Program Memorandum Intermediaries/Carriers

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal AB-02-081 **Date: JUNE 11, 2002**

CHANGE REQUEST 2189

SUBJECT: Core Security Requirements (CSR) and Associated Responsibilities

This Program Memorandum (PM) provides instructions for identifying CSR responsibilities as related to completion of the Contractor Assessment Tool for FY 02. The CSRs are identified in the CMS Business Partners System Security Manual, Appendix A – CMS Core Security Requirements and the Contractor Assessment Security Tool (CAST). This PM applies to all standard system maintainers, carriers, intermediaries, their data centers, durable medical equipment regional carriers, and coordination of benefits contractors.

The CMS's review of the FY 01 CAST submissions from carriers, intermediaries, standard system maintainers, and data centers revealed that there is confusion among Medicare contractors as to the applicability of some CSRs. A workgroup of systems security staff was convened from the consortia, the Medicare contractor community, and our technical assistance contractor, Northrup Grumman Information Technology to analyze and make recommendations as to which CSRs must be addressed in the CAST submissions of carriers, intermediaries, standard system maintainers and data centers. The CMS has reviewed and concurred with these recommendations. In view of the rapidly approaching deadlines for completing the FY 02 CAST, you may wish to consider working directly from the attached report (Gap Responsibilities), which identifies the CSRs and their applicability to CMS Business Partners.

Security Questions and Concerns

The CMS expects that you may have questions or concerns about this PM. You may send them to ContractorSystemsSecurity@cms.hhs.gov. We will provide a prompt response as well as posting it to a Frequently Asked Questions section on the CMS Medicare Contractor Information Systems Security Web page. The address is: www.hcfa.gov/extpart.

Attachment

The *effective date* for this PM is June 11, 2002.

The *implementation date* for this PM is June 11, 2002.

These instructions should be implemented within your current operating budget.

This PM may be discarded after May 31, 2003.

If you have any questions, contact Peter Koza at (410) 786-2630.

