

Date 04/01/2013



**Environmental Management Consolidated Business Center (EMCBC)**

**Subject: Software Application Development and Management**

Information Management Procedure

APPROVED:

A handwritten signature in red ink, appearing to be "A. R.", written over a horizontal line.

ISSUED BY: OFFICE OF INFORMATION RESOURCES MANAGEMENT

---

1.0 PURPOSE

The purpose of this procedure is to define the process for Non-Safety Software Application Development and Management.

2.0 SCOPE

This procedure is for all applications developed by the Office of Information Resource Management (IRM) that utilize data management software such as MYSQL, ORACLE, SQL Server, etc.

3.0 APPLICABILITY

This procedure is applicable to all general application development activities. It is not applicable for applications requiring the development of an Exhibit 300 (financial applications over \$5 million per year, other applications costing over \$5 million over three years, or designated "Critical Systems") or to Nuclear Safety or Safety Related Software.

4.0 REQUIREMENTS and REFERENCES

4.1 Requirements:

- 4.1.1 Department of Energy, Office of the Under Secretary of Energy Program Cyber Security Plan (Energy PCSP)
- 4.1.2 PL-240-08, Cyber-Security-System Security Plan for General Support
  - 4.1.2.1 IA-6, Authenticator Feedback
  - 4.1.2.2 SA-11, Developer Security Testing
  - 4.1.2.3 SI-2, Flaw Remediation
  - 4.1.2.4 SI-3, Malicious Code Protection
  - 4.1.2.5 SI-9, Information Input Restrictions
  - 4.1.2.6 SI-10, Information Input Validation
  - 4.1.2.7 SI-11, Error Handling
- 4.1.3 PS-240-06, Policy on the Control of Unclassified Electronic Information

## 4.2 References:

- 4.2.1 Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) -Application Security Checklist  
[http://iase.disa.mil/stigs/app\\_security/app\\_services/app\\_serv.html](http://iase.disa.mil/stigs/app_security/app_services/app_serv.html)
- 4.2.2 Publication 127-2 Federal Information Processing Standards (FIPS) Database Language SQL, 1993 June 02
- 4.2.3 DOE O 414.1D, Quality Assurance
- 4.2.4 DoD 5015.2-STD Electronic Records Management Software Application Design Criteria standard, 2007
- 4.2.5 NQA-1 2004 Part II, SubPart 2.7
- 4.2.6 Guide to IT Capital Planning and Investment Control (CPIC), September 2010
- 4.2.7 IMP-8308-02, Configuration Management of Computer Systems and Networks.
- 4.2.8 Management System Description – Document Control Management, Procedure 7, Control of Technical Instruction Documents
- 4.2.9 PL-414-04, Quality Assurance Implementation Plan
- 4.2.10 Management System Description – Records Management

## 5.0 DEFINITIONS

- 5.1 Alpha Testing: Testing of applications with inert data (made up data).
- 5.2 Beta Testing: Testing of applications with “real” data.
- 5.3 Content Manager: Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.
- 5.4 Content Owner: The Assistant Director responsible for the content within the given application or system.
- 5.5 Data Sensitivity: Sensitivity of the data in accordance with the EMCBC Policy on the Control of Unclassified Electronic Information, PS-240-06. See Attachment A.
- 5.6 Data Set: The entirety of the type of data that the application will be manipulating including data type and sensitivity.
- 5.7 Data Type: Data within the EMCBC is classified by type according to the sensitivity of the data. Where data types are mixed, the most stringent control shall apply. See Attachment A.
- 5.8 Developer(s): IRM staff responsible for coding, testing, placing the application into production, and maintaining the application.
- 5.9 Independent Reviewer: IRM staff responsible for conducting the Software Quality Assurance Review when required. This individual shall not also act in any of the

following roles: System Owner, Content Owner, Content Manager, or Developer for the application in question.

- 5.10 IRM Support Staff: IRM staff responsible for assisting in the completion of all required documentation related to the development and maintenance of an application.
- 5.11 Statement of Need: Defines what need is being fulfilled by the application. Address the functionality of the system, who needs to access the system, how often, and where they are located.
- 5.12 System Owner: The lead IRM individual that has overall implementation responsibility for any given application. Usually the Assistant Director for the Office of Information Resource Management (ADIRM).

