PROGRAM	1583-S TERM: May 1, 2015 THRU April 30, 2015 plus 4 Option Periods															
			The Data Center		Data Intergrators		Midwest Direct MKTG		MPM Communications		NPC, Inc		Taylor/Progressive Impressions		World Marketing Group	
TITLE	Medicare Enrollement Packages and Medicare Cards		Salt Lake City, UT		Fredericksburg, VA		Cleveland, OH		Waldorf, MD		Claysburg, PA		Bloomington, IL		Dallas, TX	
		BASIS OF	UNIT		UNIT		UNIT		UNIT		UNIT		UNIT		UNIT	
ITEM NO.	DESCRIPTION	AWARD	RATE	COST	RATE	COST	RATE	COST	RATE	COST	RATE	COST	RATE	COST	RATE	COST
I.	**COMPLETE PRODUCT:**															
A	A: MEDICARE **DOMESTIC** INITIAL ENROLLMENT															
(1)	Makeready and/or Setup Charge . . . . . .per order	12	n/c	0.00	n/c	0.00	0.00	0.00	1000.00	12,000.00	600.00	7,200.00	226.50	2,718.00	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	2196	185.30	406,918.80	161.00	353,556.00	179.33	393,808.68	240.00	527,040.00	220.50	484,218.00	324.54	712,689.84	216.49	475,412.04
B	B: MEDICARE **PUERTO RICAN** INITIAL ENROLLMENT															
(1)	Makeready and/or Setup Charge . . . . . .per order	12	n/c	0.00	n/c	0.00	0.00	0.00	500.00	6,000.00	408.00	4,896.00	258.88	3,106.56	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	36	383.20	13,795.20	100.00	3,600.00	288.63	10,390.68	225.00	8,100.00	287.00	10,332.00	344.48	12,401.28	735.79	26,488.44
C	C: MEDICARE **FOREIGN** INITIAL ENROLLMENT															
(1)	Makeready and/or Setup Charge . . . . . .per order	12	n/c	0.00	n/c	0.00	0.00	0.00	500.00	6,000.00	410.00	4,920.00	98.63	1,183.56	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	12	836.40	10,036.80	164.00	1,968.00	525.57	6,306.84	400.00	4,800.00	411.05	4,932.60	701.77	8,421.24	1783.72	21,404.64
D	D: MEDICARE **ENGLISH** GENERAL ENROLLMENT															
(1)	Makeready and/or Setup Charge . . . . . .per order	1	n/c	0.00	n/c	0.00	0.00	0.00	5000.00	5,000.00	763.90	763.90	219.04	219.04	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	694	199.70	138,591.80	112.00	77,728.00	131.74	91,427.56	200.00	138,800.00	134.00	92,996.00	204.02	141,589.88	150.63	104,537.22
E	E: MEDICARE **SPANISH** GENERAL ENROLLMENT															
(1)	Makeready and/or Setup Charge . . . . . .per order	1	n/c	0.00	n/c	0.00	0.00	0.00	750.00	750.00	525.25	525.25	201.16	201.16	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	11	321.00	3,531.00	224.00	2,464.00	126.94	1,396.34	350.00	3,850.00	321.25	3,533.75	381.11	4,192.21	530.27	5,832.97
F	F: **REPLACEMENT** MEDICARE CARDS															
(1)	Makeready and/or Setup Charge . . . . . .per order	52	n/c	0.00	n/c	0.00	0.00	0.00	500.00	26,000.00	559.50	29,094.00	142.64	7,417.28	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	6084	119.60	727,646.40	45.00	273,780.00	32.14	195,539.76	53.00	322,452.00	66.00	401,544.00	82.75	503,451.00	70.99	431,903.16
G	G: **DEEMED** MEDICARE CARDS															
(1)	Makeready and/or Setup Charge . . . . . .per order	1	n/c	0.00	n/c	0.00	0.00	0.00	750.00	750.00	559.50	559.50	175.73	175.73	N/C	0.00
(2)	Running per 1,000 Copies . . . . . .per order	22	154.30	3,394.60	71.00	1,562.00	32.14	707.08	190.00	4,180.00	145.00	3,190.00	192.68	4,238.96	290.93	6,400.46
	CONTRACTORS TOTALS			**$1,303,914.60**		**$714,658.00**		**$699,576.94**		**$1,065,722.00**		**$1,048,705.00**		**$1,402,005.74**		**$1,071,978.93**
	DISCOUNT		**0.00%**	**$0.00**	**2.00%**	**$14,293.16**	**5.00%**	**$34,978.85**	**3.00%**	**$0.00**	**0.25%**	**$2,621.76**	**0.00%**	**$0.00**	**1.00%**	**$10,719.79**
	DISCOUNTED TOTALS		**NET**	**$1,303,914.60**	**20 days**	**$700,364.84**	**20 days**	**$664,598.09**	**15 days**	**$1,065,722.00**	**20 days**	**$1,046,083.24**	**NET**	**$1,402,005.74**	**20 days**	**$1,061,259.14**
							AWARDED									

U.S. GOVERNMENT PUBLISHING OFFICE GPO

COLUMBUS REGIONAL PRINTING
PROCUREMENT OFFICE
1335 Dublin Road, Suite 112-B
Columbus, OH 43215-7034
www.gpo.gov

April 10, 2015

Dear Bidder:

This is Amendment No. 1. The specifications in our invitation for bids on Program 1583-S, scheduled for opening at 2 p.m., March 18, 2015, are amended as follows. The bid opening date is not extended.

On page 2 of the contract specifications, under "QUALITY ASSURANCE LEVELS AND STANDARDS", delete "P-10. Process Color Match…Prior-to-Production Samples".

On page 24 of the contract specifications, under "PROOFS", under the first paragraph, replace "1 set of PDF "Soft" Proofs" with "1 set of PDF Proofs or 2 sets of Content Proofs as described below".

On page 24 of the contract specifications, under "PROOFS", at the beginning of the second paragraph, add "PDF PROOFS FOR G. DEEMED MEDICARE CARDS ONLY:"

On page 24 of the contract specifications, before the third paragraph, insert the following:

> CONTENT PROOFS FOR ALL PIECES EXCEPT G. DEEMED MEDICARE CARDS: All pieces of all items except Deemed Medicare Cards require two sets of digital color content proofs. Direct to plate must be used to produce the final product with a minimum resolution of 2400 x 2400 dpi.
>
> Proofs must be created using the same Raster Image Processor (RIP) that will be used to produce the product. Proofs shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed and folded to the finished size of the product, as applicable.
>
> Pantone colors may be substituted with a similar color (with the exception of process yellow) but may not be built out of the four process colors. This requirement does not apply to inkjet proofs.
>
> Contractor may be required to submit ink draw downs on actual production stock of Pantone color(s) used on the product.

On page 26 of the contract specifications, under the third paragraph, after "pages 13 to 21.", insert "All letters shall use White Writing, basis size 17 x 22", 20 lbs. per 500 sheets, equal to JCP Code D10", as follows:

ITEM	LOCATION
A. MEDICARE DOMESTIC INITIAL ENROLLMENT PACKAGE	Page 14, under "Letter"
B. MEDICARE PUERTO RICAN INITIAL ENROLLMENT PACKAGE	Page 15, under "Letter"
C. MEDICARE FOREIGN INITIAL ENROLLMENT PACKAGE	Page 16, under "Letter"
D. MEDICARE ENGLISH GENERAL ENROLLMENT PACKAGE	Page 17, under "Letter"
E. MEDICARE SPANISH GENERAL ENROLLMENT PACKAGE	Page 19, under "Letter"

On page 28 of the contract specifications, under “SCHEDULE”, delete everything after “ORDERS WITHOUT PROOFS AND PRIOR-TO-PRODUCTION SAMPLES:” and replace with “When proofs and prior-to-production samples are not required, complete production and distribution must be made within 5 workdays after receipt of files.

On page 29 of the contract specifications, under “ORDERS REQUIRING PROOFS AND PRIOR-TO-PRODUCTION SAMPLES”, after the paragraph starting with “Revised Proofs”, insert “NOTE: G. DEEMED MEDICARE CARDS WILL NOT require Prior-to-Production Samples. Complete production and distribution to be made 5 workdays after proof approval”.

On page 29 of the contract specifications, under “(D and E) MEDICARE ENGLISH AND SPANISH GENERAL ENROLLMENT PACKAGE”, replace “on the second full week of each month, except for holidays” with “during the month of January each year”.

All other specifications remain the same.

If amendment is not acknowledged on bid, direct acknowledgement to:

U.S. Government Printing Office
Columbus Regional Printing Procurement Office
1335 Dublin Road, Suite 112-B
Columbus, OH 43215-7034

Telephone acknowledgement of this amendment is not acceptable.

BIDDER MUST ACKNOWLEDGE RECEIPT OF THIS AMENDMENT PRIOR TO BID OPENING. Failure to acknowledge receipt of amendment, by amendment number, prior to bid-opening time, may be reason for bid being declared nonresponsive.

Sincerely,

MICHAEL J. SOMMER
Contracting Officer

MJS/llp

U.S. GOVERNMENT PRINTING OFFICE

Columbus, Ohio

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Medicare Enrollment Packages and Medicare Cards

as requisitioned from the U.S. Government Printing Office (GPO) by the

Department of Health & Human Services, Center for Medicare & Medicaid Service

Single Award

CONTRACT TERM: This contract contains an Initial Testing Period and a Production Term.

INITIAL TESTING PERIOD: The Initial Testing Period begins Date of Award and ending April 30, 2015. The Initial Testing Period allows for both Security Clearance Provisions and Initial Post Award Testing.

PRODUCTION TERM OF CONTRACT: The production term of this contract begins May 1, 2015 through April 30, 2016 and 4 option year periods (May 1, 2016 through April 30, 2017; May 1, 2017 through April 30, 2018; May 1, 2018 through April 30, 2019; and May 1, 2019 through April 30, 2020). Special attention is directed to the following provision and clauses in Section 1 of this contract: "Option to Extend the Term of the Contract", and "Economic Price Adjustment".

Single Award

BID OPENING: Bids shall be publicly opened at 2:00 p.m., prevailing Columbus, Ohio time
March 18, 2015

SUBMIT SEALED BID TO: U.S. Government Printing Office, 1335 Dublin Road Suite 112-B, Columbus, Ohio 43215-7034. Bid must be clearly marked on the outermost envelope/package with company name and address of the bidder, program number, and bid date opening. **Telegraphic, facsimile, and e-mail bids transmitted to GPO offices WILL NOT be considered.**

BIDDERS PLEASE NOTE: Formerly Program 5589-S. Significant revisions have been made. Bidders are cautioned to familiarize themselves with all provisions of this contract before bidding.

PROGRAM NUMBER FOR THIS SOLICITATION HAS BEEN CHANGED FROM 5589-S TO 1583-S.

Abstract for Program 5589-S available on GPO Web Site at
http://www.gpo.gov/gpo/abstracts/abstract.action?region=Columbus

BEFORE AWARD: ANY QUESTIONS CONCERNING THESE SPECIFICATION CALL
Linda Price, (614) 488-4616, extension 7.

AFTER AWARD: REFER ALL QUESTIONS TO YOUR CONTRACT ADMINISTRATOR
Russ Woodmancy, (614) 488-4616, extension 8.

NO COLLECT CALLS

SECTION 1. – SPECIFICATIONS AND CONDITIONS

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Pub. 310.2, effective December 1, 1987 (Rev. 06/01)) and GPO Contract Terms, Quality Assurance Through Attributes Program for Printing and Binding (GPO Pub. 310.1, effective May 1979 (revised 08/02)).

GPO Publication 310.2, GPO Contract Terms, Contract Clause 5. Disputes, is hereby replaced with the June 2008 clause found at http://www.gpo.gov/pdfs/vendors/contractdisputes.pdf. This June 2008 clause also cancels and supersedes any other disputes language currently included in existing contractual actions.

These and more Government Printing Office Publications can be found at:
http://www.gpo.gov/vendors/sfas.htm.

REGULATIONS GOVERNING PROCUREMENT

The U.S. Government Printing Office (GPO) is an office in the legislative branch of the United States Government. Accordingly, the Federal Acquisition Regulation is inapplicable to this, and all GPO procurements. However, the text of certain provisions of the Federal Acquisition Regulation as contained in the Code of Federal Regulations (CFR), are referenced in this solicitation. The offeror should note that only those provisions of the Federal Acquisition Regulation which are specifically incorporated by reference into this solicitation, are applicable.

SUBCONTRACTING: The predominant production functions are downloading files, computerized variable imaging, finishing, and mailing. These items CANNOT be subcontracted. All other items, including printing of static data are not considered part of the predominant production functions. Bidder who must subcontract any of the predominant production functions will be declared non-responsible.

QUALITY ASSURANCE LEVELS AND STANDARDS: The following levels and standards shall apply to these specifications:

Product Quality Levels:
(a) Printing (Page Related) Attributes -- Level III.
(b) Finishing (Item Related) Attributes -- Level III.

Inspection Levels (from ANSI/ASQC Z 1.4):
(a) Non-destructive Tests - General Inspection Level I.
(b) Destructive Tests - Special Inspection Level S-2.

Specified Standards: The specified standards for the attributes requiring them shall be:

Attribute	Specified Standard
P-7. Type Quality and Uniformity	Prior-to-Production Samples
P-8. Halftone Match (Single and Double Impression)	Prior-to-Production Samples
P-9. Solid and Screen Tint Color Match	Pantone Matching System
P-10. Process Color Match	Prior-to-Production Samples

CONTRACTOR'S QUALITY ASSURANCE SYSTEM: The contractor must provide and maintain an effective quality assurance system that includes, at a minimum the following elements:

1. Perform a random quality inspection of records on furnished files. Samples should be tested for construction, type, and placement of data in each field.
2. Ensure that the computerized imaging is clear and legible and that the appropriate mail pieces are mailed to each address contained the furnished files.
3. Maintenance and calibration records on all applicable production and inspection equipment.
4. Controls that assure all steps in the process generate a product that conforms to all requirements of this solicitation.
5. Performance utilizing a calibration system that stops production whenever an extra piece is inserted or a piece is left out.

If errors are found or discrepancies exist between the Government furnished files and reports, e.g. print order, record layout, etc., the contractor must cease further production and contact Clinton Howard at (410) 786-1962 or clinton.howard@cms.hhs.gov and the GPO Contracting Officer.

If errors exist in the file and the contractor failed to identify them during his/her quality assurance inspection, no reimbursement for the cost of reprinting will be allowed.

Verification of Production and Mailing: Contractor will be responsible for validating the integrity of all mail pieces in all phases of computer imaging/printing, finishing, and mailing and to ensure all Medicare Packages and Medicare Cards (mail pieces) received from CMS were correctly entered into the United States postal system.

Mail Piece integrity shall be defined as follows:

- Each mail piece as defined on pages 13 to 21 shall include all pages/items (and only those pages/items) intended for the designated recipient as contained in the print files received from CMS.

The contractor is responsible for providing the automated print notice integrity control systems and processes required to prevent the commingling of mail pieces intended for different recipients into a completed notice package. The contractor's printing process must have automated systems that include notice coding and scanning technology capable of:

- Validating the count of pages in a mail piece set.
- Validating the sequence of pages in a mail piece set.
- Validating the sequence of mail piece sets in a production batch.
- Interrupting production if variances are detected.

Mailing integrity shall be defined as follows:

- All mail pieces received from CMS for each Print Order were imaged, printed, inserted and entered correctly into the United States postal system.

The contractor is responsible for providing the automated inserted notice tracking/reporting systems and processes required to validate that 100% of all mail pieces in the specifications received from CMS were imaged, printed, inserted and mailed correctly. The contractor's inserting equipment must have automated systems that include notice coding and scanning technology capable of:

- Reconciling page and item counts from CMS provided print files to Print Order control totals provided by CMS; reporting variances.
- Uniquely identifying each mail piece within a Print Order.