CMS-Pub. 60AB

Gap Responsibilities

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.1.1	Security training includes: (1) awareness training; (2) periodic security reminders; (3) user education concerning virus protection; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).	☑	☑	☑	☑	☑	☑
1.1.2	Security skill needs are accurately identified and included in job descriptions and CMS Business Partners meet these requirements.	☑	☑	☑	☑	☑	☑
1.1.3	All Medicare employees and contractor personnel are provided security awareness training prior to being allowed access to sensitive information or Medicare data, and then are provided annual security refresher training. The training is customized based on job responsibilities.	☑	☑	☑	☑	☑	☑
1.1.4	Security training is adjusted to the level of the employee's responsibilities.	☑	☑	☑	☑	☑	☑
1.1.5	The employees acknowledge, in writing, having received the security and awareness training.	☑	☑	☑	☑	☑	☑
1.1.6	A record of the security awareness training subject(s) covered is maintained.	☑	☑	☑	☑	☑	☑
1.1.7	Employees are trained so that they are aware of the restrictions against unauthorized activities and accesses, including the illegal copying of data or software.	☑	☑	☑	☑	☑	☑
1.1.8	Training in emergency procedures is conducted at least once a year.	☑	☑	☑	☑	☑	☑
1.1.9	Policy and training exists to assure that copyright information is protected in accordance with the conditions under which the information is provided.	☑	☑	☑	☑	☑	☑
1.2.1	Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.	☑	☑	☑	☑	☑	☑
1.3.1	Agencies transmitting (FTI) from a main frame computer to another computer, need only identify the: (1) bulk records transmitted; (2) approximate number of taxpayer records; (3) date of the transaction; (4) description of the records; and (5) name of the individual making/receiving the transmission. (This CSR applies to COBs only.)	☐	☐	☐	☐	☐	☐ ***This is a COB contractor requirement only.***
1.3.2	Sensitive information, other than that on magnetic tape files, disclosed outside the CMS Business Partner's system is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.	☑	☑	☑	☑	☑	☑
1.3.3	Appropriate controls are established for all sensitive data entering or leaving the facility. A system is employed that precludes erroneous or unauthorized transfer of data, regardless of media or format. Include controls that maintain a record for the logging of shipping and receipts and a periodic reconciliation of these records.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.3.4	A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.	☑	☑	☑	☑	☑	☑
1.3.5	All retired, discarded, or unneeded sensitive data is disposed in a manner that prevents unauthorized persons from using it. All sensitive data is erased from storage media before releasing as work tapes or disks. Ensure the destruction of any sensitive information hard copy documents when no longer needed.	☑	☑	☑	☑	☑	☑
1.3.6	Sensitive data and CMS Business Partner records (Part A and Part B claims and benefit check records) are stored on-site. When on-site storage is not available, commercial storage facilities are used that most closely meet Federal standards for agency records centers. (Obtain Federal standards on National Archives Record Administration [36 CFR part 1228 subpart K]).	☑	☑	☑	☑	☑	☑
1.3.7	Sensitive information is never disclosed to agents/contractors during disposal unless authorized by statute. Destruction of sensitive information is witnessed by an agency employee. However, an agency may elect to have the destruction certified by the contractor in the absence of agency participation.	☑	☑	☑	☑	☑	☑
1.3.8	Before releasing files containing sensitive information to an individual or agency or contractor not authorized access to sensitive information, care is taken to remove all such sensitive information. Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a log is used to document that all discarded or transferred items are examined for sensitive information and this information is cleared before the items are released.	☑	☑	☑	☑	☑	☑
1.3.9	FTI is physically destroyed by authorized personnel, or returned to the originator, or to the system security administrator.	☐	☐	☐	☐	☐	☐ ***This is a COB contractor requirement only.***
1.3.10	Users of FTI are required to take certain actions upon completion of use of FTI (see Section 8 of IRS Publication 1075) in order to protect its confidentiality. When FTI information is returned to CMS a receipt process is used.	☐	☐	☐	☐	☐	☐ ***This is a COB contractor requirement only.***
1.3.11	Destruction methods for sensitive information are as follows: (1) burning - the material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (2) mulching or pulping - all material is reduced to particles one inch or smaller; (3) shredding or disintegrating - paper is shredded to effect 5/16 inch wide or smaller strips, and microfilm is shredded to 1/35 - inch by 3/8 - inch strips.	☑	☑	☑	☑	☑	☑
1.3.12	Inventory records of magnetic media containing sensitive information are maintained for purposes of control and accountability. Hardcopy printout of a tape or file is recorded in a log that identifies the contents, date received, number of records, and the reel/cartridge control number. If disposed of, the date and method of disposal is recorded. All deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	☑	☑	☑	☑	☑	☑
1.3.13	Semiannual inventories of removable storage devices and media containing sensitive information are performed.	☑	☑	☑	☑	☑	☑
1.3.14	Removable storage devices and media containing sensitive information are secured before, during, and after processing, and a proper acknowledgement form is signed and returned to the originator.	☑	☑	☑	☑	☑	☑
1.3.15	Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other magnetic media are labeled as CMS Sensitive Information. Magnetic media is kept in a secure area.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.4.1	Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; and (6) assuring that system users, including maintenance personnel, receive security awareness training.	☑	☑	☑	☑	☑	☑
1.4.2	To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self assessment is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self assessment is submitted to CMS.	☑	☑	☑	☑	☑	☑
1.4.3	Reporting Improper Inspections or Disclosures of Sensitive Information - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor, who contacts CMS for submission to the appropriate authority.	☑	☑	☑	☑	☑	☑
1.4.4	Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; and (3) rules that describe expected behavior of all with access to the system.	☑	☑	☑	☑	☑	☑
1.4.5	Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. The procedures: (1) stipulate what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.	☑	☑	☑	☑	☑	☑
1.4.6	Medicare information is not used in the contractor's private line of business unless authorized by CMS as consistent with the Privacy Act.	☑	☑	☑	☑	☑	☑
1.4.7	Employees are discouraged from browsing sensitive data files by making it clear that company policy prohibits it.	☑	☑	☑	☑	☑	☑
1.5.1	The system security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for: (1) information resource owners and users; (2) information resources management and data processing personnel; (3)) senior management; and (4) security administrators.	☑	☑	☑	☑	☑	☑
1.5.2	The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.	☑	☑	☑	☑	☑	☑
1.5.3	If a site has additional SSOs at various organizational levels, security actions are cleared through the primary SSO for Medicare records and operations.	☑	☑	☑	☑	☑	☑
1.5.4	The SSO is organizationally independent of IS operations.	☑	☑	☑	☑	☑	☑
1.5.5	The SSO assures compliance with CMS's systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) ensuring that internal controls are incorporated into new ADP information systems; (5) ensuring that systems security requirements are included in RFPs and subcontracts involving Medicare claims processing; (6) maintaining systems security documentation for review by CMS Regional Officer and/or Consortium; (7) consulting with the CCMO's designated security officer on systems security issues when there is a need for guidance or interpretation; and (8) keeping up with new/advanced systems security technology; (9) is a member of all planning groups, having the responsibility to subject all new systems/installations (and major changes) to the risk assessment process; and (10) makes certain that specialists such as auditors, lawyers, and building engineers address security issues before changes are made.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.5.6	The SSO in each CMS Business Partner organization is responsible for assisting Application System Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.	☑	☑	☑	☑	☑	☑
1.5.7	Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.	☑	☑	☑	☑	☑	☑
1.6.1	Procedures exist to identify and report incidents: (1) security incident procedures; (2) report procedures; and (3) response procedures.	☑	☑	☑	☑	☑	☑
1.6.2	The CMS Business Partner's incident response capability has the following characteristics: (1) an understanding of the CMS Business Partners being served; (2) educated information owners and users that trust the incident handling team; (3) a means of prompt centralized reporting; (4) response team members with the necessary knowledge, skills and abilities; and (5) links to other relevant groups.	☑	☑	☑	☑	☑	☑
1.7.1	CMS has categorized sensitive Medicare data, FTI, and Privacy Act-protected data as sensitive information. These items are to be protected under the CMS Level 3 - High Sensitivity security designation.	☑	☑	☑	☑	☑	☑
1.8.1	Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.	☑	☑	☑	☑	☑	☑
1.8.2	Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the system security plan.)	☑	☑	☑	☑	☑	☑
1.8.3	The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	☑	☑	☑	☑	☑	☑
1.8.4	A risk assessment is conducted whenever significant modifications are made to a system, facility, and network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (Disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (Policy, procedure, separating duties, training, posters/notices/ announcements, testing/validating/editing, audit routines, audit trails/logs, alarms and fire extinguishing equipment, computer system automatic controls, manual controls, good housekeeping, secure disposal, authorizing/restricting access, relocating operations/equipment/records, modifying building/work environment, backup/encryption, insurance/bonding and maintenance/repair/replacement).	☑	☑	☑	☑	☑	☑