## 6.0 RESPONSIBILITIES

### 6.1 System Owner shall:

- 6.1.1 Approve the completed Application Project Plan (APP).
- 6.1.2 Establish the Data Base Management System and applicable user interface.
- 6.1.3 Provide the test and baseline actions required to certify or recertify the application for production.
- 6.1.4 Conduct a Make or Buy Analysis and oversee the procurement.
- 6.1.5 Include elements of Software Quality Assurance (SQA) applicable to specific projects.
- 6.1.6 Conduct annual application review.
- 6.1.7 Approve requests for software changes.
- 6.1.8 Conduct semi-annual APP Log review.

### 6.2 Content Owner or Manager (when assigned) shall:

- 6.2.1 Submit a written request, hard copy or electronic, of the perceived need for a new application, which includes a Statement of Need, Data Type, and Data Sensitivity, to the ADIRM for determination of viability.
- 6.2.2 Complete Checklists for Software Classification Determination, IMP-8308-03-F1, and Software Evaluation, IMP-8308-03-F2.
- 6.2.3 Develop a flow chart of the business system that is being automated.
- 6.2.4 Develop an analysis of the life cycle requirement for the application.
- 6.2.5 Approve the proposed schedule for completion.
- 6.2.6 Submit written requests, hard copy or electronic, for software changes to the ADIRM for approval.

### 6.3 Developer shall:

- 6.3.1 Assist in development of the APP.

- 6.3.2 Develop a schedule for completion.
- 6.3.3 Develop the code for the application.
- 6.3.4 Ensure that the application is brought into Configuration Management.
- 6.3.5 Conduct testing and develop Baseline Change(s) as necessary.
- 6.3.6 Resolve issues identified during Alpha and Beta Testing.
- 6.3.7 Complete testing documentation as required.
- 6.3.8 Complete the baseline security for web applications as required.
- 6.3.9 Document all maintenance activities in the IRM Project Management System and/or Information Management (IM) Maintenance Log as required.
- 6.3.10 Complete required fields (e.g., code location, database, etc.) in APP Log.
- 6.3.11 Ensure APP Log is updated as necessary.
- 6.4 IRM Support Staff shall:
  - 6.4.1 Develop and complete the APP for approval.
  - 6.4.2 Maintain APPs and testing documentation for IRM.
  - 6.4.3 Develop changes and revisions to APP during the life cycle.
  - 6.4.4 Maintain APP Log.
- 6.5 Independent Reviewer shall:
  - 6.5.1 Approve the completed APP.
  - 6.5.2 Conduct Software Quality Assurance review when such a review is required.

**NOTE:** The individual assigned as the Independent Reviewer shall not also act in any of the following roles: System Owner, Content Owner, Content Manager, or Developer for the application in question.

## 7.0 GENERAL INFORMATION

This procedure provides for a structured process for the inception, design, development, and testing of applications developed by the EMCBC. The intent of this procedure is to provide for a fluid and streamlined inception and design phase followed by a rigorous test phase to ensure that all data meets the requirements for availability, integrity, and security.

Software development is a complex, iterative process in which SQA principles play an important role. This procedure does not provide a detailed implementation for all tasks associated with developing or maintaining DOE software. Rather it provides the framework for controlling, managing and documenting that process. The System Owner is responsible for including those elements of SQA applicable to the specific project.

## 8.0 PROCEDURE

Applications can cover a wide variety of data control and manipulation. They range from a simple application with a single table to support simple queries on a webpage to complicated multi-tabled databases containing sensitive data with intricate user interface. Application Development and Management is controlled through an eight phase process: Initiation, Application Definition, Development, Acceptance Testing and Baseline, Production, Revision and Maintenance, Annual Review, and Retirement.