- Scanning unique identifier after insertion to ensure all mail pieces are present and accounted for.
- Tracking and reporting all mail pieces produced and mailed within a Print Order at the mail piece level.
- Identifying and reporting all missing mail pieces in the specifications that were lost or spoiled during production within a Print Order.
- Generating a new production file for all missing mail pieces in the specifications and producing and mailing them.
- Tracking and reporting all mail pieces in the specifications that were reproduced and mailed within a Print Order at the mail piece level.
- Reconciling the total of all mail pieces produced and mailed within a Print Order to the control totals provided by CMS; reporting all variances.
- Reconciling the total of all mail pieces in the specifications mailed to mailing totals contained on Postal Entry Forms within a Print Order; reporting all variances.
- Generating a final automated summary report which provides information that all mail pieces have been scanned after insertion and verifying that all pieces for each Print Order are accounted for. The summary report will contain the sequence number range for a particular Print Order, show all sequence numbers were scanned and accounted for after all mail pieces are inserted, and event information on any spoiled or missing pieces verifying that they were scanned and accounted for. A copy of the summary report must be submitted with the matching GPO Form 712(s).

Contractor must generate an automated audit report when necessary showing the tracking of all mail pieces throughout all phases of production for each mail piece. This audit report will contain all information outlined above for each phase of printing, inserting and mailing.

All mail piece tracking/reporting data must be retained in electronic form for 120 days after mailing, and must be made available to CMS for auditing of contractor performance upon request.

Unique Identification Number: The contractor is responsible for 100% accountability of all mail pieces. There shall be no more than one enrollment card or carrier sheet per envelope, and there shall be no empty envelopes mailed.

The contractor must use a unique sequential identifying number on each mail piece to track each individual item in the specifications, thereby providing 100% accountability. This enables the contractor to track each mail piece through completion of the project.

The contractor will be required to create a test sample based on the quantity submitted. This test must have a unique number and must be produced on each item.

The contractor will generate a list of the unique identifying numbers for each sample. As samples are pulled, their unique number will be marked off the list. This enables the contractor to track which samples have been produced and pulled and what records have been produced.

The unique number for each mail piece must not include the CMS furnished Medicare Claim Number and it must not be formatted like a Medicare Claim Number or Social Security Number.

A recovery system will be required to ensure that all defective or missing/mutilated pieces detected are identified, reprinted and replaced. The recovery system must use unique sequential numbers assigned to each piece to aid in the recovery and replacement of any defective or missing/mutilated pieces, and must be capable of tracking and/or locating any individual piece of mail from the time it leaves the press, up to and including when it is off-loaded at the USPS facility.

The Government will not as a routine matter request that the contractor produce individual pieces in transit within the plant, however, the contractor must demonstrate that they have an audit trail established that has the ability to comply with this type request when and if the need arises. The contractor's Quality Assurance System and the Verification of Production and Mailing plans must account for the number of pieces mailed.

The contractor shall monitor all aspects of the job including material handling and mail flow, to assure that the production and delivery of these notices meet specifications and Government requirements.

Backup Facility Plan: The contractor must have two or more owned/controlled facilities that have the capability to perform all requirements of the contract. This clause is to allow for continuous production with back-up facilities if for any reason(s) (act of God, labor disagreements, etc.) the initial production is unable to meet all the requirements of the contract.

The back-up facilities, equipment, and personnel that have completed the required security documents must be available to the Contracting Officer as part of the pre-award survey.

Failure to have a back-up facility may result in a non-responsible determination.

Technical Support: The contractor must have a highly trained technical support staff available around the clock to solve any mechanical and electrical malfunctions, plus staff and adequate telephone service to receive without interruption the transmission of any electronic media required between 8:00 a.m. Monday through midnight Friday (Baltimore, MD time).

Contractor must also have, on site, a spare parts inventory and on call technicians to avoid any delay in producing orders under this contract plus a Program Manager assigned to the project with designated backup so that a single point of contact will be available to answer any questions which may arise.

WARRANTY: The provisions of Article 15, "Warranty" Of Contract Clauses in GPO Contract Terms is amended for the solicitation to the effect that the warranty period is EXTENDED from 120 days to one calendar year from the date the check is tendered as final payment. All other provisions remain the same.

OPTION TO EXTEND THE CONTRACT TERM: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed April 30, 2020 including, any extension(s) added under this clause. Further extension may be negotiated under the "Extension of Contract Term" clause. See also "Economic Price Adjustment" for authorized pricing adjustment(s).

EXTENSION OF CONTRACT TERM: Notwithstanding the above paragraph, at the request of the Government, the term of any contract resulting from this solicitation may be extended for such period of time as may be mutually agreeable to the GPO and the contractor.

ECONOMIC PRICE ADJUSTMENT: The prices set forth in this contract shall be adjusted in accordance with the provisions of this clause, provided that, in no event will prices be revised to exceed the maximum permissible under any law existing as of the date of the contract or as may be hereafter promulgated.

Price Adjustment Period: For the purpose of this clause, the program years shall comply with the Contract Term clause. There shall be no price adjustment for orders placed during the first program year of this contract.

Price Adjustment: The prices shall be adjusted on the basis of the "Consumer Price Index For All Urban Consumers – Commodities Less Food, Seasonally Adjusted", published monthly in the CPI Detailed Report by the Department of Labor, Bureau of Labor Statistics, in the following manner:

(1) The contract price of orders placed during the adjusted period (excluding reimbursable postage or transportation costs) shall be adjusted by the percentage increase or decrease in the average, seasonally adjusted Consumer Price Index For All Urban Consumers – Commodities Less Food (seasonally adjusted) as follows: An index shall be calculated by averaging the 12 seasonally adjusted months ending 3 months prior to the expiration of the current production period of this contract. This average is then compared with the average index for the 12-month period ending 3 months prior to the beginning of the production term of the contract, called the base index. The percentage increase or decrease by comparing these two indexes shall be applied to the contractor's invoices for orders placed during the price adjustment period.

(2) The Government will notify the contractor in writing of the percentage increase or decrease to be applied to any invoices to be submitted for orders subject to price adjustment in accordance with this clause. Such percentage will be determined from the published index as set forth above. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs. Any applicable discounts will be calculated on the basis of the invoice price as adjusted.

If the Government exercises an option, the extended contract shall be considered to include this economic price adjustment clause.

PRE-AWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract. Attending the preaward survey will be representatives from the Government Printing Office and/or the Centers for Medicare and Medicaid Services. Also, the Government reserves the right to conduct postaward survey as needed.

POST-AWARD TELEPHONE CONFERENCE: Unless waived by the Government, telephone conference call between the contractor and the Government is required. The purpose of the conference will be to discuss and review all aspects of the contractor's production plan, to establish coordination of all internal and external operations, including all mailing requirements, required to complete the contract and CMS to determine appropriate level of security investigation. At the Government's option, this conference may take place at the contractor's facilities.

PRIVACY ACT NOTIFICATION: This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93 – 79, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

PRIVACY ACT

(a) The contractor agrees:

(1) to comply with the Privacy Act of 1974 and the rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals in order to accomplish an agency function when the contract specifically identifies (1) the system or Systems or records and (ii) the work to be performed by the contractor in terms of any one or combination of the following: (A) Design, (B) development, or (C) operation;

(2) to include the solicitation notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation when the statement of work in the proposed subcontract requires the design, development, or operation of a system of records on individuals to accomplish an agency function; and

(3) to include this clause, including this paragraph (3), in all subcontracts awarded pursuant to this contract which require the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved where the violation concerns the design, development, or operation of a system of records on individuals to accomplish the agency function and criminal penalties may be imposed upon the officers or employees of the agency where the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act when the contract is for the operation of a system of records on individuals to accomplish an agency function, the contractor and any employee of the contractor is considered to be an employee of the agency.

(c) The terms used in this clause have the following meanings:

(1) "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records including the collection, use and dissemination of records.

(2) "Record" means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(3) "System of records" on individuals means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

SECURITY PROVISIONS: Security of Personally Identifiable Information (PII) is a vital component of this contract. The Contractor shall guarantee strict confidentiality, integrity, and limited availability of all PII provided by the Government during the performance of this contract. Disclosure of the information/data, in whole or in part, by the Contractor can only be made in accordance with the provisions in the Data Use Agreement (DUA). See Exhibit 6.

It is the contractor's responsibility to properly safeguard PII from loss, theft, or inadvertent disclosure and to immediately notify the Government of any loss of personally identifiable information. PII includes: a person's name, address, and Medicare Claim Number.

The contractor shall not release, or sell, to any person any technical or other data received from the Government under the contract; nor shall the contractor use the data for any purpose other than that for which it was provided to the contractor under the terms of the contract. The contractor must guarantee that furnished PII will be used only to complete this contract.

Failure to secure the PII (or any negligence, unauthorized use, misuse, or abuse of data) entrusted to the contractor could adversely affect individual Medicare beneficiaries, the Government, and the contractor. Possible consequences include, but are not limited to:

- Beneficiaries: Denial of benefits; emotional distress.
- Government: Healthcare fraud; loss of public trust; incur remediation costs; civil and/or criminal penalties.
- Contractor: Civil and/or criminal penalties; Termination for Default of this contract; incur cost and liability of remedying the breach, such as the cost of notifying all affected beneficiaries and providing free credit monitoring services for one year to all affected beneficiaries.

Proper control and handling must be maintained at all times to prevent any information or materials required to produce the products ordered under these specifications from falling into unauthorized hands. All PII furnished by the Government, or duplicates created by the contractor or their representatives, and any resultant printouts must be kept accountable and under security to prevent their release to unauthorized persons. Unsecured telecommunications, including the internet, to transmit PII is prohibited.

Examples of a data breach could include, but not limited to: multiple enrollment cards or carriers sheets for different beneficiaries inserted into the same envelope; unsealed or improperly sealed envelopes containing PII released to USPS; improperly disposed printout or electronic files.

Incident Reporting Requirements: If there is a breach, or a suspected breach, of Personally Identifiable Information (PII), the incident must be reported to CMS within one hour of discovery. Report breaches to the CMS IT Service Desk at **410-786-2580** or **800-562-1963.**

Preaward/Postaward Surveys: At the Government's option, Preaward or Postaward Surveys may be conducted to review of all data handling and production areas involved along with their specific functions, and the contractor's/subcontractor's, personnel, production, security and other requirements outlined in this contract and in the contractor's Security Plan.

Personnel Security: The contractor shall have a system in place to perform criminal background investigations, Social Security Number verification, and drug testing on all employees. In addition, CMS will perform background investigations on two contractor employees who will access the TIBCO mailbox. See Exhibits 4 and 5 for more information.

Physical Security: The contractor shall have a secure work area(s) for processing and production of all CMS PII in electronic and paper format. The work area(s) shall be accessible only to authorized employees, and all work shall be monitored closely by contractor management, while CMS PII is being processed and/or produced.

Information Technology (IT) Security: The contractor shall have a system in place to comply with CMS Information Security Clause 11 in Exhibit 1.

Security Liaison(s): The contractor must appoint one or more Security Liaison(s) to handle issues regarding personnel, physical, and computer security; confidential issues that may arise at any point during the background investigation process; and to serve as a point of contract to the Government for security issues.

The Liaison's duties will include attending the Postaward Conference, submitting a security plan, discussing confidential security issues with CMS staff, submitting background applications, and resolving any issues of inaccurate or incomplete data supplied by background investigation applicants. In the event CMS discovers sensitive information during the background investigation, CMS Security may need to contact the background investigation applicant directly.

Disposal of Waste Material: All waste material containing PII must be destroyed in a manner that it is not possible to recreate the product or identity of a beneficiary; i.e. burning, pulping, shredding, macerating, or other suitable means. If the contractor selects shredding as a means of destruction, it must be a cross cut shredder with a maximum size of 5/32" x 1-1/2" cross cut particles. Strip shredding is not acceptable.

Destruction of waste must occur inside the contractor's secure production facility, close to the point of production or inspection. Sending intact waste containing PII to a municipal incinerator, or to a recycler, or any other off-site processor, is not acceptable and will be considered a data breach.

While CMS PII is being processed or produced, it is recommended that the contractor not confuse employees with separate bins for destruction and for intact waste. The contractor is encouraged to destroy all waste beyond recognition when CMS PII is in the immediate processing and production area.

Disposal of Electronic PII: Immediately after production of each print order is complete, all electronic files containing PII furnished for the print order must be permanently destroyed in accordance with Federal Information Security Management Act (FISMA) of 2002. CMS will maintain an archive of furnished files.

Expiration of Data Use Agreement (DUA): Upon expiration of this DUA, the contractor will be required to sign a certificate confirming destruction of all CMS data files and that no copies have been kept. Therefore, contractor must maintain a log listing the file name, date received from CMS, and date destroyed. Failure to certify file destruction may cause the CMS Privacy Office to refuse to issue future DUA's and data with the contractor's company or to individuals listed on this DUA. See Exhibit 7: Certificate of Data Destruction (Form CMS-10252).

Security Exhibits: The following exhibits 1 through 8 contain security clauses, information, and forms.

- **Exhibit 1: CMS Clause 11: CMS Information Security**
- **Exhibit 2: CMS Clause 09A-01 Security Clause**
- **Exhibit 3: FAQ Supplement to CMS Security Clause 09A-01**
- **Exhibit 4: Request for Physical Access to CMS Facilities (Form CMS-730A)**
  (This form is used to initiate background investigations of the two people applying for access to the TIBCO mailbox. No physical access, or badge, to CMS will be granted. Applicants must complete page 1 and sign/date page 2, and submit to CMS immediately after award and renew annually thereafter.)
- **Exhibit 5: Application for Access to CMS Computer Systems (Form CMS-20037)**
  (The same applicants for CMS-730A must complete CMS-20037, and submit to CMS immediately after award and renew annually thereafter.)
- **Exhibit 6: Data Use Agreement (DUA) (Form CMS-R-0235)**
  (Contractor management must complete CMS-R-0235, and submit to CMS immediately after award.)
- **Exhibit 7: Certificate of Data Destruction (Form CMS-10252)**
  (Contractor must complete CMS-10252 at the expiration of the DUA.)

- **Exhibit 8: Secure One HHS, Information Security Program Rules of Behavior**
  (All contractor management and employees involved in this contract must read and sign this document. Signed copies of this document for TIBCO applicants and DUA applicants must be submitted to CMS immediately after award. Signed copies for all other employees will be maintained by the contractor and furnished to the Government upon request.

The contractor must submit all completed and signed security forms (original signatures only, no photocopy or facsimile signatures will be accepted) to: CMS, Attn: Clinton Howard, SL-12-17, 7500 Security Blvd, Baltimore, MD 21244. For delivery directly to Clinton Howard, the contractor should use FedEx Overnight service and use FedEx furnished packaging. All other delivery services and packaging are opened and inspected in the CMS mailroom.

Security Plan: The contractor must have a formal, documented Security Plan that will ensure their compliance with all of the security provisions of this contract and as referenced in attached exhibits. Particular attention should be given to addressing compliance of the *Federal Information Security Management Act of 2002 (FISMA)* and the *Privacy Act of 1974* as referenced in Exhibit 1, CMS Clause 11. Minimum security requirements for FISMA compliance are defined by the Department of Commerce, National Institute of Standards and Technology (NIST) in Federal Information Processing Standards Publication (FIPS) Publication 200 "Minimum Security Requirements for Federal Information and Information Systems". This document can be found on the internet at the following web address: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

The contractor's Security Plan must, at a minimum, cover seventeen security-related areas identified in FIPS 200 with regard to protecting the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by those systems. The security-related standards include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. The seventeen areas represent a broad-based, balanced information security program that address the management, operational, and technical aspects of protecting federal information.

Within 10 workdays after award, the contractor must submit three (3) copies of their Security Plan to: CMS, Attn: Clinton Howard, SL-12-17, 7500 Security Blvd, Baltimore, MD 21244.

Release of PII by CMS does not constitute CMS' approval or acceptance of the Security Plan. At any time during this contract, if CMS finds deficiencies in the Security Plan, CMS may require correction of the deficiency.

NOTE: A copy of all forms, with Social Security Numbers redacted, are to be submitted to: US GPO; Columbus RPPO; 1335 Dublin Road, Suite 112-B; Columbus, OH 43215 at the same time the originals are sent to the CMS address listed above.

