Program:	55-S			
Title:	Medicare and You Mailing List Services			
Agency:	Department of Health and Human Services (HHS)			
Term:	Beginning May 1, 2025 and ending April 30, 2026		Peachtree Data, Inc.	
		BASIS OF	Duluth, GA	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	COST
I.	**MAIL FILE PROCESSING:**			
	The prices submitted for line items 1.(a) through			
	(d) are for both the test orders (if required) and			
	the live orders.			
(a)	Processing Records:			
1.	Monthly Order----------per 1,000 records	4,216	$1.25	$5,270.00
2.	One-time Order----------per 1,000 records	54,000	$0.75	$40,500.00
(b)	Deceased Coding results			
	--------per 1,000 records identified	70	$0.00	$0.00
(c)	Apartment Append Coding Results			
	--------per 1,000 records identified	448	$0.00	$0.00
(d)	Deduplication Results			
	---------per 1,000 records removed	7,500	$0.00	$0.00
	CONTRACTOR SUBTOTALS			$45,770.00
	DISCOUNT		0.0%	$0.00
	DISCOUNTED TOTALS			$45,770.00

AWARDED

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Medicare and You Mailing List Services

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

Department of Health and Human Services (HHS)/
Centers for Medicare and Medicaid Services (CMS)

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning May 1, 2025 and ending April 30, 2026 plus up to four (4) optional 12-month extension period(s) that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

BID OPENING: Bids shall be opened virtually at 11:00 a.m., Eastern Time (ET), on March 28, 2025 at the U.S. Government Publishing Office. All parties interested in attending the bid opening shall email bids@gpo.gov one (1) hour prior to the bid opening date and time to request a Microsoft Teams live stream link. This must be a separate email from the bid submission. The link will be emailed prior to the bid opening.

BID SUBMISSION: Bidders must email bids to bids@gpo.gov for this solicitation. No other method of bid submission will be accepted at this time. The program number and bid opening date must be specified in the subject line of the emailed bid submission. ***Bids received after the bid opening date and time specified above will not be considered for award.***

BIDDERS, PLEASE NOTE: These specifications have been extensively revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding.

Abstracts of contract prices are available at: https://www.gpo.gov/how-to-work-with-us/vendors/contract-pricing.

For information of a technical nature, contact Stacy Bindernagel at sbindernagel@gpo.gov or (202) 512-2103.

SECTION 1. – GENERAL TERMS 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 Publication 310.2, effective December 1, 1987 (Rev 01-18)).

GPO Contract Terms (GPO Publication 310.2) –
https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/contractterms2018.pdf

SUBCONTRACTING: No subcontracting is allowed.

OPTION TO EXTEND THE TERM OF THE CONTRACT: 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 five (5) years as a result of, and 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: 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 pricing under this contract shall be adjusted in accordance with this clause, provided that in no event will any pricing adjustment be made that would exceed the maximum permissible under any law in effect at the time of the adjustment.

There will be no adjustment for orders placed during the first period specified below. Pricing will thereafter be eligible for adjustment during the second and any succeeding performance period(s). For each performance period after the first, a percentage figure will be calculated as described below and that figure will be the Economic Price Adjustment for that entire next period. Pricing adjustments under this clause are not applicable to reimbursable postage or transportation costs, or to paper, if paper prices are subject to adjustment by separate clause elsewhere in this contract.

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from May 1, 2025 to April 30, 2026, and the second and any succeeding period(s) will extend for 12 months from the end of the last preceding period, except that the length of the final period may vary. The first day of the second and any succeeding period(s) will be the effective date of the Economic Price Adjustment for that period.

Pricing adjustments in accordance with this clause will be based on changes in the seasonally adjusted "Consumer Price Index For All Urban Consumers - Commodities Less Food" (Index) published monthly in the CPI Detailed Report by the U.S. Department of Labor, Bureau of Labor Statistics.