1.8.5	Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	☑	☑	☑	☑	☑	☑
1.8.6	Major applications undergo independent review or audit at least every three years.	☑	☑	☑	☑	☑	☑
1.8.7	A compliance review and self assessment is conducted once a year.	☑	☑	☑	☑	☑	☑
1.8.8	Top management initiates prompt actions to correct deficiencies.	☑	☑	☑	☑	☑	☑
1.8.9	Major systems and applications are approved by the managers whose missions they support.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.8.10	Local Information System risk factors are assessed in accordance with NIST 800-12 Chapter 7.	☑	☑	☑	☑	☑	☑
1.8.11	Management analyzes local circumstances to determine space, container, and other security needs at individual facilities that meet or exceed the minimum protection requirements for the CMS Level 3 - High Sensitivity security designation.	☑	☑	☑	☑	☑	☑
1.9.1	The following are accomplished and documented: (1) security configuration documentation; (2) hardware/software installation and maintenance review and testing for security features; (3) inventory records; (4) security testing; and (5) virus checking.	☑	☑	☑	☑	☑	☑
1.9.2	Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	☑	☑	☑	☑	☑	☑
1.9.3	A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties and covers the topics prescribed by OMB Circular A-130 such as:(a) Rules of the system/Application rules; (b) Training/Specialized training; (c) Personnel controls/Personnel security; (d) Incident response capability; (e) Continuity of support/Contingency planning; (f) Technical security/Technical controls; (g) System interconnection/Information sharing; (h) Public access controls.	☑	☑	☑	☑	☑	☑
1.9.4	A system security plan has been prepared, in accordance with the CMS SSP Methodology, to cover every application and system categorized as a Major Application (MA) or General Support System (GSS).	☑	☑	☑	☑	☑	☑
1.9.5	The Contractor System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10) authorization lists that include the designation of the individual responsible for handling security violations and each individual (or position title) responsible for individual assets; and (11) lists of other security records such as audit trails, logs, and visitor sign-in sheets.	☑	☑	☑	☑	☑	☑
1.9.6	Retention procedures are established for all CMS sensitive information.	☑	☑	☑	☑	☑	☑
1.9.7	Documentation is available to assure that the level of sensitivity and criticality designations of each system has been assigned and has been determined to be commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	☑	☑	☑	☑	☑	☑
1.9.8	Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	☑	☑	☑	☑	☑	☑
1.9.9	The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	☑	☑	☑	☑	☑	☑
1.9.10	The system security plan establishes a security management structure with adequate independence, authority and expertise.	☑	☑	☑	☑	☑	☑
1.10.1	For prospective employees, references are contacted and background checks performed.	☑	☑	☑	☑	☑	☑
1.10.2	Regular job duties or shift rotations are required for those personnel using sensitive information.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
1.10.3	Regularly scheduled vacations exceeding several days are required for those personnel using sensitive information.	☑	☑	☑	☑	☑	☑
1.10.4	Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.	☑	☑	☑	☑	☑	☑
1.10.5	Personnel reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position.	☑	☑	☑	☑	☑	☑
1.10.6	Confidentiality or security agreements are required for employees and contractors assigned to work with confidential information.	☑	☑	☑	☑	☑	☑
1.11.1	Disclosure of sensitive information is prohibited unless specifically authorized by statute.	☑	☑	☑	☑	☑	☑
1.12.1	The System Owner/Manager, System Maintainer, or Senior Management designee signs the SSP and certification package.	☑	☑	☑	☑	☑	☑
1.12.2	The safeguard selection decisions and the risk assessment reports submitted are carefully reviewed.	☑	☑	☑	☑	☑	☑
1.12.3	The CMS Business Partner is responsible for approving any necessary corrective action plans.	☑	☑	☑	☑	☑	☑
1.12.4	The CMS Business Partner's systems security certification is completed annually and is fully documented.	☑	☑	☑	☑	☑	☑
1.12.5	Formal chain of trust partner agreements (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged) are in place to cover all electronically exchanged data between the contractor and other partners.	☑	☑	☑	☑	☑	☑
1.13.1	Policy/Guideline on workstation use is available.	☑	☑	☑	☑	☑	☑
1.13.2	Policy states that employees are not permitted to bring their personally owned computers into the workplace.	☑	☑	☑	☑	☑	☑
1.13.3	All CMS-owned software (such as CAST) is secured at close of business or anytime that it is not in use. Manuals and diskettes or CD-ROMs are stored out of sight in desks or file cabinets.	☑	☑	☑	☑	☑	☑
1.13.4	If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	☑	☑	☑	☑	☑	☑
1.13.5	Policies will be established for controlling the use of laptops, notebooks and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.1.1	User account activity audits are conducted using automated audit controls.	☑	☑	☑	☑	☑	☑
2.1.2	Computers systems processing sensitive information are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing sensitive information is accountable.	☑	☑	☑	☑	☑	☑
2.1.3	All activity involving access to and modifications of sensitive or critical files is logged.	☑	☑	☑	☑	☑	☑
2.1.4	Access to audit logs is restricted.	☑	☑	☑	☑	☑	☑
2.1.5	The audit trail includes sufficient information to establish what events occurred and who or what caused them.	☑	☑	☑	☑	☑	☑
2.1.6	Audit logs are reviewed periodically and retained for the same period as the original claim.	☑	☑	☑	☐	☑	☑
2.1.7	All hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.	☐	☑	☑	☑	☑	☑
2.2.1	Physical Intrusion Detection Systems (IDS) are used for sensitive information in conjunction with other measures to provide forced entry protection for after-hours security. Alarms annunciate at an on-site protection console, a central station, or local police station. IDS include, but are not limited to: (1) door and window contacts; (2) magnetic switches; (3) motion detectors; and (4) sound detectors.	☑	☑	☑	☑	☑	☑
2.2.2	Sensitive information (including tapes or cartridges) are placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	☑	☑	☑	☑	☑	☑
2.2.3	Locking Systems for Secured Areas/Perimeters and Security Rooms - High security pin-tumbler cylinder locks are used that meet the following requirements: (1) key-oriented mortised or rim-mounted deadlock bolt; (2) dead bolt throw of one inch or longer; (3) double-cylinder design; (4) cylinders are to have five or more pin tumblers; (5) if bolt is visible when locked, it contains hardened inserts or is made of steel; and (6) both the key and the lock are "Off Master." Convenience type locking devices (card keys, sequence button activated locks, etc.) are authorized for use only during working hours. Keys to secured areas/perimeters are not in personal custody of an unauthorized employee and any combinations are stored in a security container.	☑	☑	☑	☑	☑	☑
2.2.4	Restricted areas are prominently posted and separated from non-restricted areas by physical barriers that control access. The main entrance to restricted areas is controlled/manned. Lesser entrances have cameras or electronic intrusion detection devices, such as card keys to monitor access.	☑	☑	☑	☑	☑	☑
2.2.5	Locked containers include the following features: (1) commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with locking drawers; and (2) locks must have built in key or hasp and lock.	☑	☑	☑	☑	☑	☑
2.2.6	Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new Authorized Access List (AAL) is issued monthly.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.2.7	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, or other evacuation procedures.	☑	☑	☑	☑	☑	☑
2.2.8	Transmission and Storage of Data - Sensitive information may be stored on hard disk only if CMS Business Partner approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades and are being used. Access control devices include: (1) password security; (2) audit trails; (3) encryption or guided media; (4) virus protection; and (5) data overwriting capabilities.	☑	☑	☑	☑	☑	☑
2.2.9	Unissued keys or other entry devices are secured.	☑	☑	☑	☑	☑	☑
2.2.10	Sensitive information is stored in security containers that have one of the following devices: (1) metal lateral key lock files; (2) metal lateral files equipped with lock bars on both sides and secured with security padlocks; (3) metal pull drawer cabinets with center or off-center lock bars secured by security padlocks; and (4) key lock "mini safes" properly mounted with appropriate key control.	☑	☑	☑	☑	☑	☑
2.2.11	If safes and/or vaults are used, they comply with: (1) safe - GSA approved container of Class I, IV and V and Underwriters Laboratories (UL) listing of TRTL-30, TXTL-60 and TRTL-60; and (2) vaults - hardened room that uses UL approved vault doors and meet GSA specifications.	☑	☑	☑	☑	☑	☑
2.2.12	Handling and Transporting Sensitive Information - Care is taken to safeguard sensitive information at all times. If hand carried, it is kept with an individual and protected from unauthorized disclosure. All shipments are documented on transmittal forms and monitored. All sensitive information transported through the mail or courier/messenger service is double sealed. Sensitive information is clearly labeled "CMS Sensitive Information."	☑	☑	☑	☑	☑	☑
2.2.13	Security rooms include the following features: (1) room is enclosed by slab-to-slab walls constructed of approved materials; (2) unless electronic intrusion detection devices are used, all doors entering the space are locked and strict key or combination control should be exercised; (3) door hinge pins must be non-removable or installed on the inside of the room; (4) any glass in doors or walls are security glass (a minimum of two layers of 1/8 inch plate glass with .060 [1/32] vinyl interlayer, normal thickness is 5/26 inch); (5) plastic glazing material is not acceptable; and (6) Vents or louvers are protected by Underwriters' Laboratory (UL) approved electronic detection system that will annunciate at a protection console.	☑	☑	☑	☑	☑	☑
2.2.14	Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.	☑	☑	☑	☑	☑	☑
2.2.15	Key combinations are changed when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.	☑	☑	☑	☑	☑	☑
2.2.16	All entry code combinations are changed periodically.	☑	☑	☑	☑	☑	☑
2.2.17	Workstation locations are secured.	☑	☑	☑	☑	☑	☑
2.2.18	Keys or other access devices are needed to enter the computer room and tape/media library.	☑	☑	☑	☑	☑	☑

