnerability Management
Finding Category	CAT II			
Vulnerability Key	V0016836		**IA Controls**	DCCT-1

Check

Instruction:
Ask the application representative to review the Configuration Management Plan. Ensure procedures exist which address the testing and implementation process for all patches, upgrades and application deployments.

1) If procedures do not exist or are deficient, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6060 App not decommissioned when maintenance is expired**	**STIG Section**	6.6.2 Maintenance Availability
Finding Category	CAT III			
Vulnerability Key	V0016837		**IA Controls**	DCSD-1

Check

Instruction:
Interview the application representative and determine if all the application components are under maintenance. The entire application maybe covered under one maintenance agreement. The application should be decomissioned if maintenance is no longer being provided by the vendor or by the development staff of a custom developed application.

1) If the application or any of the application components are not being maintained, this is a finding.

Finding Results

Comments:					
Finding	CAT III				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6070 No procedures exist to decommission application**	**STIG Section**	6.6.2 Maintenance Availability
Finding Category	CAT III			
Vulnerability Key	V0016838		**IA Controls**	DCSD-1

Check

Instruction:
Interview the application representative to determine if provisions are in place to notify users when an application is decommissioned.

1) If provisions are not in place to notify users when an application is decommissioned, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6080 Protections against DoS attacks not implemented**	**STIG Section**	6.8 Denial of Service
Finding Category	CAT II			
Vulnerability Key	V0016839		**IA Controls**	DCSQ-1

Check

Instruction:
Ask the application representative to review the threat model for DOS attacks. Verify the mitigations for DOS attacks are implemented from the threat model.

1) If the mitigations from the threat model for DOS attacks are not implemented this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6090 No system alerts in a low resource condition**	**STIG Section**	6.8 Denial of Service
Finding Category	CAT III			
Vulnerability Key	V0016840		**IA Controls**	ECAT-2

Check

Instruction:
Examine the system to determine if an automated, continuous on-line monitoring and audit trail creation capability is present with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.

1) If this monitoring capability does not exist, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6100 Sensitive data not purged from production export**	**STIG Section**	6.1 Database Exports
Finding Category	CAT II			
Vulnerability Key	V0006174		**IA Controls**	ECAN-1

Check

Instruction:
Ask if any database exports from this database are imported to development databases.

If no database exports exist, this check is not applicable

If there are such exports, ask if policy and procedures are in place to require the modification of the production database account passwords after import into the development database.

1) If there are no policy and procedures in place to modify production database account passwords, this is a finding.

If there are such exports, ask if the production database includes sensitive data identified by the data owner as sensitive such as financial, personnel, personal, HIPAA, Privacy Act, or classified data is included.

2) If any database exports include sensitive data and it is not modified or removed prior to or after import to the development database, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6110 Audit trail not periodically reviewed**	**STIG Section**	6.12.1 Audit Trail Monitoring
Finding Category	CAT III			
Vulnerability Key	V0016841		**IA Controls**	ECCD-2

Check

Instruction:
Interview application representative and ask for the system documentation that states how often audit logs are reviewed. Also determine when the audit logs were last reviewed.

1) If the application representative can not provide system documentation identifying how often the auditing logs are reviewed or has not audited within the last time period stated in the system documentation, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6120 IAO has no process to report IA violations**	**STIG Section**	6.12.1 Audit Trail Monitoring
Finding Category	CAT II			
Vulnerability Key	V0016842		**IA Controls**	ECAT-2

Check

Instruction:
Interview the application representative and review the SOPs to ensure that violations of IA policies are analyzed and reported.

1) If there is no policy reporting IA violations this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6130 No automated audit trail monitoring**	**STIG Section**	6.12.1 Audit Trail Monitoring
Finding Category	CAT III			
Vulnerability Key	V0016843		**IA Controls**	ECAT-2

Check

Instruction:
Interview the application representative and determine if any logs are being automatically monitored and if alerts are sent out on any activities.

1) If there are no automated alerts, this is a finding

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6140 Log files are not retained for at least one year**	**STIG Section**	6.12.2 Audit Log Retention
Finding Category	CAT II			
Vulnerability Key	V0006173		**IA Controls**	ECRR-1

Check

Instruction:
Ensure a process is in place to retain application audit log files for one year and five years for SAMI data.