The economic price adjustment will be the percentage difference between Index averages as specified in this paragraph. An index called the variable index will be calculated by averaging the monthly Indexes from the 12-month interval ending three (3) months prior to the beginning of the period being considered for adjustment. This average is then compared to the average of the monthly Indexes for the 12-month interval ending January 31, 2025**,** called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

The Government will notify the contractor by contract modification specifying the percentage increase or decrease to be applied to invoices for orders placed during the period indicated. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs and separately adjusted paper prices. Payment discounts shall be applied after the invoice price is adjusted.

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

DATA SECURITY: 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) (instructions to be provided via email).

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.

Personally Identifiable Information for the Medicare and You Handbook includes a person's name and address.

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.

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, duplicates created by the contractor or their representatives, and/or 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.

Data Custodians: If any PII is to be forwarded to additional contractor-owned locations, all security requirements also apply to those locations (all parties involved). The contractor is responsible for the actions of all locations. The contractor's project manager shall appoint up to two (2) Data Custodians at each location and shall have them complete an Addendum to Data Use Agreement (instructions to be provided via email). The contractor's project manager must collect and submit completed forms to CMS before any PII may be sent to that location.

Personnel Security: The contractor shall have a system in place to perform criminal background investigations and Social Security Number verification on all employees. In addition, CMS will perform background investigations on two (2) contractor employees who will access the electronic mailbox. (See Security Exhibits 2, 3, and 4 for more information.)

Physical Security: The contractor shall have a secure work area(s) for processing and production of all CMS PII in electronic 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 (see Security Exhibit 1).

Security Liaison(s): The contractor must appoint one (1) 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 contact to the Government for security issues. The liaison's duties will include attending the Postaward Conference; submitting a security plan (see "PROJECT PLANS, *Security Plan*" specified herein); 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 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.

Incident Reporting Requirements: If there is a breach, or a suspected breach, of PII, the incident must be reported to CMS within one (1) hour of discovery. Contractor to report breaches to the CMS IT Service Desk at (410) 786-2580 or (800) 562-1963.

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. Failure to certify file destruction may cause the CMS Privacy Office to refuse to issue future DUAs and data with the contractor's company or to individuals listed on this DUA. (Instructions for the destruction of CMS data files will be provided after award.) The contractor representative named in Section 16 of the DUA may sign one certificate for all locations.

Security Exhibits: The following Exhibits 1 through 4 contain security clauses, information, and forms.

- Security Exhibit 1: CMS Clause-11: CMS Information Security (April 2008)
- Security Exhibit 2: CMS Clause-09A-01 Security Clause – New Contract Awards (May 2007) (NOTE: This contract is designated as Low Risk.)
- Security Exhibit 3: FAQ Supplement to CMS Security Clause 09A-01 (April 2008)
- Security Exhibit 4: Secure One HHS, Information Security Program Rules of Behavior (2/12/08)

After award, all contractor management and employees involved in this contract will be instructed on how to apply for access to the electronic mailbox. Instructions for filling out the security documentation and the Data Use Agreement will also be provided after award. Submissions will be done electronically.

PREAWARD SURVEY: In order to determine the responsibility of the contractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's facility(ies) or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract.

As part of the financial determination, the contractor in line for award shall be required to provide the following financial documents:

1) Most recent profit and loss statement
2) Most recent balance sheet
3) Statement of cash flows
4) Current official bank statement
5) Current lines of credit (with amounts available)

The documents will be reviewed to validate that adequate financial resources are available to perform the contract requirements. Documents submitted will be kept confidential and used only for the determination of responsibility by the Government. Failure to provide the requested information in the time specified by the Government may result in the Contracting Officer not having adequate information to reach an affirmative determination of responsibility.

As part of the preaward survey, the Government will conduct a review of all data handling involved along with their contractor's Security Plan as required by this contract (see "PROJECT PLANS" below).

PROJECT PLANS: As part of the preaward survey, the prospective contractor must present, in writing, to the Contracting Officer within five (5) workdays of being notified to do so by the Contracting Officer or his/her representative detailed Project Plans for each of the below activities.

These proposed plans are subject to review and approval by the Government, and award will not be made prior to approval of same.

The Government reserves the right to waive some or all of these plans.