- 8.1 Initiation – The initiation process is started when a perceived need for an application to accomplish a specific task or group of tasks is developed. This need is presented to the IRM staff and from there informal discussions formulate the concept and general scope of the proposed application. Once a concept has been formulated the ADIRM will determine if the proposed application is viable and if resources are available to pursue the development. Discussion at the management level will determine if the development will go forward and will align the project schedule with the priorities of the organization.
- 8.2 Application Definition – Once there is a general agreement among management to proceed, IRM will establish an APP. APPs are controlled as Technical Instructions Documents (TIDs) in accordance with Document Control Management, Procedure 7, Control of Technical Instruction Documents. This project plan will define the overall objectives of the application; define the key roles of System Owner, Content Owner, Content Manager, and Developer; and provide the following information:
  - 8.2.1 Statement of Need – The Statement of Need defines what need is being fulfilled by the application. It should also address the functionality of the system, who needs to access the system, how often, and where they are located. Also this section should discuss reporting requirements and any manipulation of data required. The generation of a flow chart that shows the flow of data is encouraged and may be required by the Developer to assist in application design. This section will be completed using information provided by the Content Owner and/or Manager.
  - 8.2.2 Data Set – The data set is the entirety of the type of data that the application will be manipulating. This section will be completed using information provided by the Content Owner and/or Manager.
    - 8.2.2.1 Data type - The data type should be described by description or title, approximate length, and whether it is a member of a subset of data.
    - 8.2.2.2 Data Sensitivity – The data set shall also identify the sensitivity of the data in accordance with the EMCBC Policy on the Control of Unclassified Electronic Information, PS-240-06. Attachment A has a summary chart from that policy.
    - 8.2.2.3 Software Quality Assurance Checklists – The proposed purpose and functionality of the software is assessed to determine the need for a Software Quality Assurance Review utilizing the following

forms; Checklists for Software Classification Determination, IMP-8308-03-F1, and Software Evaluation, IMP-8308-03-F2.

- 8.2.2.4 Records Management –Utilizing Attachment B “Is it a Record?” and IMP-8308-03-F3 as guidance, the Records Management Implications of the proposed application is determined.
- 8.2.3 Security Requirements – Once the Data Sensitivity has been established, the security and access requirements will be defined by the Developer and documented in the APP. At a minimum, all applications are tested for SANS (SysAdmin, Audit, Network, and Security Institute) Top 20 Vulnerabilities (<http://www.sans.org/top20/>).
- 8.2.4 Development Schedule – The Developer will create a proposed schedule for completion with input from the ADIRM and Content Owner and/or Manager.
- 8.2.5 Life Cycle Analysis – This section will be completed by using the information provided by the Content Owner and/or Manager and it shall indicate a time frame for application retirement and final disposition.
- 8.2.6 Make or Buy Analysis - Once all of the above data elements are contained in the APP the System Owner or designee will conduct a Make or Buy analysis. This analysis should include Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), and the compatibility of other in-house applications or applications from other sites and reflect the criteria for SQL databases contained in the Federal Information Processing Standards (FIPS) 127-2.
- 8.2.6.1 Implementation - Once the analysis is complete, the System Owner or designee will determine how the application will be implemented. If purchased, the System Owner will oversee the procurement, and if by in-house development, the System Owner will establish the Data Base Management System and applicable user interface.
- 8.2.6.2 Cost Estimate - Applications with a rough cost estimate of fewer than 80 hours of internal resources do not require documented make or buy decision.
- 8.2.7 Approval – The ADIRM and the Independent Reviewer will approve the completed APP.
- 8.3 Development – The assigned Developer shall proceed with development, modification, or installation of the application. The Developer will work closely with the Content Manager to ensure that all the requirements of the APP are being implemented.
- 8.3.1 Changes – During the course of all development there is a need for changes that were not anticipated during the APP development. For the most part changes are minor and do not affect the development requirements established in the APP. However, if there are any changes made that would affect the sensitivity of the data or the types and locations

of users accessing the data, the APP will be updated to reflect the new needs and the Data Sensitivity and Security Requirements will be reexamined.

8.4 Acceptance Testing and Baseline – This phase has three distinct sub-phases: Alpha Testing, Beta Testing, and Conducting a Baseline. A Software Quality Assurance Review, when such a review is determined to be required by the Software Evaluation, IMP-8308-03-F2, is conducted as appropriate by the Independent Reviewer during this period. The complexity of the Software Quality Assurance Review may be as simple as an independent review of the output or as complex as a detailed Software Quality Assurance Test Plan.