1) If audit logs have not been retained for one year or five years for SAMI data, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6160 Disaster recovery plan does not exist**	**STIG Section**	6.13 Recovery and Contingency Planning
Finding Category	CAT II			
Vulnerability Key	V0006171		**IA Controls**	COTR-1

Check

Instruction:
Ensure that a disaster recovery plan is in place for the application. If the application is part of the site's disaster recovery plan, ensure that the plan contains detailed instructions pertaining to the application. Ensure that recovery procedures that indicate the steps needed for secure recovery.

1) If a disaster recovery plan does not exist or the application is not part of the site's disaster recovery plan this is a finding.

Verify that the recovery procedures include any special considerations for trusted recovery.

2) If any special considerations for trusted recovery are not documented, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6170 Application backups not in a fire rated container**	**STIG Section**	6.13 Recovery and Contingency Planning
Finding Category	CAT II			
Vulnerability Key	V0016844		**IA Controls**	COSW-1

Check

Instruction:
Verify that a licensed copy of the operating system software and other critical software is in a fire rated container or stored separately (offsite) from the operational software.

1) If operating system software and other critical software is not in a fire rated container or stored offsite, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6180 Backup and restoration device not protected**	**STIG Section**	6.13 Recovery and Contingency Planning
Finding Category	CAT II			
Vulnerability Key	V0016845		**IA Controls**	COBR-1

Check

Instruction:
Validate that backup and recovery procedures incorporate protection of the backup and restoration assets.

Verify assets housing the backup data (e.g., SANS, Tapes, backup directories, software) and the assets used for restoration (e.g., equipment and system software) are included in the backup and recovery procedures.

1) If backup and restoration devices are not included in the recovery procedures, this is a finding

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6190 Backups or backup procedures are incomplete**	**STIG Section**	6.13 Recovery and Contingency Planning
Finding Category	CAT II			
Vulnerability Key	V0006172		**IA Controls**	CODB-3 CODP-3 IAAC-1

Check

Instruction:
Check the following based on the MAC level of the application.

For MAC 3 applications
Validate backups procedures exist and are performed at least weekly.

A sampling of system backups should be checked to ensure compliance with the control.

For MAC 2 applications
Validate backups procedures exist and are performed at least daily.

Validate recovery media is stored off-site at a location and ensure the data is protected in accordance with its mission assurance category and confidentiality level. This validation can be performed by examining an SLA or MOU/MOA that states the protection levels of the data and how it should be stored.

A sampling of system backups should be checked to ensure compliance with the control.
Verify that the organization tests backup information too ensure media reliability and information integrity.

Verify that the organization selectively uses backup information in the restoration of information system functions as part of annual contingency plan testing.

For MAC 1 applications
Validate that the procedures have been defined for system redundancy and they are properly implemented and are executing the procedures.

Verify that the redundant system is properly separated from the primary system (i.e., located in a different building or in a different city). This validation should be performed by examining the secondary system and ensuring its operation. Examine the SLA or MOU/MOA to ensure redundant capability is addressed. Finding details should indicate the type of validation performed. Examine the mirror capability testing procedures and results to insure the capability is properly tested at 6 month minimum intervals.

1) If any of the requirements above for the MAC level of the application are not met this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6200 Disaster plan does not exist or is incomplete**	**STIG Section**	6.13 Recovery and Contingency Planning
Finding Category	CAT II			
Vulnerability Key	V0016846		**IA Controls**	CODP-3

Check

Instruction:
All applications should document Disaster recovery procedures to include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.

Ask the application representative to review these plans.

For MAC 1 applications verify the disaster plan exists and provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity.

For MAC 2 applications verify the disaster plan exists and provides for the resumption of mission or business essential functions within 24 hours activation.

For MAC 3 applications verify the disaster plan exists and provides for the partial resumption of mission or business essential functions within 5 days of activation.

1) If the disaster plan does not exist or does not meet the MAC level requirements, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6210 No account management process in place**	**STIG Section**	6.14 Account Management
Finding Category	CAT II			
Vulnerability Key	V0016847		**IA Controls**	IAAC-1

Check

Instruction:
Interview the application representative to verify that a documented process exists for user and system account creation, termination, and expiration.