Once approved, no changes to these plans may be made without written approval from the Contracting Officer.

Option Years: For each option year that may be exercised, the contractor will be required to review their plans and re-submit in writing the below plans detailing any changes and/or revisions that may have occurred. The revised plans are subject to Government approval and must be submitted to the Contracting Officer or his/her representative within five (5) workdays of notification of the option year being exercised.

If there are no changes/revisions, the contractor will be required to submit to the Contracting Officer or his/her representative a statement confirming that the current plans are still in effect.

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 and as specified in this contract.

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: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

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.

POSTAWARD CONFERENCE: Unless waived by the Contracting Officer, the total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the GPO, Washington, DC immediately after award. At the Government's option, the postaward conference may be held via teleconference. Person(s) that the contractor deems necessary for the successful implementation of the contract must be in attendance.

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. Orders may be issued under the contract from May 1, 2025 through April 30, 2026, plus for such additional period(s) as the contract is extended. 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" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically 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, if any.

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.

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 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties as stated in 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES. It is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a, specifically, 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES and m(1) GOVERNMENT CONTRACTORS.

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 (i) the system or systems of 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 an 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.

ADDITIONAL EMAILED BID SUBMISSION PROVISIONS: The Government will not be responsible for any failure attributable to the transmission or receipt of the emailed bid including, but not limited to, the following:

1. Illegibility of bid.
2. Emails over 75 MB may not be received by GPO due to size limitations for receiving emails.
3. The bidder's email provider may have different size limitations for sending email; however, bidders are advised not to exceed GPO's stated limit.
4. When the email bid is received by GPO, it will remain unopened until the specified bid opening time. Government personnel will not validate receipt of the emailed bid prior to bid opening. GPO will use the prevailing time (specified as the local time zone) and the exact time that the email is received by GPO's email server as the official time stamp for bid receipt at the specified location.

PAYMENT: Submitting invoices for payment via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of receiving payment. Instruction for using this method can be found at the following web address:
http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.

A copy of the email from the ordering agency confirming receipt of acceptable deliverables (mail files) and identified by purchase order, program, jacket, and print order numbers must be furnished with the contractor's billing invoice as evidence of delivery.

For more information about the billing process, refer to the General Information of the Office of Finance web page located at: https://www.gpo.gov/how-to-work-with-us/agency/billing-and-payment.

Contractor's billing invoice must be itemized in accordance with the items in the "SCHEDULE OF PRICES."

SECTION 2. – SPECIFICATIONS

SCOPE: These specifications cover the sanitization of mailing list files of recipients receiving Medicare and You Handbooks (in order to enhance the accuracy of addresses and reduce the number of multiple handbooks that are delivered to a household with multiple beneficiaries) requiring such operations as receiving address files, processing files against specified software, sanitizing (sorting/removing/changing addresses), and furnishing deliverables of final data.

TITLE: Medicare and You Mailing List Services.

FREQUENCY OF ORDERS:

Test Orders: 1 or 2 orders.

NOTE: If issued, the test orders will be done at the beginning of the base contract year. The Government does not anticipate issuing test orders in the option years. See "TEST ORDERS" below for more information.

Live Orders: Approximately 13 orders per year.

QUANTITY:

Test Orders: Up to approximately 15,000 to 16,000 records per test order.

Live Orders: Approximately 350,000 records per monthly order and a one-time order of approximately 54,000,000 records.

NOTE: The quantities specified above are for the base contract year. The total number of records may increase by approximately 50,000 per monthly order and by approximately 1 million per the one-time order per option year, if exercised.

GOVERNMENT TO FURNISH: Mailing addresses via an electronic mailbox.

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "GOVERNMENT TO FURNISH," necessary to produce the products in accordance with these specifications.

TEST ORDERS: The Government reserves the right to waive the test orders. The contractor will be notified at the postaward conference, or shortly thereafter, if the test orders will be waived.