8.4.1 Alpha Testing is conducted once the Developer releases the application to the Content Manager and other applicable persons as determined by the Developer and Content Manager for initial testing. This may be done in whole or in part at the discretion of the Developer and the Content Manager. Alpha testing may be done in-house or from remote locations. However, ALL ALPHA TESTING IS CONDUCTED WITH INERT DATA. Real data is not to be used during alpha testing as it could very easily expose sensitive data. At the end of alpha testing the testers will develop a punch list for suggested changes or corrections. The Content Manager and Developer will then review the punch list and determine the path forward. Any major changes to the application will require a revision to the APP.

8.4.2 Beta Testing is conducted with live data. At the end of Beta Testing the testers will again develop a punch list of items that need correction. The Content Manager and Developer will then review the punch list and determine the path forward.

8.4.3 A Baseline is conducted in accordance with IMP-8308-02, Configuration Management of Computer Systems and Networks. This process ensures that all cyber security controls are in place and functioning. Security Testing will be conducted in accordance with the applicable TIDs. Application specific security tests will be developed as needed and updated in the appropriate TID(s).

8.5 Production - Once all testing and security items have been resolved and with the concurrence of the Content Owner and System Owner the application is considered to be certified and is placed into production.

8.6 Revision and Maintenance

8.6.1 Minor changes may be made in accordance with the provision of Configuration Management of Computer Systems and Networks, IMP-8308-02, and **must** be documented in the IRM Project Management System and/or IM Maintenance Log as required by the Developer.

8.6.2 Requests for major changes are required to be in writing, hard copy or electronic. Acceptable requests include, but are not limited to, email or a completed software change request form IMP-8308-03-F4.

- 8.6.3 If a major revision (such as a change in data sensitivity, application access process, results of the Checklists for Software Classification Determination or Software Evaluation, or as deemed necessary by the System Owner) to the application is required, the IRM Staff will develop an addendum to the existing APP to clearly define the needed changes. The System Owner or designee will provide the necessary testing and baseline actions, including a Software Quality Assurance Review by an Independent Reviewer as appropriate, required to recertify the application for production.
- 8.7 Annual Review – Each application will be reviewed annually by the System Owner or designee to ensure that it is still needed and meets current security requirements. This review may be done in concert with other related applications. All reviews are documented in the IRM Project Management System, APP Log, and/or IM Maintenance Log as required.
- 8.8 Retirement – At the end of the life cycle the application will be retired in accordance with the APP and dispositioned according to the IRM File Plan.

## 9.0 RECORDS MAINTENANCE

Records generated as a result of implementing this document are identified as follows, and are maintained by the Office of Information Management and are managed in accordance with the EMCBC Organizational File Plan:

- 9.1 ADM 20-10.1-A – Software Development Case Files
- 9.2 GRS 24-08-C – IT Operations Records – IM Maintenance Log

## 10.0 DOCUMENTATION

- 10.1 Checklists for Software Classification Determination, IMP-8308-03-F1
- 10.2 Software Evaluation, IMP-8308-03-F2
- 10.3 Records Management Compliance Checklist, IMP-8308-03-F3
- 10.4 Software Change Request, IMP-8308-03-F4
- 10.5 APP Log