NOTE: CONTRACTOR'S BID TO INCLUDE COST OF TWO EMPLOYEE BACKGROUND INVESTIGATIONS. BACKGROUND INVESTIGATION IS TO BE SUFFICIENT TO COVER THE SECURITY PROVISIONS AS DESCRIBED IN THE CONTRACT.

ASSIGNMENT OF JACKETS, PURCHASE AND PRINT ORDERS: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented by an individual "Print Order" for each job placed with the contractor. The print order, when issued, will indicate the quantity to be produced and any other information pertinent to the particular order.

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of print orders by the Government. Production orders may be issued under the contract from **May 1, 2015 through April 30, 2016 (plus options)**. All print orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any print order. A print order shall be "issued" for purposes of the contract, when it is either deposited in the U.S. Postal Service mail or otherwise furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "Ordering". The quantities of items specified herein are estimates only, and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated", it shall not constitute the basis for an equitable price adjustment under this contract.

Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

The Government shall not be required to purchase from the contractor, requirements in excess of the limit on total orders under this contract.

Orders issued during the effective period of this contract and not completed within that time shall be completed by the contractor within the time specified in the order, and the rights and obligations of the contractor and the Government respecting those orders shall be governed by the terms of this contract to the same extent as if completed during the effective period of this contract.

If shipment/delivery of any quantity of an item covered by the contract is required by reason of urgency prior to the earliest date that shipment/delivery may be specified under this contract, and if the contractor will not accept an order providing for the accelerated shipment/delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for shipment/delivery to or performance at multiple destinations.

Subject to any limitations elsewhere in this contract, the contractor shall furnish to the Government all items set forth herein which are called for by print orders issued in accordance with the "Ordering" clause of this contract.

DELIVERY/SHIPPING STATUS INFORMATION: Contractors are to report information regarding each order for compliance reporting purposes and include date of delivery (or shipment if applicable) for proofs and delivery schedules in accordance with the contract requirements by contacting Columbus RPPO via e-mail to trackcolumbus@gpo.gov, or by calling (614) 488-4616, ext. 6, or by faxing to (614) 488-4577. Personnel receiving e-mail, phone call, or fax will be unable to respond to questions of a technical nature or transfer any inquiries.

PAYMENT: Submit all vouchers via FAX utilizing the GPO barcode coversheet program application. Instructions for the GPO barcode coversheet program application can be found at the following web address: http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

At time of invoicing, the contractor must submit a copy of the print order, contractor's invoice and all mailing and/or delivery receipts via e-mail to infocolumbus@gpo.gov and to clinton.howard@cms.hhs.gov. All mailing receipts must also be e-mailed to tina.dickens@cms.hhs.gov.

SECTION 2 – SPECIFICATIONS

SCOPE: These specifications cover the production of Medicare Domestic, Puerto Rican, and Foreign Initial Enrollment Packages (IEP), English and Spanish General Enrollment Packages (GEP), and Replacement and Deemed Medicare Cards requiring such operations as downloading files, manipulating data, computer imaging, printing, gathering, inserting into envelopes, labeling, sorting, mailing, and distribution.

TITLE: Medicare Enrollment Packages and Medicare Cards.

FREQUENCY OF ORDERS/QUANTITIES/TRIM SIZES/DESCRIPTION/CONSRUCTION:

NOTE: Pamphlets and letters may appear similar for each of the items listed but each have unique formatting and content. The contractor is to ensure the correct pamphlet/letter is inserted into the correct package.

NOTE: F: Replacement Medicare Card and the G: Deemed Medicare Card description may appear similar but each of these cards have unique formatting and content. The contractor is to ensure the correct card format and content is mailed to each recipient.

A: MEDICARE DOMESTIC INITIAL ENROLLMENT PACKAGE:

Number of Orders: One (1) order per month.

Quantity: Approximately 100,000 to 500,000 copies per order, average 183,000 copies per order.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Enrollment Card: Left mailing address block to show through window of mailing envelope.
- Pamphlet: Title page facing flap side of mailing envelope.
- BRM Envelope
- Letter: Folded to 8-1/2 x 5-1/2”, logo facing flap side of mailing envelope.

Mailing Envelope: Open side, side seams, fully gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back in black ink, no printing on flap, no bleeds. Interior prints with black security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 6 x 9-1/2”
- Window Size: 4-1/4 x 1-1/2” die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Left address block of Enrollment Card appears in the window. No other content should appear in the window area.
- Window Location: 1/2” from left and 11/16” from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Enrollment Card: Enrollment Card is perforated (slit or slot, without ink) in two locations. The intersecting perforations will form a 3-1/2 x 2-3/8" tear-out card at the top right corner. Print face and back. No bleeds. Inadequate gripper.

Face prints static data in Pantone 186U Red and 300U Blue and variable data in black ink. Variable data consists of left address block, right address block, and approximately 5 typelines. Address blocks consist of up to 5 lines plus postal markings, including Intelligent Mail Barcode (IMb).

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card are permitted.

Back prints static data in Pantone 300U Blue.

- Trim Size: 5-1/2 x 8-1/2", includes 3-1/2 x 2-3/8" tear-out card.
- Vertical Perforation: 3-1/2" from right edge of card, extending 2-3/8" from top edge of card.
- Horizontal Perforation: 2-3/8" from top edge of card, extending 3-1/2" from right edge of card.
- White 25% Index, basis size 25-1/2 x 30-1/2", 110 lbs. per 500 sheets, equal to JCP Code K20. EXCEPTION: Brightness level must be a minimum of 90.

Pamphlet (Welcome to Medicare): Prints head-to-head in Pantone 186U Red and 300U Blue and black ink with reverse type, halftones, and screen-tints throughout. Self-cover 1 (title page) bleeds top, bottom and right. Self-cover 4 bleeds bottom, left, and right. Inside text pages, including self-covers 2 and 3, bleed top, left, and right. Print masthead to and align across the bind edge throughout.

- Trim Size: 8-3/8 x 5-3/8"
- Pages: 32 pages, including self-covers.
- White Offset Book, basis size 25 x 38", 50 lbs. per 500 sheets, equal to JCP Code A60.
- Saddle stitch in two locations on the 5-3/8" dimension.

Business Reply Mail Envelope: Open side, side seams, split gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back in black ink, no printing on flap, no bleeds, no interior security tint. BRM intended for recipient use only and if used, right address block of Enrollment Card is to appear in the window.

- Trim Size: 5-3/4 x 8-3/4"
- Window Size: 3-1/2 x 1-7/16" die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Right address block of Enrollment Card, if inserted into BRM, appears in the window. No other content should appear in the window area.
- Window Location: 4-3/4" from left and 7/16" from bottom edges of envelope.
- Stock/Paper: Light Brown Kraft, basis size 17 x 22", 24 – 28 lbs. per 500 sheets, equal to JCP Code V10.

Letter: Flat Size: 8-1/2 x 11" folded to 8-1/2 x 5-1/2". Prints black ink face only with all static information.

B: MEDICARE PUERTO RICAN INITIAL ENROLLMENT PACKAGE:

Number of Orders: One (1) order per month.

Quantity: Approximately 2,000 to 5,000 copies per order, average 3,000 copies per order.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Letter: Collated and folded to approximately 8-1/2 x 3-3/4 (letter fold), mailing address to show through window of mailing envelope.
- Pamphlet: Title page facing flap side of mailing envelope.

Mailing Envelope: Open side, diagonal seams, fully gummed commercial style flap. Exterior prints face and back in black ink, no printing on flap, no bleeds. Interior prints with blue security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 4-1/8 x 9-1/2”
- Window Size: 4-9/16 x 1-3/16” die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Mailing address block of letter appears in the window. No other content should appear in the window area.
- Window Location: 7/8” from left and 1/2” from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Letter: Four page letter (2 leaves) collated. Flat Size: 8-1/2 x 11”, Finish Size 8-1/2 x 3-2/3” with two parallel wrap around folds. Page 1 prints black ink with static and variable data. Variable data consists of address block and up to 2 typelines. Pages 2, 3, and 4 print black ink with static data.

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card are permitted.

Pamphlet (Welcome to Medicare): Prints head-to-head in Pantone 286U Blue and black ink with reverse type, halftones, and screen-tints throughout. Self-cover 1 (title page) bleeds outside edges and prints to the bind edge. Self-covers 2 through 4 and inside text pages bleed top, left, and right. Print masthead to and align across the bind edge throughout.

- Trim Size: 3-1/2 x 8”
- Pages: 16 pages, including self-covers.
- White Offset Book, basis size 25 x 38”, 50 lbs. per 500 sheets, equal to JCP Code A60.
- Saddle stitch in two locations on the 8” dimension.

C: MEDICARE FOREIGN INITIAL ENROLLMENT PACKAGE:

Number of Orders: One (1) order per month.

Quantity: Approximately 700 to 1,500 copies per order, average 1,000 copies

Assembly: Contents to be inserted into mailing envelope in the following order:

- Letter: Collated and folded to approximately 8-1/2 x 3-3/4 (letter fold), mailing address to show through window of mailing envelope.
- Return Envelope
- Pamphlet: Title page facing flap side of mailing envelope.

Mailing Envelope: Open side, diagonal seams, fully gummed commercial style flap. Exterior prints face and back in black ink, no printing on flap, no bleeds. Interior prints with blue security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 4-1/8 x 9-1/2”
- Window Size: 4-9/16 x 1-3/16” die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Mailing address block of letter appears in the window. No other content should appear in the window area.
- Window Location: 15/16” from left and 1/2” from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Letter: Six page letter (3 leaves) collated. Flat Size: 8-1/2 x 11”, Finish Size 8-1/2 x 3-2/3” with two parallel wrap around folds. Page 1 prints black ink with static and variable data. Variable data consists of address block and up to 2 typelines. Pages 2 and 3 print black ink with static data. Page 4 is blank. Page 5 prints black ink with static and variable data. Variable data consists of address block and up to 2 typelines. Page 6 is blank.

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card are permitted.

Return Envelope: Open side, diagonal seams, fully gummed commercial style flap, non-window. Exterior prints face only (no printing on flap) in black ink, no bleeds. Interior prints black security tint. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 3-7/8 x 8-7/8”, non-window
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Pamphlet (Welcome to Medicare): Prints head-to-head in Pantone 286U Blue and black ink with reverse type, halftones, and screen-tints throughout. Self-cover 1(title page) bleeds outside edges and prints to the bind edge. Self-covers 2 through 4 and inside text pages bleed top, left, and right. Print masthead to and align across the bind edge throughout.

- Trim Size: 3-1/2 x 8”
- Pages: 12 pages, including self-covers.
- White Offset Book, basis size 25 x 38”, 50 lbs. per 500 sheets, equal to JCP Code A60.
- Saddle stitch in two locations on the 8” dimension.

D: MEDICARE ENGLISH GENERAL ENROLLMENT PACKAGE:

Number of Orders: One (1) order per year.

Quantity: Approximately 500,000 to 750,000 copies anticipate approximately 694,000 copies.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Letter: Collated and folded to approximately 8-1/2 x 3-3/4 (letter fold), mailing address to show through window of mailing envelope.
- BRM Envelope
- Pamphlet: Title page facing flap side of mailing envelope.

Mailing Envelope: Open side, side seams, fully gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back (flap only) in black ink, no bleeds. Interior prints with black security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 4-1/8 x 9-1/2”
- Window Size: 4-1/2 x 1-3/8” die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Mailing address block of letter appears in the window. No other content should appear in the window area.
- Window Location: 7/8” from left and 1/2” from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Letter: Four page letter (2 leaves) collated. Flat Size: 8-1/2 x 11”, Finish Size 8-1/2 x 3-2/3” with two parallel wrap around folds. Page 1 prints black ink with static and variable data. Variable data consists of address block and up to 2 typelines. Page 2 is blank. Pages 3 and 4 print black ink with static data.

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card.

Business Reply Mail Envelope: Open side, side seams, fully gummed straight flap with slightly tapered and rounded corners, non-window. Exterior prints face and back (flap only) in black ink, no bleeds, no interior security tint. BRM intended for recipient use only.

- Trim Size: 3-7/8 x 8-7/8”
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Pamphlet (Welcome to Medicare): Prints head-to-head in Pantone 286U Blue and black ink with reverse type, halftones, and screen-tints throughout. Self-cover 1 (title page) bleeds outside edges and prints to the bind edge. Self-covers 2 and 3 and inside text pages bleed top, left, and right. Print masthead to and align across the bind edge throughout. Self-cover 4 does not bleed.

- Trim Size: 3-1/2 x 8”
- Pages: 12 pages, including self-covers.
- White Offset Book, basis size 25 x 38”, 50 lbs. per 500 sheets, equal to JCP Code A60.
- Saddle stitch in two locations on the 8” dimension.

E: MEDICARE SPANISH GENERAL ENROLLMENT PACKAGE:

Number of Orders: One (1) order per year.

Quantity: Approximately 5,000 to 15,000 copies anticipate approximately 11,000 copies.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Letter: Folded to approximately 8-1/2 x 3-3/4 (letter fold), mailing address to show through window of mailing envelope.
- Pamphlet: Title page facing flap side of mailing envelope.

Mailing Envelope: Open side, side seams, fully gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back (flap only) in black ink, no bleeds. Interior prints with black security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 4-1/8 x 9-1/2”
- Window Size: 4-1/2 x 1-3/8” die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Mailing address block of letter appears in the window. No other content should appear in the window area.
- Window Location: 7/8” from left and 1/2” from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22”, 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor’s option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Letter: Four page (2 leaves) collated. Flat Size: 8-1/2 x 11", Finish Size 8-1/2 x 3-2/3" with two parallel wrap around folds. Prints black ink face and back. Page 1 prints black ink with static and variable data. Variable data consists of address block and up to 2 typelines. Pages 2 and 3 print black ink with static data. Page 4 is blank.

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card.

Pamphlet (Welcome to Medicare): Prints head-to-head in Pantone 286U Blue and black ink with reverse type, halftones, and screen-tints throughout. Self-cover 1 (title page) bleeds outside edges and prints to the bind edge. Self-covers 2 through 4 and inside text pages bleed top, left, and right. Print masthead to and align across the bind edge throughout.

- Trim Size: 3-1/2 x 8"
- Pages: 16 pages, including self-covers.
- White Offset Book, basis size 25 x 38", 50 lbs. per 500 sheets, equal to JCP Code A60.
- Saddle stitch in two locations on the 8" dimension.

F: REPLACEMENT MEDICARE CARDS:

Number of Orders: One (1) order per week.

Quantity: Approximately 80,000 to 160,000 copies per order, average 117,000 copies.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Replacement Medicare Card: Mailing address block to show through window of mailing envelope.

Mailing Envelope: Open side, side seams, split gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back in black ink, no printing on flap, no bleeds. Interior prints with black security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 3-7/8 x 8"
- Window Size: 3-3/4 x 1-3/8" die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Address block of Replacement Medicare Card appears in the window. No other content should appear in the window area.
- Window Location: 3/8" from left and 9/16" from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22", 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor's option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Replacement Medicare Card: Replacement Medicare Card is perforated (slit or slot, without ink) in two locations. The intersecting perforations will form a 3-1/2 x 2-3/8" tear-out card at the top right corner. Print face and back.

Face prints static data in Pantone 186U Red and 300U Blue and variable data in black ink. Variable data consists of address block and approximately 10 to 20 typelines. Address blocks consist of up to 5 lines plus postal markings, including Intelligent Mail Barcode (IMb).

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card.

Back prints static data in Pantone 300U Blue. No bleeds, inadequate gripper. Trim 4 sides.

- Trim Size: 7-1/2 x 3-11/16", includes 3-1/2 x 2-3/8" tear-out card.
- Vertical Perforation: 3-1/2" from right edge of card, extending 2-3/8" from top edge of card.
- Horizontal Perforation: 2-3/8" from top edge of card, extending 3-1/2" from right edge of card.
- White 25% Index, basis size 25-1/2 x 30-1/2", 110 lbs. per 500 sheets, equal to JCP Code K20. EXCEPTION: Brightness level must be a minimum of 90.