Obtain a list of recently departed personnel and verify that their accounts were removed or deactivated on all systems in a timely manner (e.g., less than two days).

1) If a documented account management process does not exist or unauthorized users have active accounts, this is a finding

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6220 Generated passwords do not comply with policy**	**STIG Section**	6.14 Account Management
Finding Category	CAT II			
Vulnerability Key	V0016848		**IA Controls**	IAIA-1 IAIA-2

Check

Instruction:
Ask the application representative to examine the organization's password policy.

1) If non-human/service accounts are used and are not included in the password policy, this is a finding

2) If non-human/service accounts policy does not require these accounts to change yearly or when someone with access to the password leaves the duty assignment, this is a finding

The configuration interface may not reveal information related to all the required elements. If this is the case, attempt to violate each element to determine if the policy is enforced. For example, attempt to change a password to one that does not meet the requirements.

3) If there are any shortcomings in the password policy or the configured behavior of any user account, this is a finding.

The finding details should note which user accounts are impacted, which of the password parameters are deficient, the current values of these parameters, and the relevant required values.

Also ask the application representative to generate two user account passwords.

4) If there is a recognizable pattern in password generation, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6230 Access granted by group authenticator**	**STIG Section**	6.14 Account Management
Finding Category	CAT II			
Vulnerability Key	V0016849		**IA Controls**	IAGA-1

Check
Instruction: Ask the application representative if a group of users share login information to the system. 1) If an account that belongs to a group that can login to the system, this is a finding. 2) If there is a login shared by more than one user, this is a finding.

Finding Results					
Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6240 Inactive userids are not disabled**	**STIG Section**	6.14 Account Management
Finding Category	CAT III			
Vulnerability Key	V0006132		**IA Controls**	IAIA-1

Check

Instruction:
If the user accounts used in the application are only operating system or database accounts this check is not applicable.

Identify all users that have not authenticated in the past 90 days.

1) If any of these are enabled, this is a finding.

Finding Results

Comments:					
Finding	CAT III ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6250 Unnecessary built-in userids are not disabled**	**STIG Section**	6.14 Account Management
Finding Category	CAT II			
Vulnerability Key	V0006133		**IA Controls**	IAIA-1

Check

Instruction:
If the user accounts used in the application are only operating system or database accounts this check is Not Applicable.

Built-in accounts are those that are added as part of the installation of the application software. These accounts exist for many common commercial off-the-shelf (COTS) or open source components of enterprise applications (e.g., OS, web browser or database software). If SRRs are performed for these components, this is not applicable because the other SRRs will capture the relevant information and findings. If not, then read the installation documentation to identify the built-in accounts. Also peruse the account list for obvious examples (e.g., accounts with vendor names such as Oracle or Tivoli). Verify that these accounts have been removed or disabled. If enabled built-in accounts are present, ask the application representative the reason for their existence.

1) If these accounts are not necessary to run the application, this is a finding.

2) If any of these accounts are privileged, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6260 Userids have default passwords**	**STIG Section**	6.14 Account Management
Finding Category	CAT I-II			
Vulnerability Key	V0006134		**IA Controls**	IAIA-1

Check

Instruction:
Run a password-cracking tool, if available, on a copy of each account database (there may be more than one in the application infrastructure).

1) If the password-cracking tool is able to crack the password of a privileged user, this is CAT I finding.

2) If the password-cracking tool is able to crack the password of a non-privileged user, this is CAT II finding.

Manually attempt to authenticate with the published default password for that account, if such a default password exists.

3) If any privileged built-in account uses a default password – no matter how complex – this is a CAT I finding.

4) If a non-privileged account has a default password, this is a CAT II finding.

Finding Results

Comments:					
Finding	CAT I ☐ CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

Environment	Production	**APP6270 DMZ not present between DoD and public networks**	**STIG Section**	6.15 Deployment Infrastructure
Finding Category	CAT II			
Vulnerability Key	V0016850		**IA Controls**	EBPW-1

Check

Instruction:
Interview the application representative and determine if the application is publicly accessible.

1) If the application is publicly accessible and traffic is not being routed through a DMZ, this is a finding.