If required – For the test orders, there will be two (2) phases (Phase One and Phase Two). For these phases, CMS will provide the contractor with three (3) test mailing address files containing approximately 29 mailing addresses, 783 mailing addresses, and 14,634 mailing addresses. The mailing test files will be sent to contractor via an electronic mailbox. These files contain names and addresses (record sheet layout attached). Test files will be used to verify contractor is counting the number of mail files correctly during the duplicate removal process.

Phase One: Initial Test Files –

Step 1: The contractor will run these three (3) files through the Coding Accuracy Support System (CASS), National Change of Address (NCOA), Deceased Coding, and Apartment Append Coding. (NOTE: The NCOA must include 48-month licensing, CASS, Delivery Point Validation (DPV), LACS Link, and Suite Link.)

Step 2: The contractor will remove all undeliverable and deceased addresses per CASS/NCOA/Deceased Coding from each mailing address file. Undeliverable addresses should be counted for each file and added to the Report Summary spreadsheet (format in Table 2 below). The contractor will then create an Excel file of these cleaned addresses called "file abc cleaned" in the format as outlined in Table 1:

Table 1: Name/Address Excel files are formatted with separate columns for:

rep payee (if applicable)
last name
first name
middle initial
address line 1
address line 2
city
state
zip code

Step 3: The contractor will deliver to CMS one (1) Excel spreadsheet for each mail file. These files will be delivered by email. The files must be password protected with the password provided in a separate email. The spreadsheets will contain all the addresses from the mail file with just the CASS/NCOA updates and the undeliverable addresses removed (detailed in step 2).

Phase Two: Revised Test Files (after Phase One) –

Step 1: Once Phase 1 is completed, the contractor will then remove duplicate addresses and count the addresses on each file in the following manner:

a. Any address that appears only one (1) time is counted as one (1) address.

b. Any address that appears two (2) to four (4) times will have all but one of that address removed and that address is then counted as one (1) address. All duplicates will be removed at the address level. Any address appearing more than one (1) time in this category will be deleted regardless of the household name.

c. Any address that appears five (5) times or more will all be counted as unique addresses, and none of these addresses will be removed.

Example One - "123 Maple Street, Woodlawn, MD 21224" appears three (3) times. Therefore, two (2) of these addresses will be removed. This address will be counted as one (1) address.

Example Two - "123 Maple Street, Woodlawn, MD 21224" appears three (3) times. The addresses appear under the names Bob Smith, Martha Smith, and John Jones. Therefore, two (2) of these addresses will be removed. This address will be counted as one (1) address.

Example Three - "456 Oak Street, Washington, DC 28045" appears six (6) times. None of these addresses will be removed. This address will be counted as six (6) addresses.

Step 2: The contractor will deliver to CMS an Excel spreadsheet for each mail file. These files will be delivered by email. The files must be password protected with the password provided in a separate email. The spreadsheets will contain all the addresses with the clean-up of duplicates removed (detailed in Step 1).

CMS will evaluate contractor results and discuss any concerns with the contractor.

For each address file, there is to be a report summary of the total number of addresses (after Step 1 has been completed). The report summary must match up with the total number of addresses in the contractor's net file after clean-up of duplicates.

Table 2: Report Summary example:

Mail File Names	No. of addresses that appear only once	No. of addresses that appear 2 to 4 times	No. of addresses that appear 5 or more times	No. of undeliverable addresses per CASS/NCOA	No. of undeliverable addresses per Deceased Coding	No. of changed addresses per Apartment Append Coding
Mail file abc	25,000	48,000	6,000			
Mail file xyz	20,000	40,000	3,000			
Totals						

LIVE ORDERS:

Phase Three - Live Files – For the live orders, there will be three (3) phases (Phase Three, Phase Four, and Phase Five).

Step 1: CMS will provide approximately 60 live electronic files containing approximately 350,000 mailing addresses per monthly order and approximately 54,000,000 mailing addresses for the one-time order (in/around the month of June) in the base contract year.

NOTE: In the option years, if exercised, the quantity may increase by approximately 50,000 addresses (monthly order) and by approximately 1,000,000 addresses (one-time order) per option year, as exercised.