G: DEEMED MEDICARE CARDS:

Number of Orders: One (1) order per year.

Quantity: Approximately 15,000 to 30,000 copies anticipate approximately 22,000 copies.

Assembly: Contents to be inserted into mailing envelope in the following order:

- Deemed Medicare Card: Mailing address block to show through window of mailing envelope.

Mailing Envelope: Open side, side seams, split gummed straight flap with slightly tapered and rounded corners. Exterior prints face and back in black ink, no printing on flap, no bleeds. Interior prints with black security tint. Security tint extends onto ungummed area of flap. Contractor may use own design for security tint, however no proprietary tints or company logos are permitted.

- Trim Size: 3-7/8 x 8"
- Window Size: 3-3/4 x 1-3/8" die-cut window with clear poly window material glued securely on all edges so as not to interfere with insertion of contents.
- Window Covering: The clear polystyrene window material shall be free of conditions with would prevent machine reading by USPS automated equipment. Window covering material MUST BE TRANSPARENT and in accordance with all applicable USPS requirements. Address block of Deemed Medicare Card appears in the window. No other content should appear in the window area.
- Window Location: 3/8" from left and 5/8" from bottom edges of envelope.
- Stock/Paper: White Writing or Wove, basis size 17 x 22", 24 lbs. per 500 sheets, equal to JCP Code V20. EXCEPTION: Contractor's option for 28 lbs. per 500 sheets, all other specifications shall be maintained.

Deemed Medicare Card: Deemed Medicare Card is perforated (slit or slot, without ink) in two locations. The intersecting perforations will form a 3-1/2 x 2-3/8" tear-out card at the top right corner. Print face and back.

Face prints static data in Pantone 186U Red and 300U Blue and variable data in black ink. Variable data consists of address block and approximately 10 to 20 typelines. Address blocks consist of up to 5 lines plus postal markings, including Intelligent Mail Barcode (IMb).

All variable data, including addresses, must be imaged in all capital letters without punctuation. Punctuation exceptions: hyphens positioned in the Medicare Claim Number and hyphens and/or apostrophes that may appear in the beneficiary name on Medicare Card.

Back prints static data in Pantone 300U Blue. No bleeds, inadequate gripper. Trim 4 sides.

- Trim Size: 7-1/2 x 3-11/16", includes 3-1/2 x 2-3/8" tear-out card.
- Vertical Perforation: 3-1/2" from right edge of card, extending 2-3/8" from top edge of card.
- Horizontal Perforation: 2-3/8" from top edge of card, extending 3-1/2" from right edge of card.
- White 25% Index, basis size 25-1/2 x 30-1/2", 110 lbs. per 500 sheets, equal to JCP Code K20. EXCEPTION: Brightness level must be a minimum of 90.

GOVERNMENT TO FURNISH: Government will furnish static and variable data.

Static Data: PDF files, fonts, color visuals, and samples to be furnished after award.

Variable Data: Data Files will be furnished via Electronic File Transmission (EFT). A TIBCO Mailbox will be setup by CMS to provide access to data files. Immediately after award, the contractor must submit two (one primary user, and one back-up user) completed "APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS" at the following internet link:

http://www.cms.hhs.gov/InformationSecurity/Dowloads/EUAaccessform.pdf.

The contractor must complete Section 2, User Information on page 1, and the Applicant's Information on page 3 on the Form.

Please note that the Applicant's Social Security Number must be provided in order to receive a USERID and gain access to CMS' computer systems. Corporate Tax Identification Numbers are not accepted in lieu of individual SSN's. The contractor must reapply for access every 12 months during the term of the contract.

Return completed form to: HHS/CMS 7500 Security Boulevard, SL-12-17, Attn: Clinton Howard, Baltimore, MD 21244-1850. The contractor is encouraged to use FedEx Overnight service. Packages delivered by other methods may be opened in the CMS mailroom.

Additional information regarding the CMS EFT Infrastructure can be found at the following link:

http://www.cms.hhs.gov/SystemLifecycleFramework/Downloads/EFTInfrastructure.pdf

Software: Contractor will need an Internet browser, the browser must be Internet Explorer 5.0 or above, or you can use GIS-compatible secure File Transfer Protocol Client (FTP).

TIBCO files furnished with variable information for imaging Medicare Domestic, Foreign and Puerto Rican Initial Enrollment Package, Replacement and Deemed Medicare Cards.

Complete record specifications will be furnished at the beginning of the contract and will be updated when changes are made in the record specifications.

Contractor must be able to read/print up to six lines of address information and insure all address carriers, envelope and windows can display address format acceptable for USPS automation processing.

PLATFORM: Microsoft's Windows XP operating system or Apple Macintosh Operating System.

STORAGE MEDIA: TIBCO mailbox.

SOFTWARE: Files will be furnished in .PDF format created on either Apple OS platform or Microsoft Windows platform from software such as Adobe Illustrator – Version 13 (CS3), Adobe Photoshop – Version 10 (CS3), Adobe InDesign – Version 5 (CS3) Adobe Acrobat Version 8, Quark – Version 6.5, Microsoft Word – Version 2003, Microsoft Excel – Version 2003.

Contractor will be required to support all current and future upgrades for Adobe PDF software.

FONTS: All printer and screen fonts will be furnished. The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.

ELECTRONIC PREPRESS: Immediately upon receipt and prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required reproduction image. Any errors, media damage, or data corruption that might interfere with proper file image processing must be reported to Columbus GPO Contracting Officer prior to further performance.

The contractor shall create or alter any necessary trapping, set proper screen angles and screen frequency, and define file output selection for the imaging device being utilized. Furnished files must be imaged as necessary to meet the assigned quality level.

Digital Deliverables: If the contractor is required to make revisions, the contractor shall, prior to making revisions, copy the files and make all changes to the copy. No revisions are to be made to the furnished files.

The contractor must furnish final production native application files (digital deliverables) with the furnished material. The digital deliverables much be an exact representation of the final printed piece and shall be returned on the same type of storage media as the original files.

Repurposed Deliverables: If the contractor is required to make revisions, the contractor shall, prior to making revisions, copy the files and make all changes to the copy. No revisions are to be made to the furnished files.

The contractor must furnish final press optimized PDF with the furnished material. The repurposed deliverables must be an exact representation of the final printed piece and shall be returned on the same type of storage media as the original files.

PREPRINTING OF STATIC DATA: At the contractor's option, contractor may preprint any static data to keep a stock on hand or print the static data when they receive the orders. It is anticipated that the contractor may want to keep a few month's supply on hand. Although the static data will generally remain the same from order to order, changes may need to be made from time to time. The Government will provide the contractor with as much advance notice as possible.

The Government will not be responsible for more than a 3-month supply of static data that is not usable due to copy changes.

ENVELOPES: Sample will be furnished as Manuscript Copy (PDF Proof Required before printing).

Print Orders (GPO Form 2511).

Delivery/Shipping Status Report

Form 905 (R. 3/90), "Labeling and Marking Specifications".

Identification markings such as register marks, ring folios, rubber stamped jacket numbers, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried on copy or film, must not appear on finished product.

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "Government to Furnish," necessary to produce the product(s) in accordance with these specifications.

Contractor must furnish all Mailing and Return envelopes.

Contractor will be required to verify that the CMS furnished files and quantity(s) are available in the TIBCO mailbox within two hours of receipt of the print order.

REPRODUCIBLES: The contractor must make all reproducibles required. The contractor is responsible for determining what type reproducibles will be used but must maintain the quality level specified in the contract. No separate charges will be allowed for the various types of reproducibles that may be used.

Further, the contractor is responsible for outputting all images contained on furnished material, regardless of the production process, at the highest effective resolution possible. The contractor is responsible for determining the appropriate output resolution to achieve optimal results for such design elements as blends, gradients, halftones, type and other images. This determination should be made using factors such as stock, imaging device (or press) being used, and other factors unique to the contractors production environment.

POST-AWARD TEST: Immediately after award, a post-award test shall be conducted. The post-award test will consist of Post-Award Test Proofs, Post-Award Test Live Data Samples, and Post-Award Test Prior-to-Production Samples. The Post-Award Test requirements shall be produced at no additional charge to the Government.

Post-Award Test Proofs: Within 5 workdays after receipt of the Government Furnished Material, contractor shall submit proofs to the Government. Proofs shall be produced and submitted in accordance with the requirements listed hereafter under "Proofs".

Post-Award Test Live Data Samples: Immediately after approval of the Post-Award Test Proofs, and prior to production of the Post-Award Test Prior-to-Production Samples, the contractor shall be required to perform a Live Data Sample test using live data records placed by CMS in the TIBCO Mailbox and downloaded by the contractor's representatives who have been granted access to the TIBCO mailbox. The data sample will also include address library data.

Within 5 workdays after receipt of Post-Award Test Proof approval, the contractor will be required to submit 50 Live Data Samples of all variable data of each package. Contractor must perform a production run per specifications as if these were live orders; however, contractor must pack completed items in a shipping container and deliver via overnight courier (i.e.: FedEX Next Day) to: **HHS/CMS, 7500 Security Boulevard, SL-12-17 Attn: Clinton Howard, Baltimore, MD 21244-1850.**

The 50 Live Data Samples shall consist of 25 sequential records and 25 randomly selected records from the remaining TIBCO files. Each sample package shall consist of all component parts of each package assembled in accordance with the contract specifications.

Each Item must consist of all component parts assembled as specified. The test work must be printed and constructed using the form, ink, *paper, equipment, and the method of production which will be used in producing the finished product. All items must be of the size, kind, and quality the contractor will furnish.

*NOTE: In lieu of White 25% Index, basis size 25-1/2 x 30-1/2", 110 lbs. per 500 sheets, equal to JCP Code K20, Live Data Samples may be printed on White Writing Paper, basis size 17 x 22", 20 lbs. per 500 sheets, equal to JCP Code D10. Items MUST be trimmed to size.

Post-Award Test Prior-to-Production Samples: Within 5 workdays after receipt of the Post-Award Test Live Data Samples approval, contractor shall submit 15 sets of Post-Award Test Prior-to-Production Samples to the Government (5 sets of each package to 3 locations). Addresses to be provided at the Post-Award Telephone Conference. Samples shall be produced and submitted in accordance with the requirements listed hereafter under "Prior-to-Production Samples".

PROOFS: It is anticipated proofs will be required after award and when copy changes are required. Copy changes are anticipated once a year, usually sometime between September and December. When indicated on the individual print order and within 5 workdays of receipt of Government Furnished Material, contractor shall submit 1 set of PDF "Soft" Proofs of all pieces (static data only) in each package via e-mail.

Contractor to submit one "Press Quality" PDF "soft" proof (for static data content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match. E-Mail proofs to the address indicated on the individual print order by the date specified.

If any contractor's errors are serious enough in the opinion of the GPO to require revised proofs, the revised proofs are to be provided at no expense to the Government. No extra time can be allowed for this reproofing; such operations must be accomplished within the original production schedule allotted in the specifications.

The contractor is cautioned that these proofs must be made from the final digital files (used for this printing) that are to be delivered to the Government.

In the event proofs are disapproved by the Government, or the contractor fails to submit proofs in a sufficient amount of time to meet the delivery schedule, the contractor may be deemed to have failed to make progress, and is subject to the termination for default clause. However, failure of the Government to terminate the contract for default in such event shall not relieve the contractor of the responsibility to deliver the contract quantities in accordance with the original production schedule allotted in the specifications.

Send proof delivery notification via facsimile to (614) 488-4577 or e-mail trackcolumbus@gpo.gov. Include GPO Jacket Number, Program/Print Order Numbers with all correspondence.

The contractor must not print prior to receipt of an "OK to Print" or "OK to Print with Corrections".

PRIOR-TO-PRODUCTION SAMPLES: It is anticipated that prior-to-production samples will be required after award and when copy changes are required. Copy changes are anticipated once a year, usually sometime between September and December. When indicated on the individual print order and within 5 workdays of receipt of proof approval (or live data sample approval after award).

The sample requirement for this contract is 15 sets of each package including variable and static data (5 sets of each package to 3 locations). The samples must be constructed as specified using the form, ink, equipment, and methods of production which will be used in producing the finished products. Paper used for samples must be of the size, kind, and quality the contractor will furnish.

Samples will be inspected and must comply with the specifications as to kind and quality of materials, and quality of reproduction.

Prior to the commencement of production of the contract production quantity, the contractor shall submit the samples, along with all of the furnished Government materials, to the addresses provided at the post-award telephone conference. It is the Government's option to review the Prior-to-Production Samples at the contractor's plant.

The package must be marked "PRE-PRODUCTION SAMPLES DO NOT DELAY"; and must include the GPO jacket number, program, print order number, dept. requisition number, and title.

It is the responsibility of the contractor to submit the preproduction samples in sufficient time to allow Government inspection of the samples and production and shipment of the final product to meet the required delivery date. The Government will approve, conditionally approve, or disapprove the samples within 24 hours of receipt thereof by telephone, fax, or e-mail.

Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

If the samples are disapproved by the Government, the Government at its option may require the contractor to submit additional samples for inspection and test, in the time and under the terms and conditions specified in the notice of rejection. Such additional samples shall be furnished, and necessary changes made, at no additional cost to the Government, and with no extension in the shipping schedule. The Government will require the time specified above to inspect and test any additional samples required.

In the event the samples are disapproved by the Government, the contractor shall be deemed to have failed to make delivery within the meaning of the default clause in which event this contract shall be subject to termination for default, provided however, that the failure of the Government to terminate the contract for default in such event shall not relieve the contractor of the responsibility to deliver the contract quantities in accordance with the shipping schedule.

In the event the Government fails to approve, conditionally approve, or disapprove the samples within the time specified, the Contracting Officer shall automatically extend the shipping schedule in accordance with article 12 "Notice of Compliance with Schedules" of contract clauses in GPO Contract Terms (Pub. 310.2, effective December 1, 1987 (Rev. 6-01)).

Manufacture of the final product prior to approval of the prior-to-production samples is at the contractor's risk. Samples will not be returned to the contractor. All samples shall be manufactured at the facilities in which the contract production quantities are to be manufactured.

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No.12" dated March 2011.

Color of paper furnished shall be of a uniform shade and a close match by visual inspection of the JCP and/or attached color sample(s). The Contracting Officer reserves the right to reject shipments of any order printed on paper the color of which, in his opinion, materially differs from that of the color sample(s).

All stock/paper used in each copy must be of a uniform shade.

See description on pages 13 to 21.

PRINTING/COMPUTERIZED IMAGING: Print/Image as indicated on pages 13 through 21. Match Pantone Number as indicated on the individual print order. Computerized imaging is defined as waterproof ink jet spray or high-density laser is the preferred method for printing variable data onto cards. Computer imaging must have a minimum resolution of 300 x 300 dpi.

MARGINS: Bleeds throughout. See item descriptions on pages 13 through 21. Margins for the side printed with "Business Reply Mail" must comply with USPS Publication 25 and Domestic Mail Manual (DMM).

LABELING AND MARKING: Refer to Contract Terms and furnished Form 905.

PACKING: Pack bulk shipments in shipping containers furnished by the contractor. Containers are not to exceed 45 pounds when fully packed.

DISTRIBUTION: Mail f.o.b. contractor's city using the provided Government "G-Permit" imprint via presorted "First Class Mail, U.S. Postage Paid".

MAIL PREPARATION: All envelopes, with the exception of the return envelope in the Foreign Initial Enrollment Package will have a printed CMS Mail Postage and Fees Paid permit. The contractor is cautioned to use the permit imprint only for mailing material produced under this contract. Using the CMS address information as provided, the contractor is required to obtain the maximum USPS postage discounts possible in accordance with the USPS First Class mail automated mail discount structure in effect at the time of mailing. In compliance with USPS Mail Preparation & Sortation Regulations, all mail must be appropriately marked and supported with the documentation necessary to ensure USPS acceptance.

Mailing Envelopes must be prepared and sealed in a manner that will ensure acceptance, security and safe delivery by the U.S. Postal Service. Gather each piece and insert into mailing envelope, and seal.