Finding Results

Comments:					
Finding	CAT II ☐				
Not a Finding		**Not Reviewed**		**Not Applicable**	

APPENDIX A: CHANGE LOG

Version	Changes				
2.0 Release 1.1	Original Release				
2.0 Release 1.2	STIG ID	Severity	Short Description	Condition	Check
	APP2010		Modified		Modified
	APP2020				Modified
	APP2040		Modified		Modified
	APP2070		Modified		
	APP2080		Modified		
	APP2100		Modified		
	APP2120				Modified
	APP2150				Modified
	APP2160				Modified
	APP3020				Modified
	APP3050				Modified
	APP3060		Modified		
	APP3080				Modified
	APP3110				Modified
	APP3130				Modified
	APP3140				Modified
	APP3150				Modified
	APP3170				Modified
	APP3220				Modified
	APP3280				Modified
	APP3290		Modified		Modified
	APP3310				Modified
	APP3320		Modified		
	APP3350	Modified			Modified
	APP3370				Modified
	APP3400				Modified
	APP3410		Modified		Modified
	APP3415		Modified		
	APP3420				Modified
	APP3430				Modified
	APP3450				Modified
	APP3460				Modified
	APP3470				Modified
	APP3510				Modified
	APP3520		Modified		Modified
	APP3640				Modified
	APP3670				Modified
	APP3740		Modified		
	APP3750		Modified		
	APP4010				Modified
	APP4030				Modified

Version	Changes				
	APP5010				Modified
	APP5040		Modified		
	APP6020				Modified
	APP6060		Modified		Modified
	APP6110				Modified
	APP6120		Modified		
	APP6140				Modified
	APP6200				Modified
	APP6210				Modified
	APP6230				Modified
	APP6260		Modified		
2.0 Release 1.3	STIG ID	Severity	Short Description	Condition	Check
	APP2010			Modified	
	APP2040			Modified	
	APP2060				Modified
	APP2070				Modified
	APP2130			Modified	
	APP2140				Modified
	APP2150				Modified
	APP2160				Modified
	APP3060				Modified
	APP3070		Modified	Modified	Modified
	APP3100				Modified
	APP3130				Modified
	APP3140				Modified
	APP3150	Modified			Modified
	APP3180				Modified
	APP3240			Modified	
	APP3250			Modified	
	APP3270				Modified
	APP3300			Modified	
	APP3310			Modified	Modified
	APP3350			Modified	
	APP3360			Modified	
	APP3390			Modified	
	APP6010				Modified
2.0 Release 1.4	STIG ID	Severity	Short Description	Condition	Check
	APP2040				Modified
	APP3050				Modified
	APP3220				Modified
	APP3430				Modified
	APP3620				Modified
	APP4030				Modified
	APP6010				Modified
	APP6040				Modified

Version	Changes				
2.0 Release 1.5	STIG ID	Severity	Short Description	Condition	Check
	APP2160				Modified
	APP3510				Modified
	APP3540				Modified
	APP5050				Modified
	APP5060				Modified
	APP5100				Modified

APPENDIX B: LIST OF ACRONYMS

Acronym	Term
ACL	Access Control List
CAC	Common Access Card
CFML	ColdFusion Markup Language
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
COBRA	Common Brokerage Architecture
COTS	Commercial Off-the-Shelf
DCOM	Distributed Common Object Model
DDL	Data Definition Language
DISA	Defense information Systems Agency
DOD	Department of Defense
DOS	Disk Operating System
FOUO	For Official Use Only
FSO	Field Security Operations
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAO	Information Assurance Officer (formerly Information Systems Security Officer)
IE	Internet Explorer
IP	Internet Protocol

Acronym	Term
MAC	Mission Assurance Category
NFS	Network File System
NIAP	National Information Assurance Partnership
NTFS	New Technology (NT) File System
OS	Operating System
PHP	Personal Home Page Construction Kit
PDI	Potential Discrepancy Item
PK	Public Key
PKI	Public Key Infrastructure
SMIL	Synchronized Multimedia Integration Language
SQL	Structured Query Language
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
SSI	Server Side Include
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
UID	User Identification
URL	Universal Resource Locator
VMS	Vulnerability Management System
VRML	Virtual Reality Modeling Language

Acronym	Term
XML	Extensible Markup Language

APPENDIX C: VMS 6.0 Instructions

C.1 : System Administrator

The following procedures are to be used by a system administrator to create or update an asset in VMS 6.0, to add an Application Security target to the asset and to update the status of vulnerabilities for the asset.

