MCR Checklist for Automated Information Systems
(Major Applications and General Support Systems)

Name of GSS or MA being reviewed: _____

Region/Office of GSS or MA being reviewed: _____

System Owner: _____

System Manager: _____

Name & title of person responsible for accomplishing the review: _____

Name(s) of the System Security Manager(s): _____

Review the topics/subject areas listed under the "Management Control Element" heading. If there are topics/subject areas that are not applicable to the GSS or MA being reviewed, put an "N/A" under the lead paragraph for the topic and provide an explanation in the comments block.

1. For each question in the Management Control column, put a "Y" for Yes, a "N" for No, "P" for Partially and a "N/A" for Not Applicable. (Note: If the entire topic has been declared N/A, do not bother to enter N/A for each following question for that topic.)

2. In the "Effective?" column, enter a "Y" for Yes, "N" for No, and a "P" for Partially.

3. In the "Comments" column, you **must** provide an explanation for every "No," "Partially," and "Not Applicable" answer in any of the other columns. Use this space to provide any additional information about the subject necessary for understanding. **Record any outstanding or positive feature found worthy of mention.**

4. Summarize your findings using the **General Control Profiles** form.

5. Report any identified Medium or High risk control weaknesses on the **Control Evaluation Report** form.

I. General Management Controls: These questions deal with automated information systems in general. Very often, these questions can be answered once for all of the GSS or MA under a single system owner.

Management Control Element	Y/N/P/NA	Effective?	Comments
A. CONFIGURATION CONTROL			
(1) Hardware Inventory Control Are there one or more current inventories that would provide a current and accurate accounting of all hardware components of the GSS or MA? This includes mini-computers, microcomputers, mainframes, servers, terminals, plotters, printers, communications equipment (including PBX switches), etc. **Provide a complete copy and attach to this review.**			

(a) Do these inventories identify ownership and responsibility for the equipment?			
(b) Do these inventories identify the specific GSS or MA the equipment is a part of?			
(2) Software Inventory Control Are there one or more inventories that would provide a current and accurate accounting of all software authorized for use on the GSS or MA? Do the inventories identify current versions of operating system, utility, system management, access control, and security software? Do not include software that resides on the individual workstation unless it is a critical component of the GSS or MA. **Provide a complete copy and attach to this review.**			
(3) Data Inventory Is there a current and complete list of all significant databases hosted on or supported by the GSS or MA? Are all sensitive databases properly identified and labeled? **Provide a copy and attach to this review.**			
B. POLICIES AND PROCEDURES: Are there established and documented procedures for accomplishing the following?			
(1) Formulating and establishing policies related to operations and maintenance of the GSS or MA?			
(2) Controlling modifications and additions to any component of the GSS or MA?			
(3) Identifying and addressing ITM support requirements for the GSS or MA?			
(4) Are there well defined, documented and enforced policies and procedures for resource acquisition? Do these policies ensure that new resources are acquired in an efficient and cost effective manner?			
(5) Ensuring that Regional, Program and Service standards are considered and followed?			
(6) Are there well defined, documented and enforced policies and procedures for implementing AIS Security as prescribed by 270 FW 7, AIS Security? Do these policies ensure that the security needs of the GSS or MA are identified, reported to management, and implemented in a cost effective manner?			
(7) Is there a process that provides for periodic reviews of GSS or MA performance and are there documented techniques for making appropriate adjustments?			
(8) Is there a review mechanism in place to ensure that Departmental, Service and/or other appropriate Federal agency requirements are satisfied in the operation of the GSS or MA?			
(9) Is there a well documented, comprehensive and current Contingency Plan for the GSS or MA?			
C. ORGANIZATIONAL / EMPLOYEE ISSUES			

(1) Are all employees that will work with or support the GSS or MA, given an orientation of the appropriate use policies, procedures, management controls and security policies before they are allowed to use the system?			
(2) Is a program in place to continuously assess the employee's skill and training requirements and to provide on-going training as needed to build and maintain skills, increase knowledge, improve understanding of management controls and to assure an understanding of necessary security practices?			
(3) Are prospective employees that will be required to work with Sensitive Systems/Applications subjected to appropriate pre-employment checks in accordance with Service and Departmental guidelines?			
(4) Are duties related to management of a GSS or MA, including administration and security, included in the position performance standards for the individuals responsible?			