It is recommended the Business Partner review section 4.3.1 of the Business Partner Systems Security Manual before answering CSRs 2.2.24, 2.2.25 and then 2.2.19 or 2.2.10. This will provide clarification as to the options available for protecting sensitive data. For example, CSR 2.2.19 is the security requirement if you have chosen security areas/perimeters as your mechanism for protection. The business partner may have chosen only to use containers in which case CSR 2.2.10 applies and CSR 2.2.19 would not apply.

CSR	SS	PartA	PartB	CWF	Dmerc	DC	
2.2.19	☑	☑	☑	☑	☑	☑	Secured area/perimeters (non-duty hours) are: (1) enclosed by slab-to-slab walls; (2) constructed of approved materials; (3) implemented by periodic inspection or other approved protection methods; and (4) any lesser type partition supplemented by UL approved electronic intrusion detection system. Unless intrusion detection devices are used, all doors entering the space are locked and strict key or combination control is exercised. In the case of a fence and gate, the fence has intrusion detection devices or is continually guarded or locked with intrusion alarms. The space is cleaned during duty hours in the presence of a regularly assigned employee. ***It is recommended the Business Partner review section 4.3.1 of the Business Partner Systems Security Manual before answering CSRs 2.2.24, 2.2.25 and then 2.2.19 or 2.2.10. This will provide clarification as to the options available for protecting sensitive data. For example, CSR 2.2.19 is the security requirement if you have chosen security areas/perimeters as your mechanism for protection. The business partner may have chosen only to use containers in which case CSR 2.2.10 applies and CSR 2.2.19 would not apply.***
2.2.20	☑	☑	☑	☑	☑	☑	Alternate work site equipment controls are: (1) only business partner owned computers and software are used to process, access, and store sensitive information; (2) specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the agency in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller, agency-owned equipment is locked in a storage cabinet or desk when not in use.
2.2.21	☑	☑	☑	☑	☑	☑	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.
2.2.22	☑	☑	☑	☑	☑	☑	Management regularly reviews the list of persons with physical access to sensitive facilities.
2.2.23	☑	☑	☑	☑	☑	☑	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.
2.2.24	☑	☑	☑	☑	☑	☑	Sensitive information in any form is protected during non-duty hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization. ***It is recommended the Business Partner review section 4.3.1 of the Business Partner Systems Security Manual before answering CSRs 2.2.24, 2.2.25 and then 2.2.19 or 2.2.10. This will provide clarification as to the options available for protecting sensitive data. For example, CSR 2.2.19 is the security requirement if you have chosen security areas/perimeters as your mechanism for protection. The business partner may have chosen only to use containers in which case CSR 2.2.10 applies and CSR 2.2.19 would not apply.***
2.2.25	☑	☑	☑	☑	☑	☑	All restricted areas used to protect sensitive information meet CMS criteria for secured area or security room, or provisions are made to store high security items in appropriate containers during non-duty hours. ***It is recommended the Business Partner review section 4.3.1 of the Business Partner Systems Security Manual before answering CSRs 2.2.24, 2.2.25 and then 2.2.19 or 2.2.10. This will provide clarification as to the options available for protecting sensitive data. For example, CSR 2.2.19 is the security requirement if you have chosen security areas/perimeters as your mechanism for protection. The business partner may have chosen only to use containers in which case CSR 2.2.10 applies and CSR 2.2.19 would not apply.***
2.2.26	☑	☑	☑	☑	☑	☑	Unauthorized personnel are denied access to areas containing sensitive information during duty hours. Methods include use of restricted areas, security rooms, and locked doors.
2.2.27	☑	☑	☑	☑	☑	☑	Procedures exist for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.2.28	Security procedures are documented for bringing hardware and software into and out of the facility and for maintaining a record of those items.	☑	☑	☑	☑	☑	☑
2.3.1	An analysis of the logical access paths is performed whenever changes to the system are made.	☑	☑	☑	☑	☑	☑
2.4.1	Access control implementation includes a procedure for emergency access and at least one of the following features: (a) context-based access; (b) role-based access; (c) user-based access.	☑	☑	☑	☑	☑	☑
2.4.2	Emergency and temporary access authorizations are: (1) documented on standard forms and maintained on file; (2) approved by appropriate managers; (3) securely communicated to the security function and; (4) automatically terminated after a predetermined period.	☑	☑	☑	☑	☑	☑
2.5.1	To meet functional and assurance requirements, the operating security features of sensitive information systems must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to sensitive information.	☑	☑	☑	☑	☑	☑
2.5.2	Classifications and criteria have been established and communicated to resource owners.	☑	☑	☑	☑	☑	☑
2.5.3	Only employees with "need-to-know" are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	☑	☑	☑	☑	☑	☑
2.5.4	Sensitive information is kept separate from other information to the maximum extent possible. Files are clearly labeled to indicate that sensitive information is included. If sensitive information is recorded on removable storage devices or media with other data, it is protected as if it were entirely sensitive information. Computer access is restricted to authorized individuals.	☑	☑	☑	☑	☑	☑
2.5.5	Every personnel position is designated with a sensitivity level and documentation supports security and suitability standards that are being met by all personnel commensurate with their position sensitivity level, and that they are subject to personnel investigation requirements.	☑	☑	☑	☑	☑	☑
2.5.6	An independent review or audit of the security controls of all major systems processing sensitive information is performed at least every three years.	☑	☑	☑	☑	☑	☑
2.5.7	CMS Business Partner office facilities processing sensitive information are subjected to an annual "self assessment."	☑	☑	☑	☑	☑	☑
2.5.8	Inspection reports, including self-assessment reports and corrective actions, are to be retained for a minimum of three years from the date of the inspection.	☑	☑	☑	☑	☑	☑
2.5.9	Security systems on sensitive information systems are tested annually to assure that they are functioning correctly.	☑	☑	☑	☑	☑	☑
2.5.10	Sensitive information system design and test documentation are available, including security mechanisms and implementation.	☑	☑	☑	☑	☑	☑
2.5.11	Sensitive information system documentation contains the test policy, test plan, test procedures, and retest procedures, and it describes how and what mechanisms were tested, and the results.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.6.1	Security violations and activities, including failed logon attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software as required by FISCAM section 4.2. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	☑	☑	☑	☑	☑	☑
2.6.2	Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.	☑	☑	☑	☑	☑	☑
2.6.3	Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including contractor employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.	☑	☑	☑	☑	☑	☑
2.7.1	Resources are classified based on risk assessments. Classifications are documented and approved by an appropriate senior official, and are periodically reviewed.	☑	☑	☑	☑	☑	☑
2.7.2	Access to sensitive information is on a strictly "need-to-know" basis. Contractors evaluate the need for the sensitive information before the data is requested or disseminated.	☑	☑	☑	☑	☑	☑
2.8.1	Security is notified immediately when system users are terminated or transferred.	☑	☑	☑	☑	☑	☑
2.8.2	All changes to security profiles by security managers are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	☑	☑	☑	☑	☑	☑
2.8.3	Security managers review access authorizations and discuss any questionable authorizations with resource owners.	☑	☑	☑	☑	☑	☑
2.8.4	The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners.	☑	☑	☑	☐	☑	☑
2.8.5	Owners periodically review access authorization listings and determine whether they remain appropriate.	☑	☑	☑	☑	☑	☑
2.8.6	Authorization lists and controls for restricted areas, such as the computer room, tape library, and workstation rooms, are maintained. Authorization lists show the following information: (1) who is authorized access to restricted areas; (2) who is authorized to operate the equipment; (3) which workstations are authorized to access the computer and computer records; and (4) who may maintain operating systems, utilities, and operational versions of application programs. A separate authorization list is maintained that designates who is authorized access in emergencies and what limits are placed on their activities.	☑	☑	☑	☑	☑	☑
2.8.7	Warning banners advising safeguard requirements for sensitive information are used for computer screens that process sensitive information.	☑	☑	☑	☑	☑	☑
2.8.8	Documented policies and procedures exist for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.	☑	☑	☑	☑	☑	☑
2.8.9	Access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.9.1	Attempts to log on with invalid passwords are limited to 3 attempts.	☑	☑	☑	☑	☑	☑
2.9.2	Use of names or words as passwords is prohibited.	☑	☑	☑	☑	☑	☑
2.9.3	Users maintain possession of their individual tokens, key cards, etc., and understand that they do not loan or share these with others, and report lost items immediately.	☑	☑	☑	☑	☑	☑
2.9.4	The use of passwords and access control measures are in place to identify who accessed protected information and limit that access to persons with a need to know.	☑	☑	☑	☑	☑	☑
2.9.5	When remotely accessing (from a location not directly connected to the LAN) databases containing sensitive information: (1) Authentication is provided through ID and password encryption for use over public telephone lines; (2) Standard access is provided through a toll-free number and through local telephone numbers to local data facilities; and (3) Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user. Smart cards should have both identification and authentication features and provide data encryption as well.	☑	☑	☑	☑	☑	☑
2.9.6	Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), (d) telephone callback procedure, or (e) token.	☑	☑	☑	☑	☑	☑
2.9.7	Password files are encrypted.	☑	☑	☑	☑	☑	☑
2.9.8	Vendor-supplied passwords are replaced immediately.	☑	☑	☑	☑	☑	☑
2.9.9	Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	☑	☑	☑	☑	☑	☑
2.9.10	Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed periodically--every 30 to 90 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least six alphanumeric characters in length and prohibited from reuse for at least 6 generations.	☑	☑	☑	☑	☑	☑
2.9.11	Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords will be utilized where supported by existing operating systems.	☑	☑	☑	☑	☑	☑
2.9.12	Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.	☑	☑	☑	☑	☑	☑
2.10.1	Security software is used to restrict access. Access to security software is restricted to security administrators only.	☑	☑	☑	☑	☑	☑
2.10.2	Security administration personnel set parameters of security software to provide access as authorized and restrict assess that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files and operating system files. Standardized naming conventions are used for resources.	☐	☐	☐	☑	☐	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC	
2.10.3	Updating of data is restricted to authorized employees.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.10.4	Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, uncatalog, scratch, and rename a file.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.10.5	Inactive users accounts are monitored and removed when not needed.	☑	☑	☑	☑	☑	☑	
2.11.1	Access to security profiles in the Data Dictionary and security tables in the DBMS is limited.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.11.2	Access and changes to DBMS software are controlled.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.11.3	Use of DBMS utilities is limited.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.11.4	Database management systems (DBMS) and data dictionary controls have been implemented that: (1) restrict access to data files at the logical data view, field and field-value level; (2) control access to the data dictionary using security profiles and passwords; (3) maintain audit trails that allow monitoring of changes to the data dictionary and; (4) provide inquiry and update capabilities from application program functions, interfacing DBMS or data dictionary facilities.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.12.1	Access to sensitive information is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.	☑	☑	☑	☑	☑	☑	
2.12.2	Medicare data is not released to outside personnel unless their identity is verified.	☑	☑	☑	☑	☑	☑	
2.13.1	Security managers investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	☑	☑	☑	☑	☑	☑	
2.13.2	Violations are summarized and reported to senior management.	☑	☑	☑	☑	☑	☑	
2.13.3	Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	☑	☑	☑	☑	☑	☑	
2.13.4	Any missing tape containing sensitive information is accounted for by documenting search efforts and the initiator is notified of the loss.	☑	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***