1. Log into VMS 6.0.
2. Select *Asset Finding Maint.* from the left hand menu.
3. Select *Assets/Findings* from the left hand menu.
4. Expand the *Location* branch of the *Navigation*
5. If the asset you wish to update has already been registered with VMS locate and select it in the *Navigation* tree view control in the right hand panel then proceed to step 8.
6. To create a new asset for the application review expand the appropriate location, then expand the Non-Computing branch of the tree and press the *Create Non-Computing Asset* button.
7. Enter the Asset Identification information on the *General, Systems/Enclaves,* and *Additional Details* pages.
8. Press the *Save Asset* button.
9. Select the *Asset Posture* tab.
10. Expand the *Non-Computing* and then the *Applications* branch of the tree in the *Available* panel of the *Asset Posture* tab.
11. Select the appropriate target from this branch of the tree using the checkbox adjacent to the target name. Your choices will be:
    - *Applications - Pre-production*
    - *Applications – Production*
    - *Applications – Additional Vulnerabilities*
12. Press the >> button to add the selected asset to the target.
13. Press the *Save Asset* button.
14. The asset has now been registered in VMS and has the appropriate targets added to it. Using the *Navigation* tree view control you may select a Vulnerability and update the *Status*, *Details*, *Comments*, *Programs*, or *POA&M* information. After updating any information press the *Save* button before proceeding to the next Vulnerability.

C.2: Reviewer

The following procedures are to be used by a reviewer to create or update an asset in VMS 6.0, to add an Application Security target to the asset and to update the status of vulnerabilities for the asset.

1. Log into VMS 6.0.
2. Select *Asset Finding Maint.* from the left hand menu.
3. Select *Assets/Findings* from the left hand menu.
4. Expand the *Visit* branch of the *Navigation* tree view.
5. If the asset you wish to update has already been registered with VMS locate and select it in the *Navigation* tree view control in the right hand panel then proceed to step 9.

6. To create a new asset for the application review expand the appropriate location, then expand the Non-Computing branch of the tree and press the *Create Non-Computing Asset* button.
7. Enter the Asset Identification information on the *General, Systems/Enclaves,* and *Additional Details* pages.
8. Press the *Save Asset* button, the asset will now appear under the *Not Selected for Review* tree branch.
9. Select the *Asset Posture* tab.
10. Expand the *Non-Computing* and then the *Applications* branch of the tree in the *Available* panel of the *Asset Posture* tab.
15. Select the appropriate target from this branch of the tree using the checkbox adjacent to the target name. Your choices will be:
    - *Applications - Pre-production*
    - *Applications – Production*
    - *Applications – Additional Vulnerabilities*
11. Press the >> button to add the selected asset to the target.
12. Press the *Save Asset* button.
13. The asset has now been registered in VMS and has the appropriate targets added to it. Using the *Navigation* tree view control you may select a Vulnerability and update the *Status*, *Details*, *Comments*, *Programs*, or *POA&M* information. After updating any information press the *Save* button before proceeding to the next Vulnerability.

APPENDIX D: Additional Resource Information

Additional information may be found from the following sources.

List of Common Vulnerabilities and Exposures	http://cve.mitre.org/
NIST site for FIPS Compliance	http://csrc.nist.gov/cryptval/
NIAP and CCEVS information	http://www.nsa.gov/ia/industry/niap.cfm

Table D-1. Additional Resource Information

APPENDIX E: Cross Reference to Application Security and Development STIG

The previous checklist was derived from the Draft Recommended Standard Application Security Requirements. The new checklist is based on the Application Security and Development STIG. A cross reference between the Draft Recommended Standard Application Security Requirements and the Application Security and Development STIG is provided below.