II. General Systems Software Issues. These issues deal with system software regardless of platform. While particularly germane to networks, computer centers and other multi-user systems, they are also applicable to micro-computers and special application equipment (for example a GIS Workstation).

Management Control Element	Y/N/P/NA	Effective?	Comments
A. OPERATING SYSTEMS			
(1) Are operating system instructions, password tables, and other security algorithms protected from unauthorized access by either hardware or software?			
(2) Is the use of privileged operating system instructions controlled or restricted?			
(3) Are strict limits placed on who may use system utilities and for what purposes? Are all users aware of these restrictions?			
B. SYSTEM SOFTWARE CHANGE CONTROL: The objective is to ensure the accuracy and reliability of the various GSS and MA by preventing unauthorized modifications to system software and unauthorized or illegal access to user data.			
(1) Are all operating system software modifications documented, approved and maintained by a system manager?			
(2) When changes occur, is the relevant documentation updated?			

III. General Facilities Issues. These issues deal with the general operating environment of the facility as it relates to the supported General Support Systems.

Management Control Element	Y/N/P/NA	Effective?	Comments
A. PHYSICAL ACCESS CONTROLS			

(1) Are there specific, well documented and enforced access procedures to the area hosting the GSS or MA?			
(2) Are equipment rooms, user access areas and other special access areas related to the GSS or MA kept locked during off-duty hours or when unattended? Is access to these areas monitored during normal working hours?			
(3) Is access to the facility controlled by cipher lock, key card or other positive identification device?			
(4) Are employees cautioned to challenge strangers and are there procedures in place to deal with unauthorized persons?			
(5) If used, are combinations changed periodically?			
(6) Are all ground floor windows or those easily accessible kept locked or otherwise protected from access?			
B. Environmental Controls: These items deal with those factors that provide a working environment suitable for the GSS or MA equipment and the personnel necessary to operate and use it.			
(1) Are the GSS or MA the work areas, maintained in a clean condition? This means trash does not accumulate, excessive materials are not stored in open areas, aisles are clear and usable, etc.			
(2) Is smoking restricted to designated areas away from the air return space for any of the GSS or MA equipment?			
(3) Is eating or drinking in close proximity to the equipment prohibited?			
(4) Is the temperature of the facility monitored and controlled to provide a safe and comfortable range for both the equipment and the employees?			
(5) Are the operating temperature ranges of the equipment known and are there established procedures for taking action beyond these ranges?			
(6) Are the facility air intakes, especially those that support the GSS or MA equipment, protected from excessive contaminants such as dust and industrial fumes?			

(7) Is the GSS or MA connected to power through surge protectors, line conditioners or other protective devices?			
(8) Are all electrical outlets properly grounded?			
(9) Are there known points of contact for major environmental components such as air conditioning, water, housekeeping, maintenance, electrical, etc.?			
(10) Are supplies of paper and stationary stored in such a manner that paper dust contamination is kept to a minimum?			
(11) Is static electricity controlled through the use of humidifiers, de-humidifiers, static free carpet/flooring, etc.?			
C. SAFETY AND HAZARDS CONTROL			
(1) Are emergency procedures well documented and posted in places that are convenient and easy to read?			
(2) Are emergency exits and power cut-off switches clearly marked?			
(3) Are there well documented policies and procedures relating to fire risk management and are they readily available to all who need them?			
(4) Are fire drills practiced periodically?			
(5) Are emergency phone numbers for the fire department, police, doctor and hospital posted in strategic locations?			
(6) Are all personnel aware of the proper notification procedures?			
(7) Are suitable hand extinguishers strategically located around the area with location markers visible?			
(8) Are all personnel aware of the proper use of the hand extinguishers?			
(9) Are there audible and visible fire alarms to accommodate the hearing impaired?			

