****

**Information Security**

**Open Source Security Assessment**

**February 2007**

# PURPOSE:

# This checklist will function as the formal checklist for InfoSec approval of Open Source code to be introduced into the IT Solutions controlled Northrop Grumman computing environment. This list will functional alongside Open Source checklists produced by Infrastructure Engineering and Legal. The output of this assessment will be a InfoSec recommendation to the Open Source Council as to Approval, Disapproval or additional steps/testing that must be accomplished prior the OS code introduction into the environment or execution steps that must be accomplished to address Information Security concerns or risks associated with the output or products created from Open Source code use in our environment. (As of March 2007 this document is DRAFT until formal ratification from Information Security is declared.Vance Field has action to obtain ratification from InfoSec.)

# GUIDANCE:

This checklist is not necessarily intended to result in a binary decision about the introduction of the Open Source code into the environment. The output of this document will be used by the Open Source Council InfoSec member to adjudicate the disposition of the OS Council InfoSec vote. This document is subject to change an may not require InfoSec ratification following change. The InfoSec Open Source Council member will determine if ratification is required.

# Public Open Source community website review

Summarize an assessment from of a minimum of two websites (such as Owasp, SecurityFocus, BugTraq) that discuss the open source code, its development life cycle. This assessment will be subjective in nature and enhanced with more explicit judgment criteria over time. This assessment will be combined with the below assessment of the code functionality for a recommendation from Information Security.

# Security Architecture

## Provide a high-level architecture diagram showing all servers, network components, etc required to host the application. Describe OS, application software, database software, etc (including versions/release levels) hosted on each server or network component.

## Provide a full data flowchart (network communication) showing all network protocols and ports between all servers and network components. Include whether the communication is uni-directional or bi-directional.

## Provide information on supported client OS, versions/release levels and hardware requirements. Provide details on software and versions/release levels required on the clients that is not part of a standard operating system installation (i.e. SQL client, Oracle client, etc). If the application is web-based, which web browsers and versions are supported?

# Authentication

## Does the application support native (built into application) username and password for authentication? What other authentication methods does the application support?

## Does the application automatically force a user to enter a new password the first time the user logs in?

## Does the application provide a means for Security Administrators/Help Desk to “reset” passwords for authorized users who have forgotten their password? If the password has been reset and the user logs in, does the application force the user to change their password?

## Does the application provide a means for users to self-administer (change) their password during subsequent access?

## Does the application mask passwords during input on the screen, when the password field is displayed on screen and do not embed passwords in clear text within emails, logs or documents?

## Does the application support customer configurable parameters for minimum/maximum password length, password complexity, and number of reiterations before a password can be reused?

## Does the application support password expiration on a definable time cycle? Is the time cycle customer configurable?

## Does the application provide a reminder to the users to change their password prior to their passwords expiring? Is the reminder period customer configurable to multiple reminders?

## Does the application support minimum password aging? Is the aging period customer configurable?

## Does the application automatically lockout the account for a period of time after a set number of failed login attempts? Is the lockout period and number of failed attempts customer configurable?

## Does the application automatically disable (requires administrator intervention to reactivate the account) an account after a set number of failed login attempts? Is the number of failed attempts customer configurable?

## Does the application indicate (error message) which part of the log on data is correct or incorrect?

## Does the application automatically disable an account after a defined period of inactivity? Is the time period customer configurable?

## Does the application have the ability to report on accounts that have been disabled for a defined period? Automatically remove accounts that have been disabled for a defined period? Is the time period customer configurable?

## Does the application allow for one user defined question and answer to be captured from a new user during the account creation process for security purposes?

## Does the application have default, maintenance or guest accounts? Can these accounts be deleted, disabled or password protected with a strong, complex password?

## Does the application automatically log off users after a pre-set idle time? Is the pre-set idle time customer configurable?

## Does the application schedule jobs to be run at a defined time (batch) and is successful authentication required prior to the job running?

## Are the batch (i.e., scheduled jobs, machine-to-machine) passwords at least 10 characters in length and not embedded in a machine-readable file in clear text?

## Does all electronic transmissions of passwords utilize 128 bit strength symmetric encryption or higher?

## Explain how passwords are protected at rest (stored).

## Does the application have the ability to store authentication credentials within a LDAP repository? If so, is the communication secured/encrypted?