The contractor must provide all mailing materials, as well as all labeling and marking, as necessary to fulfill mailing and distribution requirements. Noncompliance with the packing and labeling instructions will be cause for the Government to take corrective action in accordance with GPO Pub. 310.2.

Addresses for this mailing come from a Government maintained file. For this mailing, CMS will provide certificates indicating that within 95 days the addresses have been matched against both the USPS required Coding Accuracy Support System (CASS) and National Change of Address (NCOA) software.

In the event that the CASS and NCOA certification has expired, the contractor may be required to provide the certification prior to mailing. Reimbursement for this service will be made via contract modification.

Contractor sponsored address data enhancements to secure postal discount **MUST NOT** negatively affect deliverability and/or omit/change any required address field as provided by CMS address files. It is the contractor's responsibility to keep up to date on all USPS requirements.

Any address/mail management related questions/issues may be directed to Tina Dickens, CMS, at (410) 786-3895, or E-mail tina.dickens@cms.hhs.gov.

NOTE: THIS IS A REMINDER; DO NOT CHANGE ADDRESS FIELDS ON MEDICARE FOREIGN INITIAL ENROLLMENT PACKAGE AND MEDICARE PUERTO RICAN INITIAL ENROLLMENT PACKAGE – Contractor is **NOT** to run the Puerto Rican and Foreign Initial Enrollment Package files through addressing/mailing software. Image address information as formatted.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for domestic presorted First-Class mail, (note exception to Puerto Rican and Foreign IEP's above) mailing as applicable, and must be prepared for the most cost effective mailing rate/class obtainable, including ZIP + 4, bar-coding, and presorting for maximum postal automation discounts (as applicable). The placement and application of the full-service Intelligent Mail Barcode (IMb) must not compromise any applicable USPS addressing/imprinting requirements.

In addition, USPS has instituted a verification procedure called a "tap" test. This test is used to screen all mailings with barcoded inserts for proper barcode spacing within the envelope window. USPS will randomly select samples from a mailing and tap the pieces on their left, right, and bottom edges to test whether the barcode maintains a minimum spacing of 1/8" from the left and right edges and 1/16" from the top and bottom edges of the window. When an insert showing through the window is moved to any of its limits inside the envelope, the entire barcode must remain within the barcode clear zone, a clear space must be maintained that is at least 1/8" between the barcode and the left and right edges of the window and at least 1/25" between the barcode and the top edge of the window. Mail pieces are not to be tapped upside down (i.e., on their top edge).

All mailed copies must be sorted using the ZIP + 4 code. **Exception – Puerto Rican Package Addresses must only display +4 codes from CMS provided address file.**

Intelligent Mail Barcode (IMb): During the term of this contract, CMS mailers will be required to meet USPS requirements for using **Intelligent Mail** barcodes to access automation postal rates for presort first class mail. **Full Service IMb will be required for Domestic Mail only.**

The successful bidder **must** understand and be able to implement all mail preparation requirements enacted by the Postal Service related to using full-service **Intelligent Mail.** The requirements include, but are not limited to, preparing Intelligent Mail barcodes for the mail, trays and containers meeting USPS quality acceptance standards. Experience with assigning unique numbers for each mail piece, submitting postage statements and mailing documentation electronically, making electronic appointments, producing revised tray/pallet label formats and other similarly-detailed IMB requirements as mandated by the Postal Service is essential.

Any address/mail management related questions/issues may be directed to Tina Dickens, CMS, at (410) 786-3895, or E-mail tina.dickens@cms.hhs.gov

CERTIFICATE OF CONFORMANCE: When using Permit Imprint Mail the contractor must complete GPO Form 712 – Certificate of Conformance (Rev. 1-85) supplied by GPO and the appropriate mailing statement or statements supplied by USPS.

MAILING STATEMENTS: Contractor must complete and supply all copies of applicable and appropriate version, USPS form 3600 and GPO 712's to CMS within 2 work days of USPS certification. Copies must be sent to HHS/CMS, 7500 Security Blvd., Room SL-12-17, Baltimore, MD 21207 Attn: Clint Howard or emailed to clinton.howard@cms.hhs.gov.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for "Domestic Mail" or "International Mail" as applicable.

The contractor is cautioned that the Government Permit Imprint indicia may be used only for the purpose of mailing material produced under this contract.

The ship/deliver date indicated on the print order is the date products must be mailed.

NOTE: THE CONTRACTOR WILL BE RESPONSIBLE FOR PAYMENT OF ANY ADDITIONAL POSTAGE RESULTING FROM A LOSS OF DISCOUNT AND/OR UNDELIVERABLES CAUSED BY FAILURE TO CONFORM TO USPS REUIREMENTS.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the individual print order (GPO Form 2511).

The print orders will be furnished via fax or e-mail to the contractor and will be made available for picked up at CMS along with any furnished material.

Contractor will be required to verify that the CMS furnished files and quantity(s) are available in their TIBCO mailbox within two hours of receipt of print order.

Furnished material must be picked up from and delivered to: CMS, Attn: Clinton Howard, Room SL-12-17, 7500 Security Blvd., Baltimore, MD 21244-1850. Inside delivery is required to the room number indicated. Inside delivery is defined as delivery into a Government controlled space as directed.

If agent picks up material/proofs, the contractor must provide an adequate supply of completed manifests (airbills) to the agency placing the orders, listing his firm as both the shipper and the consignee.

The following schedule begins the workday after notification of the availability of print order and furnished material; the workday after notification will be the first workday of the schedule.

ORDERS WITHOUT PROOFS AND PRIOR-TO-PRODUCTION SAMPLES:

Complete production and distribution must be made within 5 workdays for the following:
A. MEDICARE DOMESTIC INITIAL ENROLLMENT PACKAGE, AND
D. MEDICARE ENGLISH GENERAL ENROLLMENT PACKAGE.

Complete production and distribution must be made within 4 workdays for the following:
B. MEDICARE PUERTO RICAN INITIAL ENROLLMENT PACKAGE,
C. MEDICARE FOREIGN INITIAL ENROLLMENT;
F. REPLACEMENT MEDICARE CARDS AND
G. DEEMED MEDICARE CARDS:

ORDERS REQUIRING PROOFS AND PRIOR-TO-PRODUCTION SAMPLES:

The following schedule begins the workday after notification of the availability of print order and furnished material. The numbers under the column headed "WD After" represent the number of workdays allowed to complete that certain part of the schedule after completion of the preceding part.

	WD After
Contractor deliver proofs	5
Agency approves proofs (marked "OK to Print" or "OK to Print with Corrections")	2
Contractor deliver prior-to-production samples	5
Agency approves prior-to-productions samples	2
Complete production and distribution	5

Revised Proofs: When revised proofs are required by the Government due to Government errors, 2 additional workdays will be allowed.

(A, B & C) MEDICARE DOMESTIC, PUERTO RICAN, AND FOREIGN INITIAL ENROLLMENT PACKAGE: It is anticipated that the print order and TIBCO files will be available during the second full week of each month, except for holidays.

(D and E) MEDICARE ENGLISH AND SPANISH GENERAL ENROLLMENT PACKAGE: It is anticipated that the print order and TIBCO files will be available on the second full week of each month, except for holidays.

F. REPLACEMENT MEDICARE CARDS: It is anticipated that the print order and TIBCO files will be available on Friday of each week, except for holidays.

G. DEEMED MEDICARE CARDS: It is anticipated that the print order and TIBCO files will be available during the month of February each year, except for holidays.

ALL PACKAGES: One additional workday will be allowed for every 75,000 copies that exceed 200,000.

RECEIPT FOR DELIVERY: Contractor must furnish their own receipts for delivery. These receipts must include the GPO jacket, program, and print order numbers; total quantity delivered, number of cartons, and quantity per carton; and date delivery made and signature of the Government agent accepting delivery. The original copy of this receipt must accompany the contractor's voucher for payment.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with the order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information.

RETURN OF GOVERNMENT FURNISHED PROPERTY: The contractor must return all material furnished by the Government along with any reproducibles made by the contractor, together with one copy of the Certificate of Conformance (GPO Form 712), within 5 workdays after completion of mailing to the address provided at the post-award telephone conference.

These materials must be packaged, properly labeled, and returned separate from the entire job. The contractor must be able to produce a separate signed receipt for these materials at any time during the contract.

All expenses incidental to pickup/return of materials/proofs, and furnishing sample copies must be borne by the contractor.

SECTION 3. – DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "Schedule of Prices" to the following units of production which are the estimated requirements to produce 1 year's orders under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered for a like period of time.

The following item designations correspond to those listed in the "Schedule of Prices".

I.	(1)	(2)
A.	12	2,196
B.	12	36
C.	12	12
D.	1	694
E.	1	11
F.	52	6,084
G.	1	22

SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city by Government "G Permit".

Prices must be submitted for the entire term of the contract and bids qualified for a lesser period will not be considered.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids, may be declared nonresponsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government. Bids submitted with NB (No Bid) or blank spaces for an item may be declared nonresponsive.

NOTE CONTRACTOR: THE COST OF COMPLETING ALL PAPER WORK ASSOCIATED WITH THE COMPLECTION OF THE BACKGROUND INVESTIGATIONS; INCLUDING COMPLETING FORMS IN E-QIP, FOR TWO EMPLOYEES MUST BE INCLUDED IN THE SCHEDULE OF PRICES.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the Determination of Award) that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

All vouchers submitted to the GPO shall be based on the most economical method of production.

Fractional parts of 1,000 will be prorated at the per 1,000 rate.

I. COMPLETE PRODUCT: Prices offered shall include the cost of all required materials and operations necessary for the complete production and delivery in accordance with these specifications.

A. MEDICARE DOMESTIC INITIAL ENROLLMENT PACKAGE:
   (1) Makeready and/or setup charge ..... per order ..... $_____
   (2) Running per 1,000 copies..... per order ..... $_____

B. MEDICARE PUERTO RICAN INITIAL ENROLLMENT PACKAGE:
   (1) Makeready and/or setup charge ..... per order ..... $_____
   (2) Running per 1,000 copies..... per order ..... $_____

C. MEDICARE FOREIGN INITIAL ENROLLMENT PACKAGE:
   (1) Makeready and/or setup charge ..... per order ..... $_____
   (2) Running per 1,000 copies..... per order ..... $_____

_____
(Initials)

RETURN THIS PAGE TO RPPO, COLUMBUS, OH

SCHEDULE OF PRICES

D. MEDICARE ENGLISH GENERAL ENROLLMENT PACKAGE:
(1) Makeready and/or setup charge ..... per order ..... $_____
(2) Running per 1,000 copies..... per order ..... $_____

E. MEDICARE SPANISH GENERAL ENROLLMENT PACKAGE:
(1) Makeready and/or setup charge ..... per order ..... $_____
(2) Running per 1,000 copies..... per order ..... $_____

F. REPLACEMENT MEDICARE CARDS:
(1) Makeready and/or setup charge ..... per order ..... $_____
(2) Running per 1,000 copies..... per order ..... $_____

G. DEEMED MEDICARE CARDS:
(1) Makeready and/or setup charge ..... per order ..... $_____
(2) Running per 1,000 copies..... per order ..... $_____

BID SUBMISSION AND BIDDER'S NAME AND SIGNATURE: Fill out and return all pages in "Section 4. – Schedule of Prices", initial or sign each in the space provided. See page 1 for instructions on how and where to submit bid.

Fill out and return GPO Form 910. The schedule of prices will prevail in instances where prices are inadvertently entered on GPO Form 910.

GPO Form 910 is available on GPO web site at http://www.gpo.gov/pdfs/vendors/sfas/bids910.pdf

Bidder _____
(Company Name)

_____
(Address, City, and State)

By _____
(Signature and title of person authorized to sign this bid)

_____ _____ _____
(Person to be contacted) (Telephone Number) (Fax Number)

_____ _____
(E-Mail Address(s)) (Contractor Code Number)

Mailings made from: _____
(City and State)

RETURN THIS PAGE TO RPPO, COLUMBUS, OH

EXHIBIT 1
CMS CLAUSE 11: CMS INFORMATION SECURITY
PAGE 1 OF 2

CMS Clause-11
CMS Information Security
Date: April 2008
Page 1 of 2

This clause applies to all organizations which possess or use Federal information, or which operate, use or have access to Federal information systems (whether automated or manual), on behalf of CMS.

The central tenet of the CMS Information Security (IS) Program is that all CMS information and information systems shall be protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft—whether accidental or intentional. The security safeguards to provide this protection shall be risk-based and business-driven with implementation achieved through a multi-layered security structure. All information access shall be limited based on a least-privilege approach and a need-to-know basis, i.e., authorized user access is only to information necessary in the performance of required tasks. Most of CMS' information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such, has access restrictions as required under legislative and regulatory mandates.

The CMS IS Program has a two-fold purpose:

(1) To enable CMS' business processes to function in an environment with commensurate security protections, and

(2) To meet the security requirements of federal laws, regulations, and directives.

The principal legislation for the CMS IS Program is Public Law (P.L.) 107-347, Title III, *Federal Information Security Management Act of 2002 (FISMA)*, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. FISMA places responsibility and accountability for IS at all levels within federal agencies as well as those entities acting on their behalf. FISMA directs Office of Management and Budget (OMB) through the Department of Commerce, National Institute of Standards and Technology (NIST), to establish the standards and guidelines for federal agencies in implementing FISMA and managing cost-effective programs to protect their information and information systems. As a contractor acting on behalf of CMS, this legislation requires that **the Contractor shall**:

- Establish senior management level responsibility for IS,
- Define key IS roles and responsibilities within their organization,
- Comply with a minimum set of controls established for protecting all Federal information, and
- Act in accordance with CMS reporting rules and procedures for IS.

Additionally, the following laws, regulations and directives and any revisions or replacements of same have IS implications and are applicable to all CMS contractors.

- P.L. 93-579, *The Privacy Act of 1974*, http://www.usdoj.gov/oip/privstat.htm , (as amended);
- P.L. 99-474, *Computer Fraud & Abuse Act of 1986*, www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf P.L. 104-13,

EXHIBIT 1
CMS CLAUSE 11: CMS INFORMATION SECURITY
PAGE 2 OF 2

CMS Clause-11
CMS Information Security
Date: April 2008
Page 2 of 2

Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35, www.archives.gov/federal-register/laws/paperwork-reduction;

- P.L. 104-208, *Clinger-Cohen Act of 1996* (formerly known as the Information Technology Management Reform Act), http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html;
- P.L. 104-191, *Health Insurance Portability and Accountability Act of 1996* (formerly known as the Kennedy-Kassenbaum Act) http://aspe.hhs.gov/admnsimp/pl104191.htm;
- OMB Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004, http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html;
- OMB Circular A-130, *Management of Federal Information Resources*, Transmittal 4, November 30, 2000, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html;
- NIST standards and guidance, http://csrc.nist.gov/; and,
- Department of Health and Human Services (DHHS) regulations, policies, standards and guidance http://www.hhs.gov/policies/index.html

These laws and regulations provide the structure for CMS to implement and manage a cost-effective IS program to protect its information and information systems. Therefore, **the Contractor shall** monitor and adhere to all IT policies, standards, procedures, directives, templates, and guidelines that govern the CMS IS Program, http://www.cms.hhs.gov/informationsecurity and the CMS System Lifecycle Framework, http://www.cms.hhs.gov/SystemLifecycleFramework.

The Contractor shall comply with the CMS IS Program requirements by performing, but not limited to, the following:

- Implement their own IS program that adheres to CMS IS policies, standards, procedures, and guidelines, as well as industry best practices;
- Participate and fully cooperate with CMS IS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities;
- Provide upon request results from any other audits, reviews, evaluations, tests and/or assessments that involve CMS information or information systems;
- Report and process corrective actions for all findings, regardless of the source, in accordance with CMS procedures;
- Document its compliance with CMS security requirements and maintain such documentation in the systems security profile;
- Prepare and submit in accordance with CMS procedures, an incident report to CMS of any suspected or confirmed incidents that may impact CMS information or information systems; and
- Participate in CMS IT information conferences as directed by CMS.