CSR		SS	PartA	PartB	CWF	Dmerc	DC
2.14.1	Standard forms are used to document approval for archiving, deleting, and sharing data files.	☑	☑	☑	☑	☑	☑ ***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
2.14.2	Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	☑	☑	☑	☑	☑	☑ ***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
3.1.1	Policy defines investigation of inappropriate or unusual activity and guidelines for appropriate actions to be taken.	☑	☑	☑	☑	☑	☑
3.1.2	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	☑	☑	☑	☑	☑	☑
3.1.3	The use of privileged system software and utilities is reviewed by technical management.	☑	☑	☑	☑	☑	☑
3.1.4	Systems programmers' activities are monitored and reviewed.	☑	☑	☑	☑	☑	☑
3.1.5	Systems support alarm features to provide immediate notification of predefined events.	☑	☑	☑	☑	☑	☑
3.2.1	Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.	☑	☑	☑	☑	☑	☑
3.2.2	Responsibilities for monitoring use are defined and understood by technical management.	☑	☑	☑	☑	☑	☑
3.2.3	Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	☑	☑	☑	☑	☑	☑
3.2.4	The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	☑	☑	☑	☑	☑	☑
3.3.1	Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.	☑	☑	☑	☑	☑	☑
3.3.2	Policies and procedures for restricting access to systems software exist and are up-to-date.	☑	☑	☑	☑	☑	☑
3.3.3	The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	☑	☑	☑	☑	☑	☑
3.3.4	Justification and management approval for access to systems software is documented and retained.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
3.4.1	Installation of all system software is logged to establish an audit trail and reviewed by data center management.	☑	☑	☑	☑	☑	☑
3.4.2	Migration of tested and approved system software to production use is performed by an independent library control group.	☑	☑	☑	☑	☑	☑
3.4.3	Vendor-supplied system software is supported by the vendor.	☑	☑	☑	☑	☑	☑
3.4.4	Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	☑	☑	☑	☑	☑	☑
3.4.5	Outdated versions of system software are removed from production libraries.	☑	☑	☑	☑	☑	☑
3.4.6	All system software is current and has current and complete documentation.	☑	☑	☑	☑	☑	☑
3.5.1	New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation.	☑	☑	☑	☑	☑	☑
3.5.2	Policies and procedures exist and are up-to-date for identifying, selecting, installing and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	☑	☑	☑	☑	☑	☑
3.5.3	Procedures exist for identifying and documenting system software problems. This includes: (1) using a log to record the problem; (2) the name of the individual assigned to analyze the problem; and (3) how the problem was resolved.	☑	☑	☑	☑	☑	☑
3.5.4	New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	☑	☑	☑	☑	☑	☑
3.5.5	Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time.	☐	☑	☑	☑	☑	☑
3.5.6	Procedures exist for controlling emergency changes. These procedures include: (1) authorizing and documenting emergency changes as they occur, (2) reporting the changes for management review, and (3) review of the changes by an independent IT supervisor.	☑	☑	☑	☑	☑	☑
3.6.1	All accesses to system software files are logged by automated logging facilities.	☑	☑	☑	☑	☑	☑
3.6.2	Vendor-supplied default login IDs and passwords have been disabled.	☑	☑	☑	☑	☑	☑
3.6.3	Remote access to the system master console is restricted. Physical and logical controls provide security over all workstations that are set up as master consoles.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
3.6.4	Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.	☑	☑	☑	☑	☑	☑
3.6.5	The operating system is configured to prevent circumvention of the security software and application controls.	☑	☑	☑	☑	☑	☑
3.6.6	The operating system's operational status and restart integrity is protected during and after shutdowns.	☑	☑	☑	☑	☑	☑
4.1.1	Application run manuals provide instruction on operating specific applications.	☑	☑	☑	☑	☑	☑
4.1.2	Operators are prevented from overriding file labels or equipment error messages.	☐	☑	☑	☑	☑	☑
4.1.3	Detailed, written instructions exist to guide personnel in performing their duties. Computer operator manuals provide guidance on system startup and shut down procedures, emergency procedures, system and job status reporting, and operator prohibited activities. Application-specific manuals provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.	☐	☑	☑	☑	☑	☑
4.1.4	The approval process includes review of the impact of new systems and system changes on security procedures and separation of duties.	☑	☑	☑	☑	☑	☑
4.1.5	Duties in critical control and financial functions are split. (e.g., establish special controls involving more than one person over blank and voided checks.)	☐	☑	☑	☑	☑	☑
4.2.1	All operator activities on the computer system are recorded on an automated history log.	☑	☑	☑	☑	☑	☑
4.2.2	Personnel are provided adequate supervision and review, including each shift of computer operations.	☑	☑	☑	☑	☑	☑
4.2.3	System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.	☐	☑	☑	☑	☑	☑
4.2.4	Supervisors routinely review the history log and investigate any abnormalities.	☑	☑	☑	☑	☑	☑
4.3.1	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	☑	☑	☑	☑	☑	☑
4.3.2	Documented job descriptions include definitions of the technical knowledge, skills and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	☑	☑	☑	☑	☑	☑
4.4.1	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
4.4.2	Staff's performance is monitored and controlled to ensure that objectives laid out in job descriptions are carried out.	☑	☑	☑	☑	☑	☑
4.5.1	Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	☑	☑	☑	☑	☑	☑
4.6.1	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	☑	☑	☑	☑	☑	☑
4.6.2	Local policy assigns senior management responsibility for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced and institutionalized within the organization.	☑	☑	☑	☑	☑	☑
4.6.3	Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood and followed.	☑	☑	☑	☑	☑	☑
4.7.1	Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	☑	☑	☑	☑	☑	☑
4.7.2	Management has analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. No individual has complete control over incompatible transaction processing functions.	☑	☑	☑	☑	☑	☑
4.7.3	Data processing personnel are not users of information systems. They and security managers do not initiate, input and correct transactions.	☐	☑	☑	☑	☑	☑
4.7.4	Policies and procedures for segregating duties exist and are up-to-date.	☑	☑	☑	☑	☑	☑
4.7.5	Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	☑	☑	☑	☑	☑	☑ ***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
4.7.6	Distinct systems support functions are performed by different individuals, including: (1) IS management; (2) system design; (3) application programming; (4) systems programming; (5) quality assurance/testing; (6) library management/change management; (7) computer operations; (8) production control and scheduling; (9) data control; (10) data security; (11) data administration; and (12) network administration.	☑	☑	☑	☑	☑	☑
5.1.1	Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and their operating procedures exist and are known.	☑	☑	☑	☑	☑	☑
5.1.2	Any behavior that may damage computer equipment is prohibited.	☑	☑	☑	☑	☑	☑
5.1.3	Controls have been implemented to mitigate other disasters, such as floods, earthquakes and fire.	☑	☑	☑	☑	☑	☑
5.1.4	Environmental controls are periodically tested.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
5.1.5	Redundancy exists in the air cooling system.	☑	☑	☑	☑	☑	☑
5.1.6	Fire suppression and prevention devices have been installed and are working (e.g., smoke detectors, fire extinguishers and sprinkler systems).	☑	☑	☑	☑	☑	☑
5.1.7	An uninterruptible power supply or backup generator has been provided so that power is adequate for orderly shut down.	☑	☑	☑	☑	☑	☑
5.2.1	The Contingency Plan provides for backup personnel so that it can be implemented independent of specific individuals.	☑	☑	☑	☑	☑	☑
5.2.2	User departments have developed adequate manual processing procedures for use until automated operations are restored.	☑	☑	☑	☑	☑	☑
5.2.3	The Contingency Plan clearly assigns responsibilities for recovery.	☑	☑	☑	☑	☑	☑
5.2.4	Contingency Plan consists of all components listed in the Business Partners Systems Security Manual.	☑	☑	☑	☑	☑	☑
5.2.5	Management and the SSO approve Contingency Plans.	☑	☑	☑	☑	☑	☑
5.2.6	Management and the SSO are able to show how the organization responds to specific disasters/disruptions to (1) protect lives, (2) limit damage , (3) protect sensitive data, (4) circumvent safeguards according to established bypass procedures and (5) minimize the impact on Medicare operations.	☑	☑	☑	☑	☑	☑
5.2.7	The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	☑	☑	☑	☑	☑	☑
5.2.8	Major modifications often have security ramifications that may indicate changes in other Medicare operations. Contingency plans are re-evaluated before proposed changes are approved.	☑	☑	☑	☑	☑	☑
5.2.9	Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	☑	☑	☑	☑	☑	☑
5.2.10	The Contingency Plan identifies the CMS Business Partner's critical interfaces that need to be established while recovering from a disaster.	☑	☑	☑	☑	☑	☑
5.3.1	A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.	☑	☑	☑	☑	☑	☑
5.4.1	System and application documentation are maintained at the off-site storage location.	☑	☑	☑	☑	☑	☑
5.4.2	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
5.4.3	The backup storage site is geographically removed from the primary site(s) and protected by environmental controls and physical access controls.	☑	☑	☑	☑	☑	☑
5.4.4	The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.	☑	☑	☑	☑	☑	☑
5.5.1	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	☑	☑	☑	☑	☑	☑
5.6.1	Data center staff have received training and understand their emergency roles and responsibilities.	☑	☑	☑	☑	☑	☑
5.6.2	Emergency procedures are documented.	☑	☑	☑	☑	☑	☑
5.6.3	Data center staff receive periodic training in emergency fire, water and alarm incident procedures.	☑	☑	☑	☑	☑	☑ ***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
5.6.4	Emergency procedures are periodically tested.	☑	☑	☑	☑	☑	☑
5.7.1	The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.	☑	☑	☑	☑	☑	☑
5.7.2	Contingency Plans are reviewed whenever new operations are planned or new safeguards contemplated.	☑	☑	☑	☑	☑	☑
5.7.3	Several copies of the current Contingency Plan are securely stored off-site at different locations, including homes of key staff members. It is reviewed once a year, reassessed and, if appropriate, revised to reflect changes in hardware, software and personnel.	☑	☑	☑	☑	☑	☑
5.7.4	Test results are documented and a report, such as a "lessons learned" report, is developed and provided to senior management.	☑	☑	☑	☑	☑	☑
5.7.5	The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	☑	☑	☑	☑	☑	☑
5.8.1	Resources supporting critical operations are identified and documented. Types of resources identified include: (1) computer hardware; (2) computer software; (3) computer supplies; (4) system documentation; (5) telecommunications; (6) office facilities and supplies; and (7) human resources.	☑	☑	☑	☑	☑	☑
5.9.1	Senior management periodically: (1) reviews and compares the service performance achieved with the goals; and (2) surveys user departments to see if their needs are being met.	☑	☑	☑	☑	☑	☑
5.9.2	Problems and delays encountered, including the reason and elapsed time for resolution of hardware problems, are recorded and analyzed to identify recurring patterns or trends.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
5.9.3	Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	☑	☑	☑	☑	☑	☑
5.9.4	Goals are established by senior management for the availability of data processing and on-line services.	☑	☑	☑	☑	☑	☑
5.9.5	Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	☑	☑	☑	☑	☑	☑
5.9.6	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance.	☐	☑	☑	☑	☑	☑
5.9.7	Records are maintained on the actual hardware performance in meeting service schedules.	☐	☑	☑	☑	☑	☑
5.9.8	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	☐	☑	☑	☑	☑	☑
5.9.9	Hardware maintenance policies and procedures exist and are up-to-date.	☐	☑	☑	☑	☑	☑
5.9.10	Regular and unscheduled hardware maintenance performed is documented.	☐	☑	☑	☑	☑	☑
5.9.11	Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	☐	☑	☑	☑	☑	☑
5.10.1	Arrangements and agreements have been established for a backup data center and other needed facilities that: (1) are in a state of readiness commensurate with the risks of interrupted operations; (2) have sufficient processing capacity and; (3) are available for use.	☑	☑	☑	☑	☑	☑
5.10.2	Alternate telecommunication services have been arranged.	☑	☑	☑	☑	☑	☑
5.10.3	Arrangements are planned for travel and lodging of necessary personnel, if needed.	☑	☑	☑	☑	☑	☑
5.11.1	A Contingency Plan is available for each standalone computer workstation that specifies where backup data and software are stored. A single plan can cover more than one workstation.	☑	☑	☑	☑	☑	☑
5.11.2	Standalone computer workstation backup data, software and current operating procedures are stored in accordance with the Contingency Plan.	☑	☑	☑	☑	☑	☑
5.12.1	The CMS Business Partner shall use virus identification, detection, protection, and elimination software.	☑	☑	☑	☑	☑	☑
6.1.1	Emergency changes are documented and approved by the operations supervisor, formally reported to computer operations management for follow-up and approved after the fact by programming supervisors and user management.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
6.1.2	Emergency change procedures are documented.	☑	☑	☑	☑	☑	☑
6.2.1	Clear policies restricting the use of personal and public domain software have been developed and are enforced.	☑	☑	☑	☑	☑	☑
6.3.1	Test plans are documented and approved that define responsibilities for each party involved.	☑	☑	☑	☑	☑	☑
6.3.2	Unit, integration and system testing are performed and approved in accordance with the test plan. A sufficient range of valid and invalid conditions are applied.	☑	☑	☑	☑	☑	☑
6.3.3	A comprehensive set of test transactions and data have been developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.	☑	☑	☑	☑	☑	☑
6.3.4	Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.	☑	☑	☑	☑	☑	☑
6.3.5	Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.	☑	☑	☑	☑	☑	☑
6.3.6	Program changes are moved into production only upon documented approval from users and system development management.	☑	☑	☑	☑	☑	☑
6.3.7	Test results are reviewed and documented.	☑	☑	☑	☑	☑	☑
6.3.8	Changes to detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	☑	☑	☑	☑	☑	☑
6.3.9	Test plan standards have been developed and are followed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).	☑	☑	☑	☑	☑	☑
6.3.10	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	☑	☑	☑	☑	☑	☑
6.3.11	A system development life cycle (SDLC) methodology has been developed that: (1) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (2) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (3) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements.	☑	☑	☑	☑	☑	☑
6.3.12	Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	☑	☑	☑	☑	☑	☑
6.3.13	Security policy assigns responsibility to Application System Managers for ensuring that appropriate administrative, physical and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.	☑	☑	☑	☑	☑	☑