## If Single Sign On authentication is used, is it as strong as the authentication mechanisms for each of the individual services?

## Does the application utilize session cookies for session authentication? Are the sessions validated on the server side?

## Does the application have unauthenticated sessions? If so, please explain.

## In situations where browser cookies are utilized as a component of SSO or access control, are the cookies non-persistent?

## Does the application encrypt cookies that contain sensitive data, in situations where browser cookies are utilized as a component of SSO or access control (e.g. When malicious modification could result in unapproved access by an individual with a valid account)?

## When certificate based authentication is used within the application, is it based upon an agreed upon root authority(s)?

## When utilized for client authentication, does the application store the certificates securely and protect them as described in the client certificate user obligation documentation?

## Does the application have clear mechanisms for the granting, revocation, and suspension of certificate? The certificates should be checked every time a certificate is presented.

## Does the application use FTP, Telnet, e-mail or any other services that involve authentication in the clear as part of the package?

# Authorization and Access Control

## Does the application provide role based authorization enforcement capabilities?

## Does the application provide rule based authorization enforcement capabilities?

## Does the application provide the ability to define a custom role for an individual?

## Does the application allow for multiple classes of users?

## Does the application provide the ability to define read-only roles to view security and non-security configurations and audit trails (i.e. auditors)?

## Does the application provide the ability to define a security administration role that can view and configure security parameters?

## Does the application provide the ability to define non-security administrative roles that can view and configure application specific parameters but not security parameters?

## Does the application restrict access control on a need to know basis (e.g., customer service)?

## Does the application have mechanisms to enable the data owner to manage access to data items?

## Does the application have mechanisms to enable the data owner to manage access to data repositories (e.g., folders)?

## Does the application have access control highly granular with ability to easily manage access control rights to individual data objects and collections of data objects?

## Does the application have flexible options for controlling who can add/remove members to team lists?

## Does the application have check-in and check-out capabilities of data objects?

## Does the application have iteration control of data objects?

## Does the application have file locking of data objects?

# Audit Trials

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: A user successfully logs on to the application

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Every time a user fails to authenticate to the application

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: The disabling/locking out/enabling of an account

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: A user initiated data object modification (read, modify, create, delete object) event occurs

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Team membership changes are made

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Privilege changes are made

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Role base changes are made

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Rule base changes are made

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Workflow changes are made

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Illegal system access attempts (e.g., modifying the URL).

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: There is a failed file or object access

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: There is a failed use of user rights

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: There is a successful or failed change of security configurations/parameters/policies

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: There is a failed user/group configuration/parameter/policy change

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: A user utilizes a particular service or application

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events: Access to the scripts and bin folders

## Does the application create audit trails containing at a minimum the User ID, the source IP address and a secure timestamp and include the following events for: Access to the directories that contain files that are published as part of your web site?

## Does the application have tamper resistant audit trail files?

## Does the application log at a record level where databases are involved?

## Does the application log at a field level where databases are involved?

## Does the application ensure that read access to the audit trail file be restricted to specific security administrators?

## Does the application ensure write and modify access to audit trail files be limited to only those accounts creating the audit trail files?

## Does the application provide a means for audit trails to be archived/rolled over via a definable time cycle?

## Does the application ensure that when a log file/disk is full, the system will backup the file to another electronic medium?

## Does the application include an audit trail that captures changes to the underlying operating system (e.g., use of a tripwire)?

## Does the application ensure that failure to backup audit trails when they are completely filled will stop the system from functioning?

## Does the application ensure that all server operating systems on which audit trail files are generated from, have their clocks synchronized to a common standard (Time stamps must be recorded in GMT)?

## Does the application provides the ability to read the audit trails using standard tools such as text editors, XML viewers or Web browsers?

## Does the application provide the ability to filter logging based on event type and level of events?

## Does the application provide the ability to configure alerts to be sent for security violation events?

# Information Security

## Does the application, upon receiving an unencrypted document and before placing documents in a vault, subject the document to anti-virus scanning?

## Does the application perform virus-checking capability for all data objects entering/leaving the service?

## If virus checking is reliant on signature-based methods, signatures/engines, does the application enable updated daily or specified period signatures?

## In a development activity where Active-X is used, does the development include putting a mechanism in place covering the digital signing of Controls and the quality/performance/behavior standards confirmed by the digital signature?