EXHIBIT 2
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 1 OF 5

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 1 of 5

CMS SPECIFIC PROVISIONS FOR ALL NEW SOLICITATIONS AND CONTRACTS:

Security Clause -Background - Investigations for Contractor Personnel

If applicable, Contractor personnel performing services for CMS under this contract, task order or delivery order shall be required to undergo a background investigation. CMS will initiate and pay for any required background investigation(s).

After contract award, the CMS Project Officer (PO) and the Security and Emergency Management Group (SEMG), with the assistance of the Contractor, shall perform a position-sensitivity analysis based on the duties contractor personnel shall perform on the contract, task order or delivery order. The results of the position-sensitivity analysis will determine first, whether the provisions of this clause are applicable to the contract and second, if applicable, determine each position's sensitivity level (i.e., high risk, moderate risk or low risk) and dictate the appropriate level of background investigation to be processed. Investigative packages may contain the following forms:

1. SF-85, Questionnaire for Non-Sensitive Positions, 09/1995
2. SF-85P, Questionnaire for Public Trust Positions, 09/1995
3. OF-612, Optional Application for Federal Employment, 12/2002
4. OF-306, Declaration for Federal Employment, 01/2001
5. Credit Report Release Form
6. FD-258, Fingerprint Card, 5/99, and
7. CMS-730A, Request for Physical Access to CMS Facilities (NON-CMS ONLY), 11/2003.

The Contractor personnel shall be required to undergo a background investigation commensurate with one of these position-sensitivity levels:

1) High Risk (Level 6)
Public Trust positions that would have a potential for exceptionally serious impact on the integrity and efficiency of the service. This would include computer security of a major automated information system (AIS). This includes positions in which the incumbent's actions or inaction could diminish public confidence in the integrity, efficiency, or effectiveness of assigned government activities, whether or not actual damage occurs, particularly if duties are especially critical to the agency or program mission with a broad scope of responsibility and authority.

Major responsibilities that would require this level include:

a. development and administration of CMS computer security programs, including direction and control of risk analysis and/or threat assessment;

EXHIBIT 2
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 2 OF 5

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 2 of 5

b. significant involvement in mission-critical systems;
c. preparation or approval of data for input into a system which does not necessarily involve personal access to the system but with relatively high risk of causing grave damage or realizing significant personal gain;
d. other responsibilities that involve relatively high risk of causing damage or realizing personal gain;
e. policy implementation;
f. higher level management duties/assignments or major program responsibility; or
g. independent spokespersons or non-management position with authority for independent action.

2) Moderate Risk (Level 5)
Level 5 Public Trust positions include those involving policymaking, major program responsibility, and law enforcement duties that are associated with a "Moderate Risk." Also included are those positions involving access to or control of unclassified sensitive, proprietary information, or financial records, and those with similar duties through which the incumbent can realize a significant personal gain or cause serious damage to the program or Department. Responsibilities that would require this level include:

a. the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the High Risk level to ensure the integrity of the system;
b. systems design, operation, testing, maintenance, and/or monitoring that are carried out under the technical review of a higher authority at the High Risk level;
c. access to and/or processing of information requiring protection under the Privacy Act of 1974;
d. assists in policy development and implementation;
e. mid-level management duties/assignments;
f. any position with responsibility for independent or semi-independent action; or
g. delivery of service positions that demand public confidence or trust.

3) Low Risk (Level 1)
Positions having the potential for limited interaction with the agency or program mission, so the potential for impact on the integrity and efficiency of the service is small. This includes computer security impact on AIS.

The Contractor shall submit the investigative package(s) to SEMG within three (3) days after being advised by the SEMG of the need to submit packages. Investigative packages shall be submitted to the following address:

EXHIBIT 2
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 3 OF 5

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 3 of 5

Centers for Medicare & Medicaid Services
Office of Operations Management
Security and Emergency Management Group
Mail Stop SL-13-15
7500 Security Boulevard
Baltimore, Maryland 21244-1850

The Contractor shall submit a copy of the transmittal letter to the Contracting Officer (CO).

Contractor personnel shall submit a CMS-730A (Request for Badge) to the SEMG (see attachment in Section J). The Contractor and the PO shall obtain all necessary signatures on the CMS-730A prior to any Contractor employee arriving for fingerprinting and badge processing.

The Contractor must appoint a Security Investigation Liaison as a point of contact to resolve any issues of inaccurate or incomplete form(s). Where personal information is involved, SEMG may need to contact the contractor employee directly. The Security Investigation Liaison may be required to facilitate such contact.

SEMG will fingerprint contractor personnel and send their completed investigative package to the Office of Personnel Management (OPM). OPM will conduct the background investigation. Badges will not be provided by SEMG until acceptable finger print results are received; until then the contractor employee will be considered an escorted visitor. The Contractor remains fully responsible for ensuring contract, task order or delivery order performance pending completion of background investigations of contractor personnel.

SEMG shall provide written notification to the CO with a copy to the PO of all suitability decisions. The PO shall then notify the Contractor in writing of the approval of the Contractor's employee(s), at that time the Contractor's employee(s) will receive a permanent identification badge. Contractor personnel who the SEMG determines to be ineligible may be required to cease working on the contract immediately.

The Contractor shall report immediately in writing to SEMG with copies to the CO and the PO, any adverse information regarding any of its employees that may impact their ability to perform under this contract, task order or delivery order. Reports should be based on reliable and substantiated information, not on rumor or innuendo. The report shall include the contractor employee's name and social security number, along with the adverse information being reported.

Contractor personnel shall be provided an opportunity to explain or refute unfavorable information found in an investigation to SEMG before an adverse adjudication is made. Contractor personnel may request, in writing, a copy of their own investigative results by contacting:

EXHIBIT 2
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 4 OF 5

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 4 of 5

Office of Personnel Management
Freedom of Information
Federal Investigations Processing Center
PO Box 618
Boyers, PA 16018-0618.

At the Agency's discretion, if an investigated contractor employee leaves the employment of the contractor, or otherwise is no longer associated with the contract, task order, or delivery order within one (1) year from the date the background investigation was initiated by CMS, then the Contractor may be required to reimburse CMS for the full cost of the investigation. The amount to be paid by the Contractor shall be due and payable when the CO submits a written letter notifying the Contractor as to the cost of the investigation. The Contractor shall pay the amount due within thirty (30) days of the date of the CO's letter by check made payable to the "United States Treasury." The Contractor shall provide a copy of the CO's letter as an attachment to the check and submit both to the Office of Financial Management at the following address:

Centers for Medicare & Medicaid Services
PO Box 7520
Baltimore, Maryland 21207

The Contractor must immediately provide written notification to SEMG (with copies to the CO and the PO) of all terminations or resignations of Contractor personnel working on this contract, task order or delivery order. The Contractor must also notify SEMG (with copies to the CO and the PO) when a Contractor's employee is no longer working on this contract, task order or delivery order.

At the conclusion of the contract, task order or delivery order and at the time when a contractor employee is no longer working on the contract, task order or delivery order due to termination or resignation, all CMS-issued parking permits, identification badges, access cards, and/or keys must be promptly returned to SEMG. Contractor personnel who do not return their government-issued parking permits, identification badges, access cards, and/or keys within 48 hours of the last day of authorized access shall be permanently barred from the CMS complex and subject to fines and penalties authorized by applicable federal and State laws.

Work Performed Outside the United States and its Territories

The contractor, and its subcontractors, shall not perform any activities under this contract at a location outside of the United States, including the transmission of data or other information outside the United States, without the prior written approval of the Contracting Officer. The factors that the Contracting Officer will consider in making a decision to authorize the performance of work outside the United States include, but are not limited to the following:

EXHIBIT 2
CMS CLAUSE 09A-01 SECURITY CLAUSE
PAGE 5 OF 5

CMS Clause-09A-01
Security Clause – New Contract Awards
Date: May 2007
Page 5 of 5

1. All contract terms regarding system security
2. All contract terms regarding the confidentiality and privacy requirements for information and data protection
3. All contract terms that are otherwise relevant, including the provisions of the statement of work
4. Corporate compliance
5. All laws and regulations applicable to the performance of work outside the United States
6. The best interest of the United States

In requesting the Contracting Officer's authorization to perform work outside the United States, the contractor must demonstrate that the performance of the work outside the United States satisfies all of the above factors. If, in the Contracting Officer's judgment, the above factors are not fully satisfied, the performance of work outside the United States will not be authorized. Any approval to employ or outsource work outside of the United States must have the concurrence of the CMS SEMG Director or designee.

EXHIBIT 3
FAQ SUPPLEMENT TO CMS SECURITY CLAUSE 09A-01
PAGE 1 OF 3

FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008
Page 1 of 3

CMS Security Clause 09A-01 is a mandatory clause required in all CMS contracts that require background investigations. This Frequently Asked Questions (FAQ) Supplement provides additional information specific to CMS print/mail contracts.

Acronyms
CMS – Centers for Medicare & Medicaid Services, Department of Health and Human Services
OMB – Office of Management and Budget, Executive Office of the President
OPM – United States Office of Personnel Management
PO – CMS Project Officer
PS – CMS Printing Specialist
PSC -- Program Support Center, Department of Health and Human Services
PII – Personally Identifiable Information (i.e. beneficiary name and address)
PIV – Personal Identity Verification
SEMG – CMS Security & Emergency Management Group

Who must apply for and receive a background investigation?
Contractor personnel with access to CMS' beneficiary PII under this contract *may be* required to undergo a background investigation. At a minimum, the two applicants for access to the Gentran mailbox *must* undergo a background investigation anticipated to be at a Public Trust Level 5. Depending on the outcome of the Preaward Security Survey and/or discussion at the Postaward Conference, additional contractor employees and/or subcontractors may be required to undergo background investigations. It is possible that everyone with access to the data processing and production areas, including janitors and maintenance technicians, must undergo a background investigation. SEMG and the PO will make this determination at the Postaward Conference.

Will production employees working on a different production line in the same room be subject to a CMS investigation? Even if they aren't working on a CMS job?
That will be determined by SEMG and the PO at the Postaward Conference. Depending on the sensitivity of the CMS job, it may be necessary to perform a background investigation on everyone with access to all work areas that contain CMS PII during performance of this contract. However, if the production line running the CMS job has limited and controlled access from other production lines, then workers outside of this area would not be subject to a CMS investigation.

What is a Security Investigation Liaison?
The contractor must appoint a Security Investigation Liaison to handle confidential personnel issues that may arise at any point during the background investigation process, and to serve as a point of contract to the Government for background investigation issues. The Liaison's duties will include attending the Postaward Conference, submitting background applications timely, and resolving any issues of inaccurate or incomplete data supplied by background investigation applicants. Where personal information is involved, SEMG may need to contact the background investigation applicant directly. The Security Investigation Liaison may be required to facilitate such contact. It is up to the contractor to decide if this should be the same or a different person who handles technical issues.

EXHIBIT 3
FAQ SUPPLEMENT TO CMS SECURITY CLAUSE 09A-01
PAGE 2 OF 3

FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008
Page 2 of 3

Where may I find copies of the forms listed in CMS Security Clause 09A-01?

Forms SF-85, SF-85P, OF-612, and OF-306 can be found on: www.forms.gov . However, applicants may not actually fill out these forms. These forms are listed for the similar data to be collected through "e-QIP" an online background investigation application process; more about that later in this FAQ.

The Credit Report Release Form and the FD-258 Fingerprint Card will be provided if deemed applicable at the Postaward Conference.

Form CMS-730A is provided as an attachment to this contract, contractor may reproduce as necessary at no cost to the Government. Contractor must submit a completed CMS-730A for each background investigation applicant to the PS within 5 workdays after notification by the PS Original signatures are required on this form; therefore, photocopied signatures or fax transmission is not acceptable.

The Contractor is also required to submit a PIV Spreadsheet listing all background investigation applicants. This Microsoft Excel spreadsheet will be provided to the contractor by the PS after the Postaward Conference. The PIV Spreadsheet collects the following information for each background investigation applicant: SSN, Last Name, First Name, Middle Name, Suffix, Birth Date, City of Birth, County of Birth, Country of Birth, E-mail Address, Home Phone, Previous Federal Government Background Investigations Performed, and Contracting Firm.

Send completed forms to the PS; not to the SEMG address listed on page 3 of the attached CMS Clause-09A-01. As soon as the completed forms are prepared for shipment, the contractor must e-mail transmittal information (carrier, tracking numbers, estimated time of arrival at CMS) to the PS. Email addresses will be provided at the Postaward Conference.

What is "e-QIP"?

E-QIP is a secure internet website sponsored by OPM for submission of background investigation application information. After receipt of the properly completed CMS-730A forms and PIV spreadsheet, SEMG will notify Contractor's Security Liaison that background investigation applicants are invited to enter "e-QIP". Background investigation applicants will have a 14 calendar day window to complete the e-QIP online submission. The information requested in e-QIP is similar to Forms SF-85 and SF-85P. OMB has estimated the time to complete the e-QIP application takes an average of 120 minutes. At time of e-QIP invitation notification, SEMG will also notify the Security Liaison if paper copies of Forms OF-612 and OF-306 must also be submitted by the applicants within the same 14 day window. Potential bidders may find additional information about e-QIP on the internet at: http://www.opm.gov/e-qip/ .

Why do I have to fill out a "Request for Physical Access to CMS Facilities" form?

While it is not anticipated that any contractor personnel will need physical access to CMS property, Form CMS-730A is also used to authorize CMS to perform a background investigation and to certify receipt of Privacy Act information by the applicant. Failure to provide a completed Form CMS-730A will cause a denial of access to CMS computer systems.

Why do I have to travel to CMS Central Office for fingerprinting?

CMS prefers to process electronic fingerprints generated in CMS or PSC offices. Electronic fingerprinting services are available at no cost at the CMS Central Office in Baltimore, and for a fee at each of the regional PSC offices. PSC offices are located in downtown Federal buildings in

EXHIBIT 3
FAQ SUPPLEMENT TO CMS SECURITY CLAUSE 09A-01
PAGE 3 OF 3

the following cities: Boston, New York City, Philadelphia, Atlanta, Chicago, Dallas, Kansas City, Denver, San Francisco, and Seattle. Information regarding PSC locations, hours, fees, and procedures may be obtained by emailing: security@psc.hhs.gov .

If the contractor is unable to go to the above locations for electronic fingerprints, CMS will allow the contractor to obtain ink fingerprints (non-electronic) from their local police department. **Two sets** of ink fingerprints on FD-258 hard cards must be submitted to CMS directly from the police department. CMS will supply the contractor with blank FD-258 hard cards and a self addressed, stamped Priority Mail envelope for the contractor to give the police department for return of the fingerprint cards to CMS.

At the Postaward Conference, the contractor must be prepared to discuss where fingerprints will be obtained.

A number of my employees have undergone background checks by another Federal agency. Do they have to repeat the process for CMS?

That will be decided by SEMG and the PO at the Postaward Conference. If the employee performs a duty that requires a background investigation, and they have had a background investigation successfully performed by another Federal entity within the last year, then they may not have to repeat the entire process. That employee will still have to submit a CMS-730A and be listed on a PIV spreadsheet.

What happens if I don't report terminations, resignations, or adverse information of cleared people? If I do, you are going to charge me up to $2,900 for the cost of the investigation.

The person assigned the User ID, and the contractor's company, remains responsible for all data collected via the Gentran mailbox. Failure to report terminations and resignations could result in this contract being terminated for default.

Reporting of adverse information will be investigated by SEMG and handled appropriately considering the nature of the adverse information. It is possible the User ID may be terminated immediately and the contractor may have to initiate clearance for another employee.

Is the investigation good for the entire term of the contract, including all option years?

Access to the Gentran mailbox must be renewed annually or the User ID will be revoked. The CMS-730A and PIV spreadsheet must also be submitted annually. Fingerprinting and entering data into e-QIP should only occur once unless there are changes to the employee's record that necessitate updates.

Is it possible that I can perform work outside the United States and its Territories?

No, not on contracts for CMS print/mail requirements.

