United States Department of Agriculture
Agricultural Marketing Service

Directive 3130.3 06/13/2008

DEVELOPMENT OF BROWSER-BASED APPLICATIONS

I. PURPOSE

This Directive provides guidance for the development and enhancements of AMS browser-based applications that will be hosted on the AMS Internet, Extranet, or Intranet servers. Browser-based applications are those that use an Internet browser program such as the Microsoft Internet Explorer or Netscape Navigator to run the application on the client computer. Any AMS program developing a browser-based application should reference this Directive when writing the Statement of Work or during the Requirements Analysis Phase. This directive should also be referenced prior to the application's development for a complete listing of technical requirements.

II. REPLACEMENT HIGHLIGHTS

This Directive updates AMS Directive 3130.3 Development of Browser-Based Applications, dated 3/1/06. Changes are marked with asterisks.

III. POLICY

It is the policy of AMS that all new applications or major enhancements to existing applications are browser-based or capable of being used on "thin clients," which are clients that depend primarily on a central server for processing activities. Additionally, browser-based applications shall comply with Agency and Department standards to allow applications to be securely and efficiently administered by the Information Technology Group (ITG) and the AMS programs. Exceptions to the use of these standards shall be approved in advance by the AMS Chief Information Officer (CIO).

Each application shall be designed to operate in the following environments:

IV. AGENCY PLATFORM

A. Agency Internet, Extranet, and Intranet Servers Platform:

- Windows 2003 (Clustered Environment) ;
- Internet Information Server 6.0;
- .NET Framework; and
- SQL Reporting

The use of SQL Reporting is not required. It is currently available on the AMS Internet servers and is used to provide advanced reports that can be accessed from .NET applications.

Distribution: AMS **Originating Office: S&T/ITG**

Application owners are responsible for the licensing, maintenance, and support of the application and its supporting software. ITG is responsible for the licensing, maintenance, and support of the infrastructure.

B. Browser-Based Applications: The key development components of the AMS environment are listed below. To see a full description of the AMS application development environment, review the "AMS Technical Environment" document, available on the corporate portal, AGNIS under the ITG Team site in the ITG Reference Documents document library.

- Visual Basic .NET ;
- SQL Server Clustered Environment; and
- The Microsoft Installer (MSI) for the application installation.

Exceptions to use development environments other than Visual Basic.NET for new browser-based applications must be approved in writing by the CIO in advance of any application development.

C. Client Platform:
Extranet and Intranet-based applications shall support at a minimum the Internet Explorer 6.0browser or higher. Internet-based applications shall support at a minimum the following browsers:

- Internet Explorer Version 5.x+
- Netscape Version 6.x and 7.x+
- Netscape Version 4.7x - Must provide as much functionality as possible, with the consideration that minor look and feel differences may occur compared to the latest browser versions.
- Safari Version 1.0 (Macintosh)
- Mozilla – Firefox

V. PLANNING AND DEVELOPMENT PHASE

A. Planning Sessions Consultation: When planning for the development and implementation of a browser-based application or enhancements to an existing browser-based application, the requirements must be stated to ensure that the application will operate properly within the AMS environment. It is required that AMS programs and/or AMS contractors complete the following planning documents listed below prior to application development. The documentation templates described below are available on the corporate portal, AGNIS, under the PMPSB Team site in the AMS Investment Management Handbook and Templates folder,

1. MS Project Schedule that includes all the project tasks and milestones with scheduled completion dates.
2. Functional Requirements Document that includes the functional process requirements, system performance requirements, security requirements, and quality assurance factors.

3. Design Document that includes "wireframes" and an infrastructure diagram detailing any ports required for the firewall, any connectivity between the demilitarized zone (DMZ) and backbone, and any other system-specific information relating to the specific functionality of the application.

Note: Wireframes are a structural layout of what the application page will look like See Section V.B.4 for more information about wireframes.

It is mandatory that AMS request user documentation, either in a manual or on-line format from the contractor/Agency developing the application.