## In a development activity where JAVA Applets are used, does the development include putting a mechanism in place covering the digital signing of Applets and the quality/performance/behavior standards confirmed by the digital signature?

## In a development activity where JAVA is used, does the development include Java security sandbox when Java is used on the client?

## Within the application, for applets that require file I/O and/or any other local/network permissions, do they require digitally signature, which by default will grant permissions per Sun’s default security policy?

## In situations where plug-ins are used within the application, is the distribution from a validated source (preferably NG) with NG performed quality checks?

## In the application, are all session time outs set to occur after 20 minutes of inactivity for a standard user?

## In the application, are all session time outs set to occur after 12 minutes of inactivity for a privileged user (one who has access to privileged or higher classifications of information)?

## In the application, are connections waiting for connection acknowledgement or connection activity from non-responsive subjects automatically terminated after the connection timeout period expires? Is the connection timeout period customer configurable?

## Does the application disallow simultaneous sessions from the same subject?

# Security Assessment

## Has an independent security review (code review) been conducted on the application for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

## Has an internal code review been conducted on the application? If so, what tool(s) was used, what were the results and what remediation activity has taken place?

## Describe the process to immediately disable all or part of the functionality of the application should a security issue be identified.

## Provide documentation on whether, and where the application uses Java, Javascript, ActiveX, PHP, or ASP (active server page) technology.

## Provide documentation on what language the application back-end is written in (C, Perl, Python, VBScript, etc)

## Describe the quality assurance process for detecting common security issues such as cross-site scripting, buffer overflow, command injection, numeric range overflow/underflow, etc within the application. What tools are used to detect?

## Is the application scanned for vulnerabilities, mis-configured services or ports?

## How often are major versions, minor versions and patches released for the application?

## What is a typical timeframe for releasing a remediation patch when a critical vulnerability is discovered?

## Are the patches/releases scanned with anti-virus or anti-malware tools to ensure it is free of malware before being released?

## Are digital fingerprints published with software/patch releases to verify the integrity of the software?

## Describe the quality assurance process in testing security patches for the application as well as 3rd party security patches (OS, database, etc) for software and hardware required to support the application.

## Is the application tested in a hardened environment including OS, database and other required components with industry standard hardening guidelines applied for each component as well as latest, applicable patches?

## Describe supplier’s involvement in troubleshooting/remediating issues that may arise when the application breaks or is non-operational due to the customer applying a 3rd party critical security patch (i.e. OS patch, SQL patch, etc).

## Describe what application security enhancements/patches have been released in the last 6 months.

## Describe what application security enhancements/patches will be release in the next 6 months.

# Cryptography

## Does the application use symmetric cryptography? Explain encryption algorithm(s), key length(s) and where it is used. Does the application provide the ability to change symmetric keys on a definable time cycle? Is this time cycle customer configurable?

## Does the application use asymmetric cryptography? Explain encryption algorithm(s) and key length(s) and where it is used.

## Does the application require Public Key Infrastructure (PKI) services? If so, explain.

## Does the application use random number generation to generate keys for symmetric and asymmetric cryptographic operations? Explain when it is used.

## Does the application use hashes or digital signatures? Explain the hashing algorithm(s) and where it is used.

## If the application stores/transmits sensitive (i.e. passwords, personally identifiable information, company-sensitive/proprietary information) information, does the application support end-to-end document encryption? Explain encryption algorithm and key length.

## Does the application provide the ability to encrypt sensitive data at the field level? Explain encryption algorithm and key length.

## If and when sensitive data is extracted from a database of the application and displayed to a user’s screen, does the application display/label the sensitivity of the data prominently on the user’s display?

## When cryptography is used within the application, are the encryption keys universal for all customers or are the encryption keys specific for each customer?

## If the encryption keys are universal, what has been solution for customers desiring to produce their own internal reports on sensitive data that is encrypted?

## Are there tools within the application to perform multiple overwrite (DoD 5220.22M) of stored sensitive data?

# Assessment of Supplier Information Security

## Does the supplier have a security officer who oversees and is accountable for the security within their application?

## Does the supplier have an information security staff responsible for reviewing secure coding and security development within their application?

## Do the application developers and support team attend regular security training? Explain frequency and type of training.

## How does the application developers and support team stay current on security vulnerabilities?

## Is there any application or code development performed outside the United States?

## Are there any employees who are foreign nationals that may be handling/accessing Northrop Grumman data?