

APPLICATION SECURITY ASSESSMENT REPORT

Vision Industries, Inc.
Oracle Financials UK

MARCH 28, 2009

Table of Contents

EXECUTIVE SUMMARY	6
Findings	6
Configuration Assessment	6
External Penetration Testing.....	6
Additional Findings and Recommendations.....	7
SCOPE AND METHODOLOGY	8
Assessment Scope	8
Technical Scope	9
Application Modules	9
Servers	9
Network Infrastructure	9
Operating System.....	10
Customizations.....	10
Sarbanes-Oxley Compliance	11
Timeline and Staffing	11
Target Environment	11
Methodology	11
Vulnerability Information	12
Risk	12
Complexity	12
Remediation Effort	13
Remediation Risk	13
ORACLE APPLICATIONS	14
Accounts and Passwords	14
Default Application Accounts.....	14
Application Passwords	14
Application User Accounts	15
Generic Application User Accounts.....	15
Responsibilities.....	16
Segregation of Duties for System Administration	16
Responsibility Analysis.....	17
Functional Security	17
Menu Analysis	17
Function Analysis.....	17
User Profile Options.....	18
Security Profile Options	18
Auditing Profile Options	18
Other Profile Options	19
Auditing and Logging.....	19
Applications Auditing	19
Application Log files	20
File Permissions.....	20
Patches	21
Oracle Critical Patch Updates.....	21
Recommended Security Patches.....	22

Other High Priority Patches	23
DATABASE ASSESSMENT	24
Accounts and Passwords	24
Default Database Accounts	24
Default Database Accounts Passwords	25
Custom Database Accounts	26
Database Account Password Analysis	26
Custom Password Verification Function	27
System and Object Privileges	28
System Privileges	28
Database Roles	29
Object Privileges	29
Database Links	30
Initialization Parameters	30
File Permissions	31
Security Patches	32
Oracle Critical Patch Updates	32
Other Database Security Patches	32
Database Listener	32
Auditing	33
Logging	34
APPLICATION SERVER ASSESSMENT	36
Apache	36
HTTPD Configuration Directives	36
Logging	37
J2EE Configuration	38
File Permissions	38
Forms Server	39
Reports Server	40
Security Patches	41
Oracle Critical Patch Updates	41
Other Security Patches	42
OPERATING SYSTEM ASSESSMENT	43
User Accounts	43
UNIX Security Patches	44
Configuration	44
Auditing and Logging	45
NETWORK AND DMZ ASSESSMENT	46
Reverse Proxy Configuration	46
Firewall Configuration	46
Recommended Open Ports	46
Application Firewall Configuration	47
CUSTOMIZATION ASSESSMENT	48
Development Process	48

Coding Standards	48
Code Review Process.....	48
Change Management Process	49
Custom Database Objects	50
Human Resources Interface.....	50
Order Entry Interface	51
Other Interfaces	52
iSupplier Customizations.....	53
SQL Injection	53
Cross Site Scripting (XSS).....	54
Required Code Modifications	54
iStore Customizations.....	55
Authentication Issue.....	55
Item Security Bypass	56
Cross Site Scripting (XSS).....	57
Required Code Modifications	58
Self-Service Customizations	59
Custom Reports.....	60
OPERATIONAL ASSESSMENT	61
Summary	61
User Management (1.1)	62
Segregation of Duties (1.2)	63
Database Security (1.3).....	64
Network and Web Security (1.4)	65
Operating System Security (1.5)	66
Applications Auditing (2.1)	67
Database Auditing (2.2).....	68
Web Logging (2.3)	69
OS Auditing (2.4).....	70
Application Monitoring and Troubleshooting (3.1)	71
Database Monitoring and Troubleshooting (3.2)	72
Web and Forms Monitoring and Troubleshooting (3.3)	73
Operating System Monitoring and Troubleshooting (3.4).....	75
Object Migrations (4.1).....	76
Application Configuration Change Management (4.2)	77
Database Change Control (4.3).....	78
Database Configuration Change Management (4.4).....	79
Web Server Change Control (4.5).....	80
Operating System Change Control (4.6)	81
Application Patching (5.1)	82
Database Patching (5.2)	83
Application Server Patching (5.3)	84
Operating System Patching (5.4)	85
Application Development (6.1).....	86
Database Development (6.2)	87
Web Development (6.3).....	88
Shell and File Transfer Development (6.4)	89
ACTION ITEMS	90

Summary	90
Critical	91
High Priority.....	92
Low Priority	93
Optional	94
APPENDICES	96
INDEX	103
ABOUT INTEGRITY	108

ABOUT INTEGRIGY

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.


Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com