These addresses will be sent via an electronic mailbox. The files contain names and addresses (record sheet layout attached). Contractor will run these files through CASS, NCOA, Deceased Coding, Apartment Append Coding, and Deduplication software. (NOTE: The NCOA must include 48-month licensing, CASS, DPV, LACS Link, and Suite Link.)

Step 2: The contractor will remove all undeliverable and deceased addresses per CASS/NCOA/Deceased Coding from each mailing address file.

Undeliverable addresses will be counted for each file and added to the Report Summary spreadsheet required in Step 4 below.

Step 3: The contractor will then remove duplicate addresses and count the addresses on each file in the following manner:

a. Any address that appears only one (1) time is counted as one (1) address.

b. Any address that appears two (2) to four (4) times will have all but one of that address removed and that address is then counted as one address. All duplicates will be removed at the address level. Any address appearing more than one (1) time in this category will be deleted regardless of the household name.

c. Any address that appears five (5) times or more will all be counted as unique addresses, and none of these addresses will be removed.

Example One - "123 Maple Street, Woodlawn, MD 21224" appears three (3) times. Therefore, two (2) of these addresses will be removed. This address will be counted as one (1) address.

Example Two - "123 Maple Street, Woodlawn, MD 21224" appears three (3) times. The addresses appear under the names Bob Smith, Martha Smith, and John Jones. Therefore, two (2) of these addresses will be removed. This address will be counted as one (1) address.

Example Three - "456 Oak Street, Washington, DC 28045" appears six (6) times. None of these addresses will be removed. This address will be counted as six (6) addresses.

Step 4: CMS will provide the contractor an Excel spreadsheet of names and addresses that appear five (5) or more times in a single mail file where that location would like to reduce the number of addresses in the file to a designated quantity listed in the spreadsheet.

Example: "123 Main Street, Baltimore, MD 2144" appears 75 times. CMS may require the contractor to delete 70 addresses at random with five (5) addresses remaining in the file.

Step 5: Contractor will provide CMS with an Excel spreadsheet Report Summary (formatted like Table 2 above) for all the live files.

Contractor must retain the final files for one (1) year after completion of each order.

Contractor will also provide CMS with an Excel spreadsheet containing all live file names and the final number of addresses per file. This summary will be the total number of mailing addresses per file to which a copy of the Medicare and You Handbook will be sent. (See Table 3 for format.)

Table 3:

Final Address Tally:

Mail File Name	No. of Addresses
Mail file abc	1,482,000
Mail file xyz	290,000
Totals	

Step 6: CMS will evaluate contractor results and discuss any concerns with the contractor. Once CMS has given approval, contractor will then provide to CMS approximately 60 cleaned-up files with duplicates removed. The contractor will save these files back into the electronic mailbox. (CMS will provide additional instructions to follow regarding exact location of where to save them, what to title each file, etc.)

NOTE: The contractor may sort the addresses so that all names, street addresses, city, state, zip, for example, appear in the same columns but no data is to be removed in the process.

Phase Four – Identification and removal of addresses appearing more than 30 times –

The contractor must identify any address that appears more than 30 times in a mail file, and CMS must have the option of removing some of those addresses from a mail file. For example, if an address appears 35 times on a mail file, CMS may instruct the contractor to delete all but five (5) of those addresses. For addresses appearing more than 30 times in a mail file, the contractor is to provide an Excel spreadsheet listing each address and how many times it appeared.

Phase Five: Reason for files dropped –

Contractor may be asked to provide a list of all dropped addresses and the reason the addresses were dropped. Contractor to provide via email a password protected excel spreadsheet, with the password provided in a separate email.

DISTRIBUTION: Deliver f.o.b. destination the completed mail lists to CMS' secure electronic mailbox (i.e., contractor must upload the completed mail lists to the electronic mailbox).

Upon completion of each order, contractor must notify the ordering agency (on the same day each order's files are sent to the electronic mailbox) via email to the address indicated on the print order. The subject line of the email shall be "Distribution Notice for Program 55-S, Print Order XXXXX, Jacket Number XXX-XXX."

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).

Print orders will be furnished via email.