-AMS programs and/or the AMS contractor must meet with E-Business at the following times:

1. At the start of the project, to review the application requirements prior to starting the project;
2. Three to four weeks prior to deployment on AMS' Test server, to verify that all of the application requirements will be ready for deployment to the Test server. The developers must insure that the code is well documented and the complete set of documentation, as listed in Section VII, is delivered and accepted by the Information Technology Group (ITG). At this time, ITG must be provided with bandwidth, server, and other IT related requirements;
3. Prior to application deployment (refer to section V.B.5 for details regarding the deployment schedule); and
4. Post-deployment, for a knowledge-transfer meeting with ITG to discuss system maintenance and provide detailed system documentation.

Larger applications will require more consultation than smaller applications.

B. Mandatory Development Requirements: The following information must be provided to the E-Business Branch for all applications. Utilize the Form AMS-21 "Application Development Check List" (Attachment 1) for ease of reporting and for the deadline of each document. This Check List is a tool for verifying that all requirements have been met prior to application deployment.

1. Documentation:

It is required that AMS programs and/or the AMS contractor complete the following documents. Required documentation templates are available on the corporate portal, AGNIS, under the PMPSB Team site in the AMS Investment Management Handbook and Templates folder.

a. Software Version Description Document
b. System Administration Plan
c. Deployment Plan, including installation and rollback instructions and test scripts
d. Conversion Plan, if applicable.

2. Section 508 of the Rehabilitation Act:

The program shall ensure that all technology delivered complies with standards set forth in Section 508 of the Rehabilitation Act of 1973, as amended, particularly 36 CFR 1194.21-22. Outline the development strategy to ensure Section 508 compliance. For more information, see http://www.section508.gov and AMS Directive No. 3130.2, Section 508 Information Access Requirements.

3. e-Authentication Requirements:

Web-based Internet applications that require user authentication (the identity of the user must be known to access the application) and/or user authorization (the identity of the user is used to determine what parts of the application the user should be allowed to access) must use the USDA e-Authentication service or obtain a waiver from the Department. This service will allow public users and USDA employees to use a single account and password to access all USDA applications that they use to conduct business. A member of E-Business will be made available during the planning phase to evaluate the e-Authentication requirements and discuss the e-Authentication implementation, if required. This applies for both in-house and outsourced applications.

E-Business is the key e-Authentication integrator for the AMS program areas and provides full support in all phases of e-Authentication integration. The E-Business consultation activities include: initial eAuthentication overviews, completion of the requirements and risk assessment forms, eAuthentication integration design and programming for the AMS application, eAuthentication integration database design and integration of the eAuthentication Web Service (developed by E-Business) in the AMS application. The developer will be responsible for the programming of the AMS application.

4. USDA Web Style Guide (WSG) Requirements:

All web-based applications that are available on the AMS Internet website are required to comply with the USDA Web Style Guide. All new and enhanced Internet applications must conform to the WSG. All pre-existing applications have been grandfathered in and will not need to comply with the WSG until they are enhanced.

Refer to chapters three and six of the WSG for web application requirements and to chapter four for overall style guidelines. Wireframes only apply to Internet applications and must be submitted to Public Affairs and approved prior to application development. These may be submitted separately or as part of the Design Document. Wireframes do not include graphics. One wireframe will be needed for each page type. A final review and approval is required by AMS Public Affairs prior to application deployment into the Pre-Production and Production environments. Failure to submit wireframes prior to application development may result in a delayed deployment. The WSG is available on the corporate portal, AGNIS, under the E-Business Team Site in the Shared Documents team library, under the Web Presence folder. For current guidelines or clarification, please contact the AMS Public Affairs Staff at 202.720.8998.

5. Deployment Schedule:

AMS has two environments that an application must pass through successfully prior to production deployment: Test and Pre-Production. The Test and Pre-Production environments are used to determine that the application will operate correctly in the AMS environment and the infrastructure will properly support it. The program owner must familiarize themselves with the AMS technical environment documentation and ensure that their application will run correctly in the AMS infrastructure before bringing the application to AMS to begin deployment. Load testing and other testing results must be provided to further document the stability of the application.