IV. User Billing and Charge-back Controls. If this GSS or MA supports some form of user billing or charge-back, ensure procedures and are consistent with the guidelines established in 376 DM 6. Skip this section if User Billing and Charge-back are not supported on this GSS or MA.

Management Control Element	Y/N/P/NA	Effective?	Comments
A. IF USER BILLING AND CHARGE-BACK ARE ASPECTS OF THIS GSS or MA:			

(1). Are the procedures well documented and consistent with Departmental directives?			
(2). Does a formal billing and charge-back agreement exist between the users and the installation?			
(3). Is the user billing and charge-back procedures tied to the job accounting system for the component?			
(4). Is the user billing and charge-back based on an equitable accounting method appropriate to the component and organization?			
(5). Do procedures exist for determining a users share of system development consists and overhead if appropriate?			
(6). Is there an equitable procedure for charging reruns to the user so that user errors are properly charged to the user and installation errors are charged to the installation?			
(7). Are current installation/component costs consistent with budgeted costs?			
(8). Do users get periodic billing statements that provide a detailed accounting of use and the algorithm used.			

V. AIS Security Issues

Management Control Element	Y/N/P/NA	Effective?	Comments
A. ACCOUNTABILITY			
(1). Has an System Security Manager been appointed for this GSS or MA in accordance with 270FW7, AIS Security?			
B. SECURITY POLICIES AND PROCEDURES			
(1). Are security policies and procedures related to this GSS or MA current and readily available?			
C. CONTINGENCY PLAN			
(1) Is there a well documented, comprehensive and current Contingency Plan for this GSS or MA?			
(2) Does the plan identify who is authorized to initiate the actions identified and under what conditions?			
(3) Does the plan identify critical and sensitive files, software, or data and critical components for priority recovery?			
(4) Has the plan been tested within the last year?			
(5) Is the location of the plan known and is it accessible by those who would need to implement it?			

(6) Does the Contingency Plan contain procedures for backing up critical software and data and for storing these backups in appropriate locations for emergencies?			
(7) If a sensitive system or application is being supported, is an uninterruptible power supply or other form of backup power used to help guarantee continued service and availability?			
D. ACCESS CONTROLS			
(1) Are the GSS or MA access controls clearly defined and are there written procedures for controlling, removing, and monitoring access permissions?			
(2) When "guest" accounts are established to access the GSS or MA, is access to system utilities and general administration functions restricted? Is the account removed immediately when no longer needed?			
(3) Is there a reliable user authentication technique in place for any dial-up access to the GSS or MA?			
(4) Are User IDs and Passwords required for access to the GSS or MA and its hosted functions?			
(5) Are Passwords at least 5 characters in length?			
(6) Are Passwords required to be changed every 90 days and is re-use of passwords controlled?			
(7) Are users trained in how to properly construct and control a password?			
(8) Is it clearly understood by management and users that the use of a password in an automatic log-on file such as a script is a high risk and is prohibited by Service policy?			
(9) Have all factory set, default passwords been removed from the GSS or MA?			
(10) Is there a mechanism in place to suspend a persons log on privileges after a maximum of 3 invalid attempts?			
(11) Are there well documented procedures for resetting or restoring a persons password after they have bee locked out or if they forget their password?			
(12) Is it well understood by GSS or MA users that a User ID and Password constitute a valid signature and that sharing passwords is a very high risk undertaking and is to be avoided?			
(13) Is there an effective technique to validate and control access to the GSS or MA by dial-up users?			
(14) If passwords are stored on the GSS or MA, are they encrypted?			