EXHIBIT 4
REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (FORM CMS-730A)
PAGE 1 OF 4

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approval
OMB No. 0938-0812

REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (NON-CMS ONLY) Date _____

PART I — TO BE COMPLETED BY REQUESTOR *(Please type or print)*

Social Security Number | Phone Number *(include extension)*

Applicant's Name *(Print Clearly)* *(Last)* *(First)* *(Middle)*

Contract Company Name *(if subcontractor, include parent company)*

PART II — REASON FOR APPLICATION *(Required)*

Reason:
- ❑ Change in job requirements
- ❑ Renewal
- ❑ Initial Issuance
- ❑ Replacement due to loss
- ❑ Name change from *(Print former name below)*: _____

PART III — TYPE OF BADGE *(Required for initial issuance only)*

Type:
- ❑ Contractor
- ❑ Security
- ❑ Former HCFA/CMS Employee *(Ethics Officer Signature required)*

_____

PART IV — ELECTRONIC ACCESS *(required for all accesses to CMS secured areas)* (Pin # Selection - Pin # *(4 digit)* ___ ___ ___ ___

ELECTRONIC ACCESSES *(check all accesses needed to perform duties)*:
- ❑ CMS Data Center
- ❑ Voice Data Switch
- ❑ LBD ADP Room
- ❑ ITF Room
- ❑ Mailroom
- ❑ LBD Voice Room
- ❑ Secure Server
- ❑ ASG Siteman
- ❑ Gov. Court
- ❑ CDC Warehouse
- ❑ 'S' Sign-in Authority *(*see bold statement in Privacy Act on reverse side)*

❑ ADP Satellite Room(s) — *(specify room numbers)*

PART V — ELECTRONIC ACCESS JUSTIFICATION *(Required for all accesses requested in PART IV)*

Electronic Access Justification

PART VI — PROPERTY PASS INFORMATION

Property Description
1 _____
2 _____

Property Serial No.
1 _____
2 _____

OOM/SSS Authorization
_____

PART VII — BACKGROUND INVESTIGATION

- ❑ Non-Sensitive **LEVEL 1**
- ❑ Public Trust **LEVEL 5**
- ❑ Public Trust **LEVEL 6**

PART VII — AUTHORIZATIONS *(required)*

Project Officer – *(Print name clearly)* Phone Number

Project Officer – Signature Date

Note: You are required to collect Government issued ID and/or Access Card(s) at end of Contractor's project.

Contract Officer – *(Print name clearly)* Phone Number

Contract Officer – Signature Date

Contract Number

Contract Expiration Date

Form CMS-730A (11/03) (ALL OTHER EDITIONS OBSOLETE)

EXHIBIT 4
REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (FORM CMS-730A)
PAGE 2 OF 4

PRIVACY ACT ADVISORY STATEMENT

As required by 5 U.S.C. 552a (The Privacy Act of 1974 and Executive Order No.9397), you are advised that the Centers for Medicare & Medicaid Services (CMS) is authorized to collect the data on this form by 63 Stat. 390, 40 U.S.C. 86(c), and 41 C.F.R. 101-20.111. Your response to the questions on this form is not required by law. However, if you do not provide this information, your application for privileges may be denied or delayed in processing. No disclosure of this information will be made unless required by law or with written consent.

The information on side 1 of this form is collected and maintained under the authority of 41 CFR 101-20.302, "Conduct on Federal Property" and "OMB Circular A-123, Internal Control Systems." This information is used for assigning, controlling, tracking and reporting permanently or temporarily issued unescorted access into a Government Facility. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances. Public Law 93-579, the Privacy Act of 1974, provides penalties of up to $5,000 for willful disclosure of material in any manner to any person or agency not entitled to protected information, which includes the utilization of your badge to sign-in individuals or groups which you do not escort throughout the complex. ***Your signature authorizing admittance to anyone into any CMS facility means that you are responsible for the whereabouts and conduct of said person(s). Please be advised that all persons being signed in to the CMS facilities are considered visitors. ONLY Visitor badges will be issued. If any visitor is found unescorted within the complex, they may be escorted off the premises. By signing below you acknowledge and accept these requirements necessary for this privilege. If you are found to be in violation of any of these requirements, this privilege may be revoked.**

The information you furnish on this form will be maintained in the Records of Individuals Issued Card Key System (RICKS) and the CMS Employee Pass File (EMPASS) Systems of Record and may be disclosed as a routine use disclosure under those uses established for this system as published in the Federal Register and as CMS may establish in the future by publication in the Federal Register.

By signing below you accept the responsibility of being issued an official Civilian Government Employee Identification Badge. This includes immediate notification to the security office if your badge is lost or stolen.

All CMS Government issued identification, access cards, and parking permits must be returned to the ASG, Security and Safety Staff prior to the last day of employment at CMS, or expiration of authorized access. Individuals who do not return their Government issued Access card(s) within 48 hours following separation from CMS (regardless of contract date), will be permanently barred from the CMS complex and are subject to fines and penalties associated with theft of Government property under Federal Property Management Regulations, Title 41, Code of Federal Regulations, Preservation of Property Subpart 101-20.303.

_____ _____
Signature Date

REQUIRED APPROVALS

OIS / OOM Use Only

CARD NO._____

OIS/TMG Physical Security Officer for Computer Facilities _____

OOM/SSS Personnel Security Representative _____

Background Investigation Conducted ❑ Level 1 ❑ Level 5 ❑ Level 6

OOM/SSS Badging Personnel Initials _____

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0812. The time required to complete this information collection is estimated to average 15 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to CMS, Attn: PRA Reports Clearance Officer, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

Form CMS-730A (11/03) (ALL OTHER EDITIONS OBSOLETE) 2

EXHIBIT 4
REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (FORM CMS-730A)
PAGE 3 OF 4

INSTRUCTIONS: REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES

Prior to submitting form CMS-730A to the Security and Safety Staff, ASG, OOM (SLL-11-05), ALL required signatures MUST be obtained, otherwise this form will not be processed. NO EXCEPTIONS.

All forms, requiring electronic access to any CMS facility, must be submitted to the OIS/TMG Physical Security Officer for Computer Facilities (m/s N1-19-18 — desk N1-24-17).

NOTE: Each time a CMS-730A form is revised it supersedes the previous form. You must enter all accesses needed.

Purpose of this Form

Information from this form is used primarily as the basis to grant access to any CMS facility and secured areas.

Part I – Applicant Information: *(To be completed by Applicant – Required)*

SSN – Provide SSN
Phone Number – Provide the phone number where you can be contacted during duty hours.
Applicant's Name – Print full name clearly.
Company Name – Print company name *(clearly – if subcontractor, please include parent company name).*

Part II – Reason For Application: *(Required)*

Check the reason for this application.

Part III – Type of Badge: *(Required for initial issuance only)*

Enter type of badge needed.

PART IV – Electronic Access: *(Required for access to secured areas)*

Be sure to select a personal 4-digit pin number in the space provided.

Electronic Access areas *(secured areas)* should only be requested if you need them to perform your duties. A thorough justification is mandatory for anyone requesting electronic access (PART V).

PART V – Electronic Access Justification: *(Required for all accesses checked in PART IV)*

A thorough justification is required for all accesses requested in PART IV. Just stating access is needed will not be accepted as a justification.

PART VI – Property Pass Information:

Provide a description and serial number for each item you are bringing into the building.

EXHIBIT 4
REQUEST FOR PHYSICAL ACCESS TO CMS FACILITIES (FORM CMS-730A)
PAGE 4 OF 4

PART VII – Background Investigation:

Provide a level of investigation that corresponds to your job duties/responsibilities *(position sensitivity determination)*.

PART VIII – Authorizations: *(To be completed by Project Officer)*

Project Officer's Name – Print name clearly.
Project Officer's Signature – Sign name and date. *(see Note)*

Authorizations: *(To be completed by Contract Officer)*

Contract Officer's Name – Print name clearly.
Contract Officer's Signature – Sign name and date.
Contract Number – Provide the contract number of applicant's company.
Contract Expiration Date – Provide the contract expiration date of applicant's company.

You are responsible for reading the Privacy Act Statement on Page 2 of the Request for Physical Access to CMS Facilities Form. Your signature is required, as indicated under the Privacy Act Statement, to acknowledge you have read these requirements.

EXHIBIT 5
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 1 OF 3

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

EUA WorkFlow Request No.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

1. TYPE OF REQUEST *(Check only one)*:

- ❑ NEW *(Issue a CMS UserID)*
- ❑ CONNECT/DISCONNECT *(Add/remove access authorities)*
- ❑ CERTIFY *(Due date: ____/_____ mo yr)*
- ❑ CHANGE USER INFORMATION *(Note new info)*
- ❑ DELETE *(Remove CMS UserID from all CMS systems)*

USERID *(Capital Letters)*

2. USER INFORMATION

- ❑ CMS Employee
- ❑ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using HPMS Only
- ❑ Medicare Advantage / Medicare Advantage with Prescription Drug / Prescription Drug Plan / Cost Contracts – Using Other Systems
- ❑ CITIC Contractor
- ❑ Program Safeguard Contractor
- ❑ Medicare Contractor/Intermediary/Carrier
- ❑ Contractor (non-Medicare contract with CMS)
- ❑ Researcher
- ❑ Quality Improvement Organization
- ❑ End-Stage Renal Disease Network
- ❑ State Agency (State of _____)
- ❑ Federal Govt – Baltimore HR Center
- ❑ Federal Govt – Centers for Disease Control & Prevention
- ❑ Federal Govt – Commission Corps
- ❑ Federal Govt – Dept of Health & Human Services
- ❑ Federal Govt – HHS – OMHA
- ❑ Federal Govt – Dept of Justice
- ❑ Federal Govt – Dept of Veterans Affairs
- ❑ Federal Govt – Government Accountability Office
- ❑ Federal Govt – General Services Administration
- ❑ Federal Govt – Internal Revenue Service
- ❑ Federal Govt – Office of General Counsel
- ❑ Federal Govt – Office of Inspector General
- ❑ Federal Govt – Railroad Retirement Board
- ❑ Federal Govt – Social Security Administration
- ❑ Federal Govt – Other: _____
- ❑ Other: _____

First Name *(As you want it published)*	MI	Last Name *(As you want it published)*

Company/Organization/Department Name

Mailing Address *(Include Suite/Mailstop)*

City	State	ZIP Code

Office Telephone *(Include Extension)*	Company Telephone *(If different)*	E-Mail Address

IF CMS EMPLOYEE Org Name/Admin Code

Are you a Manager? ❑ Yes ❑ No

IF ONSITE AT CMS LOCATION CMS Region/Facility (Check One)

- ❑ R4 (AFC) Atlanta
- ❑ R10 (BLNCH) Seattle
- ❑ CO (CENTRAL) Central Office
- ❑ R5 (CHIICB) Chicago
- ❑ DC (COHEN) DC
- ❑ R6 (DAL1301) Dallas
- ❑ R8 (DENCSB) Denver
- ❑ R7 (FOBKAN) Kansas City
- ❑ DC (HHH) DC
- ❑ R9 (HWTHRN) San Francisco
- ❑ R1 (JFKBOS) Boston
- ❑ R2 (JKJNYC) New York
- ❑ CO (LBDCO) Central Office
- ❑ CO (NORTH) Central Office
- ❑ R3 (PHIPLB) Philadelphia
- ❑ CO (SOUTH) Central Office
- ❑ Other _____

Mail Stop	Desk Location

Form CMS-20037 (09/05) EF 09/2005

EXHIBIT 5
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 2 OF 3

3. WORKLOAD INFORMATION

Contract Number(s) *(for Medicare Advantage/Medicare Advantage with Prescription Drug/Prescription Drug Plan/Cost Contracts — Hxxxx, Sxxxx, etc.)*

Carrier Number(s) *(for Medicare Contractors/Intermediaries/Carriers — 12345)*

Contract and Task Number *(for Contractors — CMS-05-0001 : 0001)*

Grant Number *(for Researchers)*

Inter-Agency Agreement Number

4. REQUIRED ACCESSES *(See http://www.cms.hhs.gov/mdcn/bmcjcreport.asp for list of available jobcodes)*

❑ Connect	❑ Disconnect	❑ Keep	Default CMS Employee (standard desktop & network with CMS e-mail acct)	❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	Default Non-CMS Employee (standard network access)	❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
				❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____
❑ Connect	❑ Disconnect	❑ Keep	_____	❑ Connect	❑ Disconnect	❑ Keep	_____

5. JUSTIFICATION *(If name change, show Old Name =, New Name =)*

6. APPROVALS: *(See http://www.cms.hhs.gov/mdcn/reqsigchart.pdf for approval info)*

PROVIDE SIGNATURES BELOW OR APPROVE ONLINE EUA WORKFLOW REQUEST NUMBER REFERENCED ON PAGE 1.

Authorization: We acknowledge that our Organization is responsible for all resources to be used by the person identified above and that requested accesses are required to perform their duties. We have reviewed and verified the workload information supplied is accurate and appropriate. We understand that any change in employment status or access needs are to be reported immediately via submittal of this form or EUA WorkFlow request.

1st APPROVER *(CMS Project Officer, CMS Contact, CMS Supervisor, MCIC Contact, etc.)*

Printed Name		Telephone Number
CMS UserID	Signature	Date

2nd APPROVER *(Not required for CMS employees, BHRC or Commissioned Corps)*

Printed Name		Telephone Number
CMS UserID	Signature	Date

APPLICANT: Read, complete and sign next page.

EXHIBIT 5
APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS (FORM CMS-20037)
PAGE 3 OF 3

EUA WorkFlow Request No.

APPLICATION FOR ACCESS TO CMS COMPUTER SYSTEMS

Printed Name *(As you want it published)*

Social Security Number

CMS USERID

PRIVACY ACT STATEMENT

The information on page 1 of this form is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10) (The Privacy Act of 1974). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on this form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid Services (CMS) Data Center Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED.REG.41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

The Social Security Number (SSN) is used as an identifier in the Federal Service because of the large number of present and former Federal employees and applicants whose identity can only be distinguished by use of the SSN. Collection of the SSN is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary. However, if you do not provide this information, you will not be granted access to CMS computer systems.

SECURITY REQUIREMENTS FOR USERS OF CMS COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information, which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to your component's Information Systems Security Officer.

Applicant's Signature	Date

Form CMS-20037 (09/05) EF 09/2005 Page 3

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 1 OF 6

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

INSTRUCTIONS FOR COMPLETING THE DATA USE AGREEMENT (DUA) FORM CMS-R-0235

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

This agreement must be executed prior to the disclosure of data from CMS' Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, the Privacy Rule and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing protected health information and individual identifiers.

Directions for the completion of the agreement follow:

Before completing the DUA, please note the language contained in this agreement cannot be altered in any form.

- First paragraph, enter the Requestor's Organization Name.
- Section #1, enter the Requestor's Organization Name.
- Section #4 enter the Study and/or Project Name and CMS contract number if applicable for which the file(s) will be used.
- Section #5 should delineate the files and years the Requestor is requesting. Specific file names should be completed. If these are unknown, you may contact a CMS representative to obtain the correct names The System of Record (SOR) should be completed by the CMS contact or Project Officer. The SOR is the source system the data came from.
- Section #6, complete by entering the Study/Project's anticipated date of completion.
- Section #12 will be completed by the User.
- Section #16 is to be completed by Requestor.
- Section #17, enter the Custodian Name, Company/Organization, Address, Phone Number (including area code), and E-Mail Address (if applicable). The Custodian of files is defined as that person who will have actual possession of and responsibility for the data files. **This section should be completed even if the Custodian and Requestor are the same.** This section will be completed by Custodian.
- Section #18 will be completed by a CMS representative.
- Section #19 should be completed if your study is funded by one or more other Federal Agencies. The Federal Agency name (other than CMS) should be entered in the blank. The Federal Project Officer should complete and sign the remaining portions of this section. If this does not apply, leave blank.
- Sections #20a AND 20b will be completed by a CMS representative.
- Addendum, CMS-R-0235A, should be completed when additional custodians outside the requesting organization will be accessing CMS identifiable data.

Once the DUA is received and reviewed for privacy and policy issues, a completed and signed copy will be sent to the Requestor and CMS Project Officer, if applicable, for their files.