CSR	SS	PartA	PartB	CWF	Dmerc	DC	
6.4.1	Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	☑	☑	☑	☑	☑	☑	
6.4.2	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	☐	☑	☑	☑	☑	☑	***Consideration should be given by Part A, B and D contractors as it may apply to mainframe, standard system, PC based or client-server application processes.***
6.4.3	Production source code is maintained in a separate archive library.	☑	☑	☐	☐	☐	☑	
6.4.4	Separate libraries are maintained for program development and maintenance, testing, and production programs.	☑	☑	☑	☑	☑	☑	
6.5.1	Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.	☑	☑	☑	☑	☑	☑	
6.5.2	Standardized procedures are used to distribute new software for implementation.	☑	☑	☑	☑	☑	☑	
6.6.1	Library management software is used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.	☑	☑	☑	☑	☑	☑	
6.7.1	Change requests are approved by both system users and data processing staff.	☑	☑	☑	☑	☑	☑	
6.7.2	Software change request forms are used to document requests and related approvals.	☑	☑	☑	☑	☑	☑	
6.8.1	Images of program code are maintained and compared before and after changes to ensure that only approved changes are made.	☑	☑	☑	☑	☑	☑	
6.8.2	A group independent of the user and programmers controls movement of programs and data among libraries.	☑	☑	☑	☑	☑	☑	
7.1.1	For batch application systems, a batch control sheet is prepared for a group of source documents and includes; date, control number, number of documents, a control total for a key field, and identification of the user submitting the batch.	☐	☑	☑	☐	☑	☑	
7.1.2	Access to blank documents (checks, claims forms, etc.) is restricted to authorized personnel.	☐	☑	☑	☐	☑	☐	
7.1.3	Source documents (checks, claims forms, etc.) are pre-numbered to maintain control over the documents. Key source documents require authorizing signatures.	☐	☑	☑	☐	☑	☑	
7.2.1	Before transactions are processed, they are verified using master files of approved vendors, employees, etc., as appropriate for the application.	☑	☑	☑	☑	☑	☑	