(15) Is the time and date of last use of the password maintained as part of the system audit trail?			
(16). Are there procedures in place and used to identify all GSS or MA users while they are active? Is there an access log that can be reviewed to help identify suspicious activity?			
(17). Are there procedures for assigning, controlling, and removing user access from the GSS or MA?			
(18). Is there an effective Virus protection package implemented on the GSS or MA?			
(19). Is there a warning notice, at log on, advising users that the GSS or MA is an official Government system and cautioning them against unauthorized access and use?			
E. RISK ASSESSMENT			
(1) Are procedures in place to accomplish a risk assessment at least every three years per 270 FW 7, AIS Security and OMB A-130, Appendix 3?			
(2). Has a risk analysis been accomplished within the last 3 years? If so:			
(3) Has a report of findings and recommendations been provided to the appropriate manager?			
(4) Is there a recorded response from management on these findings and recommendations?			
(5) For all countermeasures that were to be implemented, has implementation been completed or scheduled?			
(6) For all countermeasures that will not be implemented, has a rationale been provided for the record?			

VI. Records Management Controls for the GSS or MA. This is to ensure that electronic records created and/or maintained on the GSS or MA are managed and protected in accordance with Federal requirements (36 CFR 1234 Electronic Records Management).

Note: Guidelines for defining Electronic Records is not an ITM function. Definition of what constitutes a Record is the responsibility of the Records Manager. **However, for those items defined as records, the GSS or MA must provide the appropriate level of control and management. This includes electronic mail, Web pages, and other repositories of electronic information.**

Management Control Element	Y/N/P/NA	Effective?	Comments
A. REGARDING RECORDS MANAGEMENT ON THIS GSS or MA:			
(1). Does the system provide an appropriate level of security to ensure integrity of the documents? This includes protection against unauthorized access, modification, or deletion.			

(2). Does the system ensure electronic records are disposed of according to National Archive Records Administration (NARA) approved schedules?			
(3). Does the system provide a standard interchange format if it is necessary to exchange records on electronic media between systems?			
(4). Have appropriate personnel been trained to safeguard sensitive, proprietary, confidential, or privacy records?			
(5). Does the system facilitate the distinction between record and non-record materials?			
(6). Are system management audit reports retained on file for a reasonable amount of time?			
(7). If applicable, does the system provide for electronic signature and surnaming on records that require this capability?			
(8). Does the system retain records in a usable format until their authorized disposition data? Does the system ensure that the information is not lost because of changing technology or deterioration?			
(9). Are there procedures to identify storage locations of official records and to ensure that such records are not stored or archived in unauthorized locations?			

VII. Sensitive System\Sensitive Application. This information is to be collected for all GSS or MA applications that are Sensitive or process sensitive information. If the GSS or MA does not host a sensitive application or sensitive data, this section may be omitted.

Management Control Element	Y/N/P/NA	Effective?	Comments
A. FOR SENSITIVE APPLICATIONS ON THIS GSS or MA:			
(1). Is there a current and comprehensive list of all sensitive applications and/or sensitive databases hosted on the GSS or MA?			
(2). Is there a System Owner / Data Steward identified for each sensitive application and/or sensitive database?			
(3). Are there well documented, comprehensive and current contingency plans for each sensitive application and sensitive database?			
(4). Are there written procedures for backing up sensitive data files, for properly labeling them and keeping the separate from non-sensitive data?			
(5). Are there written procedures for controlling access to the back up files containing sensitive data?			

(6). Is there a formal Sensitive System Security Plan for each sensitive application and is it reviewed annually? (Note: This is required by OMB A-130, Departmental and Service policy but a Sensitive plan can be a component of a GSS or MA security plan and need not be a separate document.)			
(7). Is sensitive information removed from on-line storage before equipment is turned over for maintenance or is maintenance accomplished by a bonded agent authorized to by contract to deal with repair or destruction of sensitive media?			
(8). When an employee terminates, are all accesses to sensitive information removed immediately?			
(9). Are all storage media containing sensitive information clearly labeled and identifiable from non-sensitive media? This can be in the form of physical labels for removable media or access controls for internal media.			
(10). Are there appropriate "erase" utilities used to remove sensitive information from magnetic media when necessary? Standard delete functions are not adequate for this purpose.			
(11). If the transfer of sensitive information is allowed over either a local area network or a wide area network, including the Internet and intranet, are there procedures in place to ensure proper delivery?			
(12). Is data encryption available and used for the storage and/or transmission of sensitive information?			
(13). Are all personnel dealing with sensitive information properly trained and aware of the handling restrictions for such data?			
(14). Are audit trails utilized to ensure that sensitive information is not improperly accessed, copied or archived?			
(15). Does the sensitive application provide a warning to all users at the time of initial access that the application processes sensitive information and use is restricted to authorized personnel?			
(16). Has the sensitive application been certified within the last three years?			