## 11.0 ATTACHMENTS

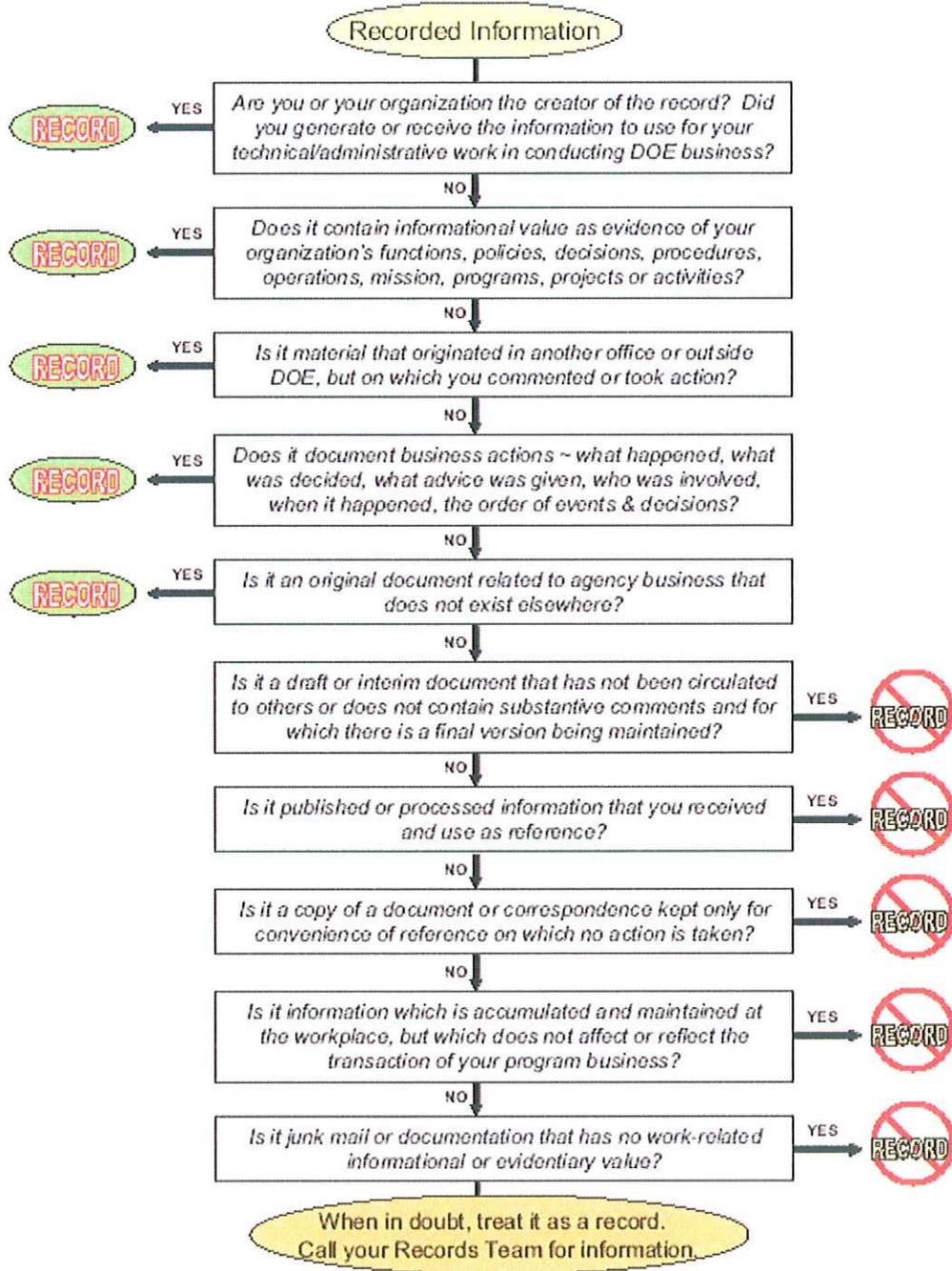
- 11.1 Attachment A - Summary Chart on Controls for Electronic Information
- 11.2 Attachment B – Is It A Record?
- 11.3 Attachment C – Forms IMP-8308-03-F1, IMP-8308-03-F2, IMP-8308-03-F3, and IMP-8308-03-F4

**ATTACHMENT A**  
**Summary Chart on Controls for Electronic Information**

Type	Definition	Control
I-P II	Data defined as PII by regulation or requirement	Data is only stored on network storage devices. Access is controlled by network credentials. Special authorization required for transportation on mobile devices. Users receive special training to ensure protection of this data.
I	Data that has been specifically defined as needing encryption by requirement such as Sensitive Unclassified Information	Data is stored or transported encrypted as required and, requires two factor authentication for remote access. Users receive special training to ensure protection of this data.
II	Business Sensitive Data – data that has a direct bearing on business decisions that if compromised could result in an unfair advantage to parties conducting business or in legal action with the department. Type II data is designated by the Content Owner	Data access is controlled through the network and requires two factor- authentications for remote access. Data is protected by encryption in transport.
III	Information about Business Sensitive Data that requires protection to ensure data integrity, and a level of confidentiality, or data needs to be screened from the general public. Type III data is designated by the Content Owner	Data access is controlled through the network, requires username and password for remote access. Files transported on removable media should be protected by password.
IV	Public data that may be released at any time. Web site data makes up the bulk of this data	Data access is controlled through the network. Data is posted to the web as directed by the Content Manager. Precautions are taken to ensure data integrity.