VMS Key	Original Checklist	New Checklist	Short Name:
V0006127	APP0120	APP3280	The application is not PK-enabled.
V0006128	APP0125	APP3290	The application utilizes a PKI other than DOD PKI.
V0006129	APP0130	APP3305	The application honors invalid certificates.
V0006130	APP0140	APP3320	App. authentication process is inadequate.
V0006168	APP0160	APP3300	Application client authentication
V0006131	APP0210	APP3380	Application userids are not unique.
V0006132	APP0220	APP6240	Inactive userids are not disabled.
V0006133	APP0230	APP6250	Unnecessary built-in userids are not disabled.
V0006134	APP0240	APP6260	Userids have default or weak passwords.
V0006135	APP0310	APP3210	Sensitive app. data not protected at rest.
V0006136	APP0320	APP3250	Sensitive app. data .not protected in transit.
V0006137	APP0330	APP3150	Unapproved cryptographic module
V0006138	APP0410	APP3680	App. security auditing is inadequate
V0006139	APP0420	APP3650	No warning when app. log near full
V0006140	APP0430	APP3690	Application audit records are vulnerable
V0006141	APP0510	APP3480	Separation of duties not enforced.
V0006142	APP0515	APP3240	Actions not authorized before execution
V0006143	APP0520	APP3500	App. process runs with unnecessary privileges
V0006144	APP0530	APP3410	Session limits do not exist for the application.
V0006145	APP0550	APP2040	Classification guide does not exist
V0006146	APP0560	APP3270	Classification labels not appropriately displayed
V0006147	APP0570	APP5030	App. access control not restrictive enough
V0006148	APP0580	APP3020	User interface can be circumvented
V0006149	APP0610	APP3050	Inactive code/libraries not removed
V0006150	APP0620	APP3060	Application code and data are collocated.
V0006151	APP0630	APP6030	Unnecessary services or software not removed
V0006198	APP0640	APP2160	Application client not STIG compliant
V0006169	APP0710	APP2100	Application network architecture exposes resources
V0006170	APP0730	APP2070	Products are not NIAP/Common Criteria approved
V0006171	APP0740	APP6160	Disaster recover plan does not exist
V0006172	APP0750	APP6190	Backups or backup procedures are incomplete.
V0006173	APP0760	APP6140	Incomplete process to retain app. logs
V0006174	APP0770	APP6100	Sensitive data not purged from production export
V0006197	APP0780	APP2010	An IAO or IAM has not been assigned
V0006152	APP0810	APP3440	Warning message not displayed

V0007013	APP0815	APP3010	App. interfaces not identified/protected.
V0006153	APP0820	APP3430	Authentication credentials not removed
V0006154	APP0830	APP3470	Non-privileged not adequately protected
V0006155	APP0840	APP3420	App. does not provide proper session termination
V0006156	APP0850	APP3350	Authentication credentials or sensitive data is st
V0006157	APP0870	APP3080	Application code contains invalid references to ne
V0006158	APP0910	APP3740	App. sends e-mail containing executable code
V0006159	APP0920	APP3700	App transmits unsigned Cat 1A or 2 mobile code
V0006160	APP0930	APP3720	App transmits mobile code that attempts OS access
V0006161	APP0940	APP3710	App. accepts uploaded mobile code w/o signature
V0006162	APP0950	APP3730	App uses mobile code with no established policy
V0006163	APP1010	APP3100	Temporary objects not removed from system
V0006164	APP1020	APP3510	Insufficient input validation
V0006165	APP1030	APP3590	The application is vulnerable to buffer overflows.
V0006166	APP1040	APP3120	Inadequate error handling
V0006167	APP1050	APP3140	App. failure can result in an insecure state
V0006117	APP7100	APP2100	Additional Application Check 1
V0006118	APP7110	APP2120	Additional Application Check 2
V0006119	APP7120	APP2130	Additional Application Check 3
V0006120	APP7130	APP2140	Additional Application Check 4
V0006121	APP7140	APP2150	Additional Application Check 5
V0006122	APP7150	APP2160	Additional Application Check 6
V0006123	APP7160	APP2170	Additional Application Check 7
V0006124	APP7170	APP2180	Additional Application Check 8
V0006125	APP7180	APP2190	Additional Application Check 9
V0006126	APP7190	APP2200	Additional Application Check 10