VIII. Telecommunications. Telecommunications, in the case of an Internal PBX or other kind of managed telephone network is considered a General Support System and requires certification as such. A complete checklist would be completed as appropriate.

Management Control Element	Y/N/P/NA	Effective?	Comments
A. ALL GENERAL SUPPORT SYSTEMS MUST INCLUDE THOSE COMPONENTS OF TELECOMMUNICATIONS NECESSARY FOR THE OPERATION OF THE GSS or MA. (IE: MODEMS, DIAL-UP AND CABLE CONNECTIONS, ETC.)			
(1). Is an inventory of all telecommunications equipment maintained and is it current?			

(2). Is a telecommunications planning process in place that deals with short and long term requirements to ensure support for the Service mission, user needs, and overall goals and objectives?			
(3). Do plans include cost/benefit analyses and budget alternatives?			
(4). Do plans address GSS or MA and communication security?			
(5). Is the responsibility for telecommunications management clearly defined and assigned?			
(6). Are all external access points to the GSS or MA protected by appropriate procedures and/or technology?			
(7). Is the present telecommunications/ network configuration documented and current to the degree necessary to ensure continuity of operations?			
(8). Are there adequate safeguards in place to prevent unauthorized access to Government communications and computing resources.			
(9). Are there disaster recovery (contingency) plans in place to prevent or mitigate loss of telecommunications capability?			
(10). Are voice and data services clearly defined and integrated to the maximum practical extent?			
(11). Is there a Telephone Acquisition plan?			
(12). Is the telephone system configuration documented and updated on a regular basis?			
(13). Is an inventory of local circuits, government and commercial, maintained and updated at least annually?			
(14). Are station message detail records and call detail records reviewed periodically to ensure unauthorized use is minimized?			
(15). Is the issuance of FTS2000 Federal Calling Cards and number controlled.			
(16). Is the policy on authorized and unauthorized use of the telephone published and disseminated to all affected employees?			
(17). Are employees aware that government telephones, including voice mail, are not private and that conversations and voice mail may be monitored, intercepted, or other wise affected if necessary?			
(18). Is there adequate control of the telephone wiring closets, switch rooms and other components?			
(19). Are the provisions for the hearing impaired adequate? Are access numbers of the telecommunications devices for the deaf (TDD) published in Service directories?			

IX. Radio System Controls

Management Control Element	Y/N/P/NA	Effective?	Comments
A. THE SERVICE RADIO PROGRAM SHOULD BE TREATED AS A GSS or MA AND THE FOLLOWING QUESTIONS ANSWERED ONCE FOR ALL UNLESS SPECIFIC EXCEPTIONS ARE NOTED BY THE NATIONAL RADIO MANAGER			
(1). Has an individual been designated as the radio liaison for the Service, to deal with all matters pertaining to radio communications and frequency management? (377 DM 1.5H and 377 DM 1.3)			
(2). Do long range plans for radio systems include a budget proposal for replacement costs, operating expenses and future expansion?			
(3). Are radio system files documented and up-to-date? Are radio frequency assignments current, reflecting the actual installed configuration?			

X. Segregation of Duties

Management Control Element	Y/N/P/NA	Effective?	Comments
(1). Are sensitive functions divided among different individuals?			
(2). Are distinct systems support functions performed by different individuals?			
(3). Is there separation of duties between security personnel who administer access control functions and those who administer auditing functions?			
(4) Where functions cannot be segregated, are there compensating controls established for review of system administration and security administration work by knowledgeable staff?			