ATTACHMENT B

Is it a Record?



**ATTACHMENT C  
FORMS**

*Checklists for Software Classification Determination*

***PART A: Checklist for Nuclear Safety-Impacting Software***

Software Title(s): \_\_\_\_\_

Software Owner: \_\_\_\_\_ Project/Program Information Officer \_\_\_\_\_

Check as applies:

1. \_\_\_\_\_ New Software    \_\_\_\_\_ Existing Software
2. \_\_\_\_\_ Off-the-Shelf    \_\_\_\_\_ Spreadsheet/Database Report
- \_\_\_\_\_ Custom, Vendor    \_\_\_\_\_ Custom, In-house    \_\_\_\_\_ Process Control

This checklist determines if the software being assessed impacts nuclear safety, using these definitions:

**Nuclear Safety:** Prevention of radiological harm to workers, the public, or the environment from nuclear activities.

**Nuclear Activities:** Activities with the potential to cause radiological harm from ionizing radiation.

NUCLEAR SAFETY-IMPACTING SOFTWARE CHECKLIST			
NO.	QUESTION	YES	NO
1	Does the software <u>ONLY</u> support objectives in one or more of the following functional areas? Technology Programs (TP)                      Financial Management (FM) Project Control (PC)                              Public Involvement (PI) Human Resources (HR)                          Property Management (PM)		
IF THE ANSWER TO QUESTION 1 IS "YES," THE SOFTWARE IS NOT NUCLEAR SAFETY-IMPACTING. DO NOT COMPLETE THE REMAINDER OF PART A. CONTINUE WITH PART B OF THIS FORM.			
IF THE ANSWER TO QUESTION 1 IS "NO," CONTINUE WITH PART A.			
2	Does this software produce data used to determine personnel access to radiological areas?		
3	Is the software used to detect or measure radioactivity, or does it support the management and control of radiological areas including posting?		
4	Does this software perform tracking or accountability for Enriched Restricted Material (ERM)?		
5	Is this software used to determine ERM physical storage dimensions/arrays?		
6	Does this software determine or monitor personnel, facility, or environmental radiation exposure or contamination (e.g., release, radiation work limits, dose rates)?		
7	Is this software used to measure or test facility, component, equipment, or container conformance for nuclear material to an established requirement (e.g., performance grading, quality level, or specification)?		
8	Does this software determine or implement emergency actions related to nuclear safety?		
9	Is this software necessary to develop a safety basis requirement (SBR) or technical safety requirement (TSR)?		
10	Does this software determine or control operational limits, settings, status, or equipment configurations (e.g., flows, temperatures, positions, process logic controls, human machine interfaces, operational parameters) established or described in safety basis documentation (SBD)?		
IF THE ANSWER TO <u>ANY</u> OF QUESTIONS 2 THROUGH 10 IS "YES," CHECK THE "YES" BOX BELOW. THE SOFTWARE IS NUCLEAR SAFETY-IMPACTING. DO NOT COMPLETE PART B OF THIS FORM. CONTINUE WITH PART C OF THIS FORM.			
IF THE ANSWER TO <u>ALL</u> OF QUESTIONS 2 THROUGH 10 IS "NO," CHECK THE "NO" BOX BELOW. THE SOFTWARE IS NOT NUCLEAR SAFETY-IMPACTING. CONTINUE WITH PART B OF THIS FORM.			

RESULT: IS THE SOFTWARE NUCLEAR SAFETY-IMPACTING?