All system configuration and testing for connectivity to the Internet, database, File Transfer Protocol (FTP), eAuthentication, electronic mail and other software needed by the application (e.g. SQL reporting) is performed in these environments. Under normal circumstances an application may spend up to one week in each environment prior to moving to the next. The developer is responsible for providing detailed deployment instructions, infrastructure diagrams, and instructions to test connection points (including account information to access the application). AMS is responsible for the deployment of the application and the testing of all connection points, in all environments, using the installation and rollback instructions and test scripts provided in the Deployment Plan. The application owner must provide E-business with a minimum of three business days notice prior to moving to the next environment.

a. Test Environment:

The applications are deployed to the Test environment first. In the Test environment, the applications will be accessing the Test database. Applications that do not need integration with eAuthentication can be tested by both internal USDA users and external users. If an application is integrated with eAuthentication, the internal USDA users and external users will need static Internet Protocol (IP) addresses to access the application in the test environment.

The high level connection testing is to ensure that an application can successfully access all infrastructure software and services needed to perform its functionality. For example, if an application needs to access the database, send mail, perform file transfers (FTP), integrate with eAuthentication, and use Reporting Service for reporting purposes, each of these components will need to be tested separately and test scripts must be provided for all required tests. AMS will ensure that applications can access all software and connect to them before releasing it for “User Testing.” The application shall be fully tested prior to being submitted to AMS for deployment and code fixes are not needed. User Testing will involve detailed testing of business functionality of the application. If the users find defects with the application, the code has to be fixed by the developer and submitted to AMS for redeployment in the Test environment. Once the business owner approves that testing of the application is complete, AMS will deploy the application to the next environment: Pre-Production.

b. Pre-Production Environment:

The applications in Pre-Production will point to the “Production databases.” This environment is a duplicate of the production environment. A successful test in the Pre-Production environment should result in a very smooth migration to the Production environment. In the Pre-Production environment, applications that do not need integration with eAuthentication can be tested by both internal USDA users and external users. If an application is integrated with eAuthentication, the internal USDA users and external users will need static IP addresses to access the application in the Pre-Production environment.

AMS is responsible for deployment of the application and testing of all connection points. Once the testing has successfully completed, AMS will release the application for User Testing. After User Testing, the business owner needs to provide approval in order to deploy the application to the production environment.

c. Production Environment:

AMS is responsible for deployment of application to the production environment. "Connection Testing" by AMS and the "User Testing" by the business owner is required prior to announcing the availability of the application to the general public. Neither the contractor nor the program shall discuss Internet application features or availability with the press prior to clearing this communication with the Public Affairs Staff and obtaining the concurrence of the E-Business Branch.

All external and internal users will have access to the application in the production environment.

Deployment to production servers must occur during non-business hours (e.g., Saturday, Sunday, or early morning on a weekday with installation, testing, and rollback, if necessary, completed by 7 a.m. with instructions provided). The application owner and/or contractor will hold a post-deployment, knowledge-transfer meeting with ITG and program personnel to discuss system maintenance and provide detailed system documentation.

VI. RESPONSIBILITIES

A. The Application Owner shall:

1. Host all Internet applications on Agency-owned servers, operated by ITG. Intranet applications may be hosted either on the Agency Intranet server or on a program-owned Intranet server;
2. Provide security and infrastructure support for program-managed servers;
3. Work cooperatively with ITG and the E-Business Branch throughout the lifecycle of the project as described in Section V., above;
4. Comply with Agency and Departmental security standards and be subject to periodic security audits;
5. Encrypt sensitive information stored in configuration files, including but not limited to database connection strings, file share usernames and passwords, FTP usernames and passwords, and Web Service usernames and passwords;
6. Provide a method for decrypting data, if appropriate;

7. Maintain the unique functionality of the application, including any application-specific third party software;
8. Develop and test the application using non-infrastructure equipment that is of a compatible configuration to that of the AMS environment which will house the application. The AMS infrastructure equipment will not be made available for development and contractor testing;
9. Obtain Public Affairs approval for all Internet applications; and
10. Submit to ITG all of the required documentation listed in Section VII, in accordance with the templates provided at the start of the project, including Form AMS-19, "Browser-Based Application Development Agreement"(Attachment 2). The AMS-19 is required prior to application development.
11. Submit to ITG the AMS-21, the "Application Development Check List" to verify that all requirements have been met prior to application deployment.