CSR		SS	PartA	PartB	CWF	Dmerc	DC
7.2.2	Master files and program code that does the verification are protected from unauthorized modification.	☑	☑	☑	☑	☑	☑
7.3.1	All transactions are logged as entered, along with the User ID of the person entering the data.	☑	☑	☑	☑	☑	☑
7.3.2	Each operator is required to use a unique password and identification code before being granted access to the system.	☑	☑	☑	☑	☑	☑
7.3.3	When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	☑	☑	☑	☑	☑	☑
7.3.4	Data entry workstations are connected to the system only during specific periods of the day, which corresponds with the business hours of the data entry personnel.	☑	☑	☑	☑	☑	☑
7.3.5	Each workstation automatically disconnects from the system when not used after a specific period of time.	☑	☑	☑	☑	☑	☑
7.3.6	Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	☑	☑	☑	☑	☑	☑
7.3.7	Data entry workstations are located in physically secure environments.	☑	☑	☑	☐	☑	☐
7.4.1	Authorization profiles for users limit what transaction data entry personnel can enter.	☑	☑	☑	☑	☑	☑
7.4.2	Authorization profiles for users or workstations limit what transactions can be entered from a given workstation.	☑	☑	☑	☑	☑	☑
7.5.1	Exceptions, based on parameters established by management, are reported for their review and approval.	☑	☑	☑	☑	☑	☑
7.6.1	Procedures are in place for a multilevel review of CMS sensitive input data before it is released for processing.	☑	☑	☑	☑	☑	☑
7.6.2	Data control unit personnel monitor data entry and processing of source documents.	☐	☑	☑	☐	☑	☑
7.6.3	Data control unit personnel verify that source documents are properly prepared and authorized.	☐	☑	☑	☐	☑	☑
8.1.1	Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	☑	☑	☑	☑	☑	☑
8.1.2	Sequence checking is used to identify missing or duplicate transactions.	☑	☐	☐	☐	☐	☐

CSR		SS	PartA	PartB	CWF	Dmerc	DC
8.1.3	Transactions without preassigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.	☑	☑	☑	☑	☑	☑
	When responding consider manual systems utilized such as correspondence, unsolicited reference, etc.						
8.1.4	Preassigned serial numbers on source documents are entered into the computer and used for sequence checking.	☐	☑	☑	☐	☑	☑
8.2.1	Reports of missing or duplicate transactions are produced and items are investigated and resolved in a timely manner.	☑	☑	☑	☑	☑	☑
8.2.2	Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate transactions.	☑	☑	☑	☑	☑	☑
8.2.3	For high-value, low volume items, individual transactions or source documents are compared with a detailed listing of items processed by the computer.	☑	☑	☑	☐	☑	☑
8.3.1	Reconciliations are performed to determine the completeness of transactions processed, master files updated and outputs generated.	☑	☑	☑	☑	☑	☑
8.4.1	Record counts and control totals are established over and entered with transaction data, and reconciled to determine the completeness of data entry.	☑	☑	☑	☑	☑	☑
8.4.2	Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.	☑	☑	☑	☑	☑	☑
8.4.3	Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	☑	☐	☐	☑	☐	☑
8.4.4	System interfaces require that the sending system's output control counts equal the receiving system's input counts.	☑	☑	☑	☑	☑	☑
8.4.5	A data processing control group receives and reviews control total reports and determines the completeness of processing.	☐	☑	☑	☑	☑	☑
8.5.1	For on-line or real time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness of data entry and processing.	☑	☑	☑	☐	☑	☑
8.5.2	User-prepared record count and control totals established over source documents are used to help determine the completeness of data entry and processing.	☐	☑	☑	☐	☑	☐
9.1.1	Errors are corrected by the user originating the transaction.	☐	☑	☑	☐	☑	☐
9.1.2	Error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	☑	☑	☑	☑	☑	☑
9.1.3	All corrections are reviewed and approved by supervisors before the corrections are reentered. (Based on Medicare operating environment CMS business partners may have other compensating controls in place.)	☐	☑	☑	☐	☑	☐