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 2 OF 6

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved
OMB No. 0938-0734

DATA USE AGREEMENT

DUA # _____

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

CMS agrees to provide the User with data that reside in a CMS Privacy Act System of Records as identified in this Agreement. In exchange, the User agrees to pay any applicable fees; the User agrees to use the data only for purposes that support the User's study, research or project referenced in this Agreement, which has been determined by CMS to provide assistance to CMS in monitoring, managing and improving the Medicare and Medicaid programs or the services provided to beneficiaries; and the User agrees to ensure the integrity, security, and confidentiality of the data by complying with the terms of this Agreement and applicable law, including the Privacy Act and the Health Insurance Portability and Accountability Act. In order to secure data that reside in a CMS Privacy Act System of Records; in order to ensure the integrity, security, and confidentiality of information maintained by the CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and _____ *(Requestor)* _____ enter into this agreement to comply with the following specific paragraphs.

1. This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (HHS), and _____ *(Requestor)* _____, hereinafter termed "User."

2. This Agreement addresses the conditions under which CMS will disclose and the User will obtain, use, reuse and disclose the CMS data file(s) specified in section 5 and/or any derivative file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the files specified in section 5 and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services or any of its components with respect to the data specified herein. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS point-of-contact or the CMS signatory to this Agreement shown in section 20.

3. The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

4. The User represents, and in furnishing the data file(s) specified in section 5 CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

Name of Study/Project

CMS Contract No. *(If applicable)*
Program 1583-S

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, that have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 5 will be put.

The User agrees not to disclose, use or reuse the data covered by this agreement except as specified in an Attachment to this Agreement or except as CMS shall authorize in writing or as otherwise required by law, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement. The User affirms that the requested data is the minimum necessary to achieve the purposes stated in this section. The User agrees that, within the User organization and the organizations of its agents, access to the data covered by this Agreement shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated in this section (i.e., individual's access to the data will be on a need-to-know basis).

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 3 OF 6

5. The following CMS data file(s) is/are covered under this Agreement.

File	Years(s)	System of Record

6. The parties mutually agree that the aforesaid file(s) (and/or any derivative file(s)) including those files that directly identify individuals and those that can be used in concert with other information to identify individuals may be retained by the User until, *Date* hereinafter known as the "Retention Date." The User agrees to notify CMS within 30 days of the completion of the purpose specified in section 4 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, the User agrees to destroy such data. The User agrees to destroy and send written certification of the destruction of the files to CMS within 30 days. The User agrees not to retain CMS files or any parts thereof, after the aforementioned file(s) are destroyed unless the appropriate Systems Manager or the person designated in section 20 of this Agreement grants written authorization. The User acknowledges that the date is not contingent upon action by CMS.

   The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon notice of termination by User, CMS will cease releasing data from the file(s) to the User under this Agreement and will notify the User to destroy such data file(s). Sections 3, 4, 6, 8, 9, 10, 11, 13, 14 and 15 shall survive termination of this Agreement.

7. The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (**http://www.whitehouse.gov/omb/circulars/a130/a130.html**) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" (**http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf**); and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (**http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf**). The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the file(s) specified in section 5 is prohibited. Further, the User agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in section 17 without written approval from CMS unless such movement, transmission or disclosure is required by a law.

8. The User agrees to grant access to the data to the authorized representatives of CMS or DHHS Office of the Inspector General at the site indicated in section 17 for the purpose of inspecting to confirm compliance with the terms of this agreement.

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 4 OF 6

9. The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in section 5, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death.

   The User agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 5 or any data derived from such files) must adhere to CMS' current cell size suppression policy. This policy stipulates that no cell (eg. admittances, discharges, patients) less than 11 may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell less than 11. By signing this Agreement you hereby agree to abide by these rules and, therefore, will not be required to submit any written documents for CMS review. If you are unsure if you meet the above criteria, you may submit your written products for CMS review. CMS agrees to make a determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries

10. The User agrees that, absent express written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement to do so, the User shall not attempt to link records included in the file(s) specified in section 5 to any other individually identifiable source of information. This includes attempts to link the data to other CMS data file(s). A protocol that includes the linkage of specific files that has been approved in accordance with section 4 constitutes express authorization from CMS to link files as described in the protocol.

11. The User understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from the appropriate System Manager or the person designated in section 20 of this Agreement.

12. The parties mutually agree that the following specified Attachments are part of this Agreement:

    _____

13. The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement or another written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement, CMS, at its sole discretion, may require the User to: (a) promptly investigate and report to CMS the User's determinations regarding any alleged or actual unauthorized use, reuse or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by CMS, submit a formal response to an allegation of unauthorized use, reuse or disclosure; (d) if requested by CMS, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and (e) if requested by CMS, return data files to CMS or destroy the data files it received from CMS under this agreement. The User understands that as a result of CMS's determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

    The User agrees to report any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2850 or by e-mail notification at **cms_it_service_desk@cms.hhs.gov** within one hour and to cooperate fully in the federal security incident process. While CMS retains all ownership rights to the data file(s), as outlined above, the User shall bear the cost and liability for any breaches of PII from the data file(s) while they are entrusted to the User. Furthermore, if CMS determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the User agrees to carry out these remedies without cost to CMS.

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 5 OF 6

14. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated sec. (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.
15. By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.
16. On behalf of the User the undersigned individual hereby attests that he or she is authorized to legally bind the User to the terms this Agreement and agrees to all the terms specified herein.

Name and Title of User *(typed or printed)*		
Company/Organization		
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature		Date

17. The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and will be the person responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

    The Custodian hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this Agreement on behalf of the User.

Name of Custodian *(typed or printed)*		
Company/Organization		
Street Address		
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
Signature		Date

EXHIBIT 6
DATA USE AGREEMENT (DUA) (FORM CMS-R-0235)
PAGE 6 OF 6

18. The disclosure provision(s) that allows the discretionary release of CMS data for the purpose(s) stated in section 4 follow(s). (To be completed by CMS staff.) _____

19. On behalf of _____ the undersigned individual hereby acknowledges that the aforesaid Federal agency sponsors or otherwise supports the User's request for and use of CMS data, agrees to support CMS in ensuring that the User maintains and uses CMS's data in accordance with the terms of this Agreement, and agrees further to make no statement to the User concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretation or compliance with the terms of this Agreement to the CMS official named in section 20 (or to his or her successor).

Typed or Printed Name	Title of Federal Representative
Signature	Date
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*

20. The parties mutually agree that the following named individual will be designated as point-of-contact for the Agreement on behalf of CMS.

    On behalf of CMS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name of CMS Representative *(typed or printed)*		
Title/Component		
Street Address		Mail Stop
City	State	ZIP Code
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*	
A. Signature of CMS Representative		Date
B. Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date
Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date
Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0734. The time required to complete this information collection is estimated to average 30 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: Reports Clearance Officer, Baltimore, Maryland 21244-1850.

EXHIBIT 7
CERTIFICATE OF DATA DESTRUCTION (FORM CMS-10252)
PAGE 1 OF 2

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved
OMB No. 0938-1046

INSTRUCTIONS FOR COMPLETING THE CERTIFICATE OF DATA DESTRUCTION FOR DATA ACQUIRED FROM THE CENTERS FOR MEDICARE & MEDICAID SERVICES

This certificate is to be completed and submitted to CMS to certify the destruction of all CMS data covered by the listed Data Use Agreement (DUA). This includes any copies made of the files, any derivative or subsets of the files, and any manipulated files. The requestor may not keep any copies, derivative or manipulated files—all files must be destroyed. CMS will close the listed DUA upon receipt and review of this certificate.

Directions for the completion of the certificate follow:

- Complete the Requestor and Custodian's Organization and Contact information as listed in the DUA.
- Provide the DUA number.
- Provide the Project/Study Name as listed on the DUA.
- Provide the CMS Project Officer, if applicable.
- Please list all data files and years covered by the DUA.
- A signature is required on this certification. The signature should be the requestor or Custodian listed on the DUA. If the DUA is for a CMS Contract/Demonstration, the CMS Project Officer must also sign the certificate.

Please submit this certificate to:
Director, Division of Privacy Compliance
Division of Privacy Compliance
Mailstop: N2-04-27
7500 Security Blvd.
Baltimore, MD 21244

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-1046. The time required to complete this information collection is estimated to average 10 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850.

EXHIBIT 7
CERTIFICATE OF DATA DESTRUCTION (FORM CMS-10252)
PAGE 2 OF 2

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CERTIFICATE OF DATA DESTRUCTION FOR DATA ACQUIRED FROM THE CENTERS FOR MEDICARE & MEDICAID SERVICES

REQUESTOR ORGANIZATION	DATA USE AGREEMENT (DUA) NO.
REQUESTOR CONTACT NAME	PHONE NO.
REQUESTOR ADDRESS	
CUSTODIAN ORGANIZATION	
CUSTODIAN CONTACT NAME	
CUSTODIAN ADDRESS	PHONE NO.
PROJECT/STUDY NAME	
CMS PROJECT OFFICER *(IF APPLICABLE)*	

CMS Data Files Destroyed:	Files	Years

By signing this Certification of Data Destruction, I confirm that the data acquired under DUA # _____ have been completely destroyed and no copies have been kept.

REQUESTOR OR CUSTODIAN PRINTED NAME	SIGNATURE	DATE
CMS PROJECT OFFICER *(IF APPLICABLE)* PRINTED NAME	SIGNATURE	DATE

Form CMS-10252 (12/07) 2

EXHIBIT 8
SECURE ONE HHS, INFORMATION SECURITY PROGRAM RULES OF BEHAVIOR
PAGE 1 OF 4

Secure One HHS

Information Security Program Rules of Behavior

The *HHS Rules of Behavior* (HHS Rules) provides common rules on the appropriate use of all HHS technology resources and information[1] for Department users, including federal employees, interns and contractors. The HHS rules work in conjunction with the *HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources*, dated February 17, 2006, and are issued under the authority of the HHS-OCIO-2007-0002, Policy for Department-wide Information Security, dated September 25, 2007. Both references may be found at URL: http://www.hhs.gov/ocio/policy/index.html.

All users of Department technology, resources, and, information must read these rules and sign the accompanying acknowledgement form before accessing Department data/information, systems and/or networks. This acknowledgement must be signed annually, preferably as part of Information Security Awareness Training, to reaffirm knowledge of and agreement to adhere to the HHS rules. The HHS rules may be presented to the user in writing or electronically, and the user's acknowledgement may be obtained by written or electronic signature. Each Operating Division (OPDIV) Chief Information Officer (CIO) shall determine how signatures are to be submitted, retained, and recorded[2]; and may append any necessary information or fields to the signature page. For electronic signatures, the specific version number of the HHS rules must be retained along with the date, and sufficient identifying information to uniquely link the signer to his or her corresponding information system accounts. Electronic copies of the signed Signature Page may be retained in lieu of the original. Each OPDIV CIO shall ensure that information system and information access is prohibited in the absence of a valid, signed HHS rules from each user.

Each HHS OPDIV may require user certification to policies and requirements, more restrictive than the rules prescribed herein, for the protection of OPDIV information and systems.

Furthermore, supplemental rules of behavior may be created for systems which require users to comply with rules beyond those contained in the HHS Rules. In such cases, users must additionally sign these supplemental rules of behavior prior to receiving access to these systems, and must comply with any ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners shall document system-specific rules of behavior and any recurring requirement to sign them in the System Security Plan for their systems. Each OPDIV CIO shall implement a process to obtain and retain the signed rules for such systems and shall ensure that user access to their information is prohibited without a signed, system-specific rules and a signed HHS Rules.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively, implement their own system-specific rules.

These HHS Rules apply to both the local and remote use of HHS information (in both electronic and physical forms) and information systems by any individual.

- Information and system use must comply with Department and OPDIV policies and standards, and with applicable laws.
- Use for other than official, assigned duties is subject to the HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources, dated February 17, 2006.
- Unauthorized access to information or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII)[3]

EXHIBIT 8
SECURE ONE HHS, INFORMATION SECURITY PROGRAM RULES OF BEHAVIOR
PAGE 2 OF 4

Users shall:

- In accordance with OPDIV procedures, immediately report all lost or stolen HHS equipment, known or suspected security incidents, known or suspected information security policy violations or compromises, or suspicious activity. Known or suspected security incidents is inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the OPDIV.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on Departmental systems.
- Wear identification badges at all times in federal facilities.
- Log-off or lock systems when leaving them unattended.
- Use provisions for access restrictions and unique identification to information and avoid sharing accounts.
- Complete security awareness training before accessing any HHS/OPDIV system and on an annual basis thereafter. Also, complete any specialized role-based security or privacy training, as required. See Memo from HHS CIO: Training of Individuals Developing and Managing Sensitive Systems, dated November 7, 2007.
- Permit only authorized HHS users to use HHS equipment and/or software.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with HHS records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (i.e., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published system of records notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary, to assure fairness in making determinations about an individual.

Users shall **not**:

- Direct or encourage others to violate HHS policies.
- Circumvent security safeguards or reconfigure systems except as authorized (i.e., violation of least privilege).
- Use another person's account, identity, or password.
- Remove computers or equipment.
- Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums.
- Exceed authorized access to sensitive information.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on portable devices such as laptops, personal digital assistants (PDA) and universal serial bus (USB) drives or on remote/home systems without authorization or appropriate safeguards, as stipulated by the HHS Encryption Standard for Mobile Devices and Portable Media, dated August 21, 2007.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others. (See 18 U.S.C. 2071)
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner.
- Modify software without management approval.

EXHIBIT 8
SECURE ONE HHS, INFORMATION SECURITY PROGRAM RULES OF BEHAVIOR
PAGE 3 OF 4

The following are prohibited on Government systems per the HHS-OCIO-2006-0001, Policy for Personal Use of Information Technology Resources, dated February 17, 2006:

- Sending or posting obscene or offensive material in messages or forums.
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages.
- Sending messages supporting political activity restricted under the Hatch Act.
- Conducting any commercial or "for-profit" activity.
- Utilizing peer-to-peer software without OPDIV CIO approval.
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material.
- Operating unapproved web sites.
- Incurring more than minimal additional expense, such as using non-trivial amounts of storage space or bandwidth for personal files or photos.
- Using the Internet or HHS workstation to play games, visit chat rooms, or gamble.

Users shall ensure the following protections are properly engaged, particularly on non-HHS equipment or equipment housed outside of HHS facilities:

- Use antivirus software with the latest updates.
- On personally-owned systems, use of anti-spyware and personal firewalls.
- For remote access and mobile devices, a time-out function that requires re-authentication after no more than 30 minutes of inactivity.
- Adequate control of physical access to areas containing sensitive information.
- Use of approved encryption to protect sensitive information stored on portable devices or recordable media, including laptops, thumb drives, and external disks; stored on remote or home systems; or transmitted or downloaded via e-mail or remote connections.
- Use of two-factor authentication for remote access to sensitive information.

Users shall ensure that passwords:

- Contain a minimum of eight alphanumeric characters and (when supported by the OPDIV environment) at least one uppercase and one lowercase letter, and one number, and one special character.
- Avoid words found in a dictionary, names, and personal data (e.g., birth dates, addresses, social security numbers, and phone numbers).
- Are changed at least every 90 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords).
- Are not reused until at least six other passwords have been used.
- Are committed to memory, or stored in a secure place.

EXHIBIT 8
SECURE ONE HHS, INFORMATION SECURITY PROGRAM RULES OF BEHAVIOR
PAGE 4 OF 4

-4-

SIGNATURE PAGE

I have read the *HHS Rules of Behavior* (HHS Rules), version 2008-0001.003S, dated February 12, 2008 and understand and agree to comply with its provisions. I understand that violations of the HHS Rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities. I understand that exceptions to the HHS Rules must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Signatures: _____

Date Signed: _____

Employee's/User's Name: _____
(Print)

APPROVED BY AND EFFECTIVE ON:

/s/ February 12, 2008

Michael Carleton
HHS Chief Information Officer

DATE

The record copy is maintained in accordance with GRS 1, 18.a.