YES

NO

Checklists for Software Classification Determination

**PART B: Checklist for Mission/Business-Essential Software**

This checklist determines if the software is Mission/Business-essential, Select, or Other Managed software, using these definitions:

**Mission-Essential:** Supports an activity/process that is necessary for successful achievement of the site's mission.

**Business-Essential:** Supports a core business activity or process.

**Select:** Not Nuclear Safety-Impacting or Mission/Business-Essential but still requires control.

**Other Managed:** Software used for display of informational data only.

MISSION/BUSINESS-ESSENTIAL, SELECT, OTHER MANAGED SOFTWARE CHECKLIST			
NO.	QUESTION	YES	NO
1	Is this software used for the display of informational data only?		
IF THE ANSWER TO QUESTION 1 IS "YES," THE SOFTWARE IS OTHER MANAGED. DO NOT COMPLETE THE REMAINDER OF PART B. CONTINUE WITH PART C OF THIS FORM.			
IF THE ANSWER TO QUESTION 1 IS "NO," CONTINUE WITH PART B.			
2	Is this software used to engineer, analyze, or calculate facility equipment designs, and/or configurations?		
3	Will the loss of irreplaceable or difficult-to-construct data (e.g., tests, samples, etc.) cause an unacceptable break in the continuity of operation for the user or owner organization?		
4	Is this software used to determine or select remedial actions for environmental cleanup of contaminated sites or facilities?		
5	Is this software used to evaluate present or future hazards from an implemented or proposed remedial action?		
6	Is this software used to protect facilities from inside or outside threats (e.g., facility security, fire protection)?		
7	Will a software-processing error or failure require more than \$100K to resolve?		
8	Does this software determine or implement emergency actions other than nuclear-related?		
9	Would a processing error or failure of the software have a legal impact or external milestone impact?		
10	Will this software take more than 8 man-months of effort to develop, or cost more than \$50K to procure or change?		
11	Is this software required to comply with state and federal regulations?		
12	Does the system/application process sensitive information?		
13	Is this software used to track procurement or contractual actions, including credit card purchases?		
14	Is this software used to provide budgets and budget components necessary to make sound business decisions?		
15	Is this software used to perform employee-related duties such as payroll or benefits?		
16	Is this software used to track government-furnished property?		
17	Is this software integral to the financial management of the project?		
IF THE ANSWER TO <u>ANY</u> OF QUESTIONS 2 THROUGH 17 IS "YES," CHECK THE "YES" BOX BELOW. THE SOFTWARE IS MISSION/BUSINESS-ESSENTIAL. CONTINUE WITH PART C OF THIS FORM.			
IF THE ANSWER TO <u>ALL</u> OF QUESTIONS 2 THROUGH 17 IS "NO" CHECK THE "NO" BOX BELOW. THE SOFTWARE IS SELECT SOFTWARE. CONTINUE WITH PART C OF THIS FORM.			

RESULT: IS THE SOFTWARE MISSION/BUSINESS-ESSENTIAL?

YES

NO

IF NO, SOFTWARE IS SELECT SOFTWARE

Checklists for Software Classification Determination

**PART C: Complete for All Software**

1. Name of the vendor who provided the existing software or who will provide the new software (if applicable).	
2. If new, is this software an upgrade to an application currently used at the EMCBC? If so, name the application.	
3. Describe the purpose of the software.	
4. Describe the technical requirements of the software. For example, is it standalone or LAN-based? Are current network communications adequate? If new, what is the impact on other software and systems? If new, what are the hardware requirements (memory, printers, monitors, etc.)? Not required for subcontractor.	
5. What organizations use or will be affected by this software?	
6. List the names of the key users or subject matter experts. Individual names not required for subcontractor.	
7. Who supports, or will support, this software (for example, installation, testing, maintenance, license updates, upgrades, user support)? Information Management? Software Owner? Vendor? If more than one, explain the division of the responsibilities.	
8. Identify those who are authorized to approve and accept the software before initial implementation and before changes are implemented. Individual names not required for subcontractor.	
Project/Program Software Owner (print/sign):	Date:
Project/Program Information Officer (print/sign):	Date:
Manager, Information Management (print/sign):	Date:

**ATTACHMENT C  
FORMS**

**Software Evaluation**

<p><i>Software Name:</i></p>	
<p>1. What is the software classification determination?</p> <p> <input type="checkbox"/> Nuclear Safety-Impacting               <input type="checkbox"/> Mission/Business-Critical               <input type="checkbox"/> Select Software               <input type="checkbox"/> Other Managed Software           </p>	
<p>2. Has a Software Documentation Folder been created and is it being maintained as a record?</p> <p> <input type="checkbox"/> Yes   <input type="checkbox"/> No               Enter file code: _____           </p>	
<p>The following questions serve as a self-assessment to ensure all major elements of Software Quality Assurance commensurate with the software classification determination have been addressed. Attach additional documents as needed or make reference to the Software Documentation Folder.</p>	
<p>3. Was testing documentation consistent with requirements of IMP-8308-03, Software Application Development and Management?</p>	
<p>4. Identify individuals acting as independent reviewers or acceptance testers. (Individual names not required for subcontractor software.)</p>	
<p>5. Describe the Software Configuration Management Plan (or make reference to the procedure). Is the plan consistent with requirements of IMP-8308-03, Software Application Development and Management?</p>	
<p>6. Are the source code and data security sufficient to avoid inadvertent loss (for example, not on open group drive, password-protected, etc.)?</p>	
<p>7. Does sufficient documentation exist for use and management of the system so that another person with proper subject matter knowledge could use and support the system?</p>	
<p>8. Overall assessment: Were the appropriate documentation, test documentation, and change control elements applied commensurate with the software classification level?</p>	
<p>Project/Program Software Owner (print/sign):</p>	<p>Date:</p>
<p>Project/Program Information Officer (print/sign):</p>	<p>Date:</p>
<p>Manager, Information Resource Management (print/sign): (not required for Select or Other Managed Software)</p>	<p>Date:</p>

**ATTACHMENT C  
FORMS**

**Records Management Compliance Checklist**

**Section 1:** Determination of Records Implications

A Yes answer to any questions below indicates that the proposed application has records implications. Include this determination in the Application Project Plan.

1. Does the proposed application replace a paper-based system that currently generates records?
2. Is the proposed application an upgrade or extension of an existing system that has been determined to have records implications?
3. Does the proposed application create or manage any of the following types of information? Unclassified? Official Use Only? Privacy Act? Quality Assurance? Vital Records? Permanent Records?
4. Based on the above information and Attachment B, (Is It a Record?), will the proposed application contain or produce or declare information to be records?
5. Is the proposed application an Electronic Records Management System (ERMS) that identifies records and applies retention periods?

**Section 2:** If the proposed application has records implications as per Section 1, include the following information in the Application Project Plan.

6. If the proposed application contains records (Yes to question 4) and is not an ERMS (No to question 5), does the functionality include the transfer of the records to a separate ERMS that meets DoD 5015.2-STD, "Design Criteria for Electronic Records Management Software Applications?"
7. If the application is an ERMS (Yes to question 5), does the proposed application meet DoD 5015.2-STD, "Design Criteria for Electronic Records Management Software Applications?"
8. If the proposed application contains records (Yes to question 4), is not an ERMS (No to question 5), and does not include functionality to transfer the records to an ERMS (No to question 6) then does the work process include printing the records in hardcopy?
9. Describe how the software and metadata to support retrieval will be retained for the life of the information/record?

**ATTACHMENT C  
FORMS**

**Software Change Request Form**

Requestor Name		Date Submitted	
Requestor Email		Requestor Phone	
Requestor Organization		Requestor Location	

Application Name	
Short description of request (Attach detailed specification)	
Justification for change	
Classification of Data as per IMP-8308-03	
Will this change alter the results of the Software Quality Assurance Checklist of the application? If yes, explain.	
Target date	

**Review & Approval Status**

<b>Content Manager Approval</b>		
Name:	Signature:	Date:

<b>IRM Approval</b>		
Name:	Signature:	Date:

**EMCBC RECORD OF REVISION**

DOCUMENT TITLE: Software Application Development and Management

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- I Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- I Placing the words GENERAL REVISION at the beginning of the text.

---

<b>Rev. No.</b>	<b>Description of Changes</b>	<b>Revision on Pages</b>	<b>Date</b>
0	Initial Information Management Procedure Supersedes IP-240-03, Rev. 2	Entire Document	08/30/12