CSR	SS	PartA	PartB	CWF	Dmerc	DC
9.2.1 Effective use is made of automated entry devices to reduce the potential for data entry errors.	☑	☑	☑	☐	☑	☑
9.3.1 Rejected data are automatically written on an automated suspense file and held until corrected. Each erroneous transaction is annotated with: (1) codes indicating the type of data error; (2) date and time the transaction was processed and the error identified; and (3) the identity of the user who originated the transaction.	☑	☑	☑	☑	☑	☑
9.3.2 A control group is responsible for controlling and monitoring rejected transactions.	☐	☑	☑	☐	☑	☑
9.3.3 General controls effectively protect the suspense file from unauthorized access and modification.	☑	☑	☑	☐	☑	☑
9.3.4 The suspense file is purged of transactions as they are corrected.	☑	☐	☐	☐	☐	☐
9.3.5 Record counts and control totals are established over the suspense file and used in reconciling transactions processed.	☑	☑	☑	☑	☑	☐
9.3.6 The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected errors.	☐	☑	☑	☐	☑	☐
9.4.1 The source document is well-designed to aid the preparer and facilitate data entry . Transaction type and date field codes are preprinted on the source document.	☑	☑	☑	☑	☑	☑
9.5.1 Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.	☑	☑	☑	☐	☑	☑
9.6.1 Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design.	☑	☑	☑	☑	☑	☑
9.6.2 The computer system automatically checks the output message before displaying, writing, and printing to make sure the output has not reached the wrong workstation device. A connection must be established to a specific device (workstation, printer, etc.) and verified by the system before transmitting data.	☑	☑	☑	☑	☑	☑
9.6.3 The data processing control group, or some alternative, has a schedule by application that shows: (1) when outputs are completed; (2) when they need to be distributed; (3) who the recipients are; and (4) the copies needed. The group then reviews output products for general acceptability and reconciles control information to determine completeness of processing.	☐	☑	☑	☑	☑	☑
9.6.4 Printed reports contain a title page with report name, time and date of production, the processing period covered and an "end-of-report" message.	☑	☑	☑	☑	☑	☑
9.6.5 Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output.	☑	☑	☑	☑	☑	☑
9.6.6 Outputs transmitted to every terminal device in the user department are summarized daily, printed, and reviewed by the supervisors.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
9.6.7	A control log of output product errors is maintained, including the corrective actions taken.	☑	☑	☑	☑	☑	☑
9.6.8	Every output transmission to a user's terminal device is logged.	☑	☑	☑	☑	☑	☑
9.6.9	Output from reruns is subjected to the same quality review as the original output.	☑	☑	☑	☑	☑	☑
9.7.1	Users review output reports for data accuracy, validity, and completeness. The reports include error reports, transaction reports, master record change reports, exception reports and control totals balance reports.	☑	☑	☑	☐	☑	☑
9.8.1	The following are protected from unauthorized modifications: (1) Program code for data validation and editing and associated tables or files; (2) Program code and criteria for test of critical calculations; and (3) Exception criteria and the related program code. Programs perform limit and reasonableness checks on critical calculations.	☑	☑	☐	☐	☐	☑
9.8.2	Programmed validation and edits include checks for: (1) reasonableness; (2) dependency; (3) existence; (4) mathematical accuracy; (5) range; (6) check digit; (7) document reconciliation; (8)) relationship or prior data matching.	☑	☑	☑	☑	☑	☑
9.8.3	Validation and editing are performed at the computer workstation during data entry or are performed as early as possible in the data flow and before updating the master files. All data fields are checked for errors before rejecting a transaction.	☑	☑	☑	☐	☑	☑
9.9.1	Preformatted computer workstations screens are utilized and allow prompting for data to be entered and editing of data as it is entered.	☑	☑	☑	☑	☑	☑
10.1.1	An access list of personnel authorized to access a data center to process sensitive data is controlled.	☑	☑	☑	☑	☑	☑
10.1.2	Physical access to enclosures housing network equipment is restricted.	☑	☑	☑	☑	☑	☑
10.2.1	Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.	☑	☑	☑	☑	☑	☑
10.2.2	Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network.	☑	☑	☑	☑	☑	☑
10.2.3	Intrusion detection software is implemented providing real-time identification of unauthorized use, misuse, and abuse of computer assets by internal network users and external hackers.	☑	☑	☑	☑	☑	☑
10.3.1	Telephone numbers of the facsimile machines receiving sensitive information are verified before transmitting data.	☑	☑	☑	☑	☑	☑
10.3.2	When sending or receiving sensitive fax information, have a trusted staff member at both sending and receiving fax machines, or have a locked room for the fax machine with custodial coverage over outgoing and incoming transmissions.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
10.3.3	Policy exists identifying appropriate use of the E-mail system by employees, and procedures exist to enforce E-mail security, privacy, and message integrity	☑	☑	☑	☑	☑	☑
10.3.4	Security policy exists and audit reviews include checks, to assure that system administrators and others with special system level access privileges are prohibited from reading the E-mail messages of others unless authorized on a case by case basis by appropriate management officials.	☑	☑	☑	☑	☑	☑
10.3.5	Fax procedures for sensitive information require a cover sheet that explicitly provides guidance to the recipient, which includes: (1) Notification of sensitive data and need for protection, and (2) Notice to unintended recipients to telephone the sender, collect if necessary, to report the disclosure and confirm destruction of the information.	☑	☑	☑	☑	☑	☑
10.4.1	Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.	☑	☑	☑	☑	☑	☑
10.4.2	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.	☑	☑	☑	☑	☑	☑
10.5.1	Passwords are transmitted and stored using secure protocols and algorithms.	☑	☑	☑	☑	☑	☑
10.6.1	CMS Business Partner's Internet connections must be in accordance with the CMS Internet Security Policy. When a determination for Internet use has been made, it shall include at a minimum of Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems (CMS Internet Security Policy November 24, 1998).	☑	☑	☑	☑	☑	☑
10.7.1	Purchased software is used in accordance with contract agreements and copyright laws	☑	☑	☑	☑	☑	☑
10.7.2	Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software	☑	☑	☑	☑	☑	☑
10.7.3	A change-control mechanism that maintains control of changes to hardware, software, and security mechanisms is implemented.	☑	☑	☑	☑	☑	☑
10.8.1	Any connection to the internet, or other external networks or systems, occurs through a gateway/firewall.	☑	☑	☑	☑	☑	☑
10.8.2	Strong authentication is used to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; (3) grant access to the functions of critical network devices; (4) procedures for the above are documented.	☑	☑	☑	☑	☑	☑
10.8.3	The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.	☑	☑	☑	☑	☑	☑
10.8.4	Workstation with dial-up access generate a unique identifier code before connection is completed.	☑	☑	☑	☑	☑	☑
10.9.1	A plan is in place to assess the risks to the network.	☑	☑	☑	☑	☑	☑

CSR		SS	PartA	PartB	CWF	Dmerc	DC
10.9.2	A plan is developed for eliminating significant vulnerabilities.	☑	☑	☑	☑	☑	☑
10.9.3	A plan is developed for alerting, containing, and rebuffing a physical or cyber attack on the CMS Business Partner IS systems.	☑	☑	☑	☑	☑	☑
10.9.4	Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	☑	☑	☑	☑	☑	☑
10.10.1	Communication software has been implemented to verify workstation identifications in order to restrict access through specific workstations: (1) verify IDs and passwords for access to specific applications; (2) control access through connections between systems and workstations; (3) restrict an application's use of network facilities; (4) protect sensitive data during transmission; (5) automatically disconnect at the end of a session; (6) maintain network activity logs; (7) restrict access to table that define network options, resources, and operator profiles; (8) allow only authorized users to shutdown network components; (9) monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; (10) restrict in-house access to telecommunications software; (11) control changes to telecommunications software; (12) ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage and; (13) restrict and monitor access to telecommunications hardware or facilities.	☑	☑	☑	☑	☑	☑