B. ITG and the E-Business Branch shall:

1. Provide pre-project consulting regarding the AMS environment;
2. Provide technical consulting and support during the development, implementation, and deployment phases of the project;
3. Secure and maintain Agency-managed servers; and
4. Provide infrastructure support during the lifecycle of the application.

VII. DOCUMENTATION

Each browser-based application must have, at a minimum, the documentation listed below prior to implementation. Documentation templates are available on the corporate portal, AGNIS, under the PMPSB Team site in the AMS Investment Management Handbook and Templates folder. Each of the documents listed below is applicable at varying stages of the application life cycle. Please refer to the Application Development Check List for the applicable timeframes. For application updates and refreshers, application owners must update all documents accordingly and provide new installation and rollback instructions and code for the installation.

Each application must be approved for accreditation by AMS and the Department in advance of its deployment as a production system.

A. System Documentation: System documentation shall be provided to ITG prior to implementation for full support of the application. The system documentation includes the following documents and shall be submitted to ITG during the Planning Sessions and Mandatory Development Requirements Phase.

1. MS Project Schedule, including all the project tasks and milestones with scheduled completion dates;

2. Functional Requirements Document, including the functional process requirements, system performance requirements, security requirements, and quality assurance factors;

3. Design Document, including wireframes and an infrastructure diagram detailing any ports required for the firewall, any connectivity between the DMZ and backbone, and any other system specific information relating to the specific functionality of the application;

4. Software Version Description Document, including the inventories of materials released, software contents, data definition language scripts, data manipulation language scripts, and database and installation instructions;

5. System Administration Plan, including the system architecture, installation and configuration instructions, maintenance instructions, and security requirements;

6. Deployment Plan, including installation and rollback instructions and test scripts;

7. User documentation, including the User Manual and on-line help, as appropriate; and

8. Conversion Plan Document (if applicable), describing how data will be migrated from one format into another, such as from an Excel spreadsheet a SQL Server database.

All system documentation is required prior to deployment. However, the application installation and rollback instructions and the latest copy of the application source code must be provided to ITG prior to installation onto the Test application server.

B. IT Continuity of Support Plan: An IT continuity of support plan describes how to sustain major applications and general support systems in the event of a significant disruption. This plan will include the Disaster Recovery Plan for continuing critical operations during a significant disruption, and the Business Resumption Plan for returning to normal operations following the disruption. A minimum of six weeks prior to deployment in the Production environment, E-Business must be provided with:

1. Any application specific software or hardware requirements;
2. A paragraph describing the application's functions, information processed, and a program contact (if available);
3. The criticality of the application; and
4. The required recovery time objectives (how long can the application be down), and the recovery point objectives (how much data can be reentered)

This information will be incorporated into the DMZ Contingency Plan, Disaster Recovery Plan, and Business Resumption Plan.

VIII. OUTSOURCING

When an application is constructed and implemented using outside contractors for deployment on the AMS Internet or Intranet, the following requirements shall be addressed within the Statement of Work:

A. The contractor will be required to meet all specified security requirements depending on the application and where it will be hosted (e.g., personnel physical access, identification (badges)/escorts, background checks or clearances, security and privacy training, as required).

B. The application shall be fully tested according to contract specifications prior to deployment on AMS infrastructure equipment.

C. The application owner remains responsible for complying with this directive even when the application development is outsourced.

IX. QUESTIONS

If you have any questions concerning browser-based application development, contact the E-Business Branch Chief, Information Technology Group.

/s/

Lloyd C. Day
Administrator

Attachment 1, Application Development Check List
Attachment 2, Browser-Based Application Development Agreement