The following schedules begin the workday after notification of the availability of print order and furnished files; the workday after notification will be the first workday of the schedule.

Test Orders (If Ordered) –

- Delivery of Phase One deliverable (Excel spreadsheet) must be made within two (2) workdays of receipt of notification of the availability of print order and furnished files.

- Delivery of Phase Two deliverable (Excel spreadsheet) must be made within two (2) workdays of receipt of ordering agency approval to proceed after completion of Phase One.

Live Orders –

- Delivery of Phase Three, Step 3 and Phase Four (if applicable) deliverables (Excel spreadsheets) must be made within seven (7) workdays of receipt of notification of the availability of print order and furnished files.

- Delivery of Phase Three, Step 5 completed, sanitized mail file list (with ordering agency's requested corrections) and deliverable (Excel spreadsheet) must be made within three (3) workdays of receipt of notification of requested corrections.

- If required, delivery of Phase Five deliverables must be made within three (3) workdays of receipt of notification of requested information.

For the purpose of this contract, the ship/deliver date indicated on the print order is the date products ordered for delivery f.o.b. destination must be delivered to the destination specified as applicable to this contract (see "DISTRIBUTION").

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.

For compliance reporting purposes, the contractor must notify the U.S. Government Publishing Office of the date of shipment or delivery, as applicable. Upon completion of each order, contractor must contact the Shared Support Services Compliance Section via email at compliance@gpo.gov; or via telephone at (202) 512-0520. Personnel receiving the email or call will be unable to respond to questions of a technical nature or to transfer any inquiries.

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 one (1) year's production 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.	(a)	1.	4,216
		2.	54,000
	(b)		70
	(c)		448
	(d)		7,500

SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. destination, as applicable to this contract (see "DISTRIBUTION").

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 non-responsive.

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), NA (Not Applicable), or blank spaces for an item may be declared non-responsive.

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 invoices 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.

Contractor's billing invoice must be itemized in accordance with the line items in the "SCHEDULE OF PRICES."

I. MAIL FILE PROCESSING: Prices offered must be all-inclusive and include the cost of all materials and operations necessary for the complete processing of the furnished records, production of the required deliverables, and distribution of the deliverables listed in accordance with these specifications.

Prices submitted for line items I.(a)1. and 2. must include the cost to process the furnished records through CASS, NCOA, Deceased Coding, Apartment Append Coding, and Deduplication software, as specified in these specifications.

Prices submitted for line items I.(b), (c), and (d) are for the results only of the initial processing. NOTE: Prices must include any corrections/adjustments to the files requested from the ordering agency after the initial review. Additionally, prices must include the cost for any Phase Five requests.

The prices submitted for line items I.(a) through (d) are for both the test orders (if required) and the live orders.

(a) Processing Records:

1. Monthly Order ..... per 1,000 records .....$_____

2. One-time Order ..... per 1,000 records .....$_____

(b) Deceased Coding Results ..... per 1,000 records identified .....$_____

(c) Apartment Append Coding Results ..... per 1,000 records identified .....$_____

(d) Deduplication Results ..... per 1,000 records removed .....$_____

_____
(Initials)

SHIPMENTS: Shipments will be made from: City _____ State _____.

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment is not made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent _____ Calendar Days. See Article 12 "Discounts" of Solicitations Provisions in GPO Contract Terms (Publication 310.2).

AMENDMENT(S): Bidder hereby acknowledges amendment(s) number(ed) _____.

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within _____ calendar days (60 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated point(s), in exact accordance with specifications. *Failure to provide a 60-day bid acceptance period may result in expiration of the bid prior to award.*

BIDDER'S NAME AND SIGNATURE: Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certifications and representations as required by the solicitation and GPO Contract Terms – Publication 310.2. When responding by email, fill out and return one copy of all pages in "SECTION 4. – SCHEDULE OF PRICES," including initialing/signing where indicated. Valid electronic signatures will be accepted in accordance with the Uniform Electronic Transactions Act, §2. Electronic signatures must be verifiable of the person authorized by the company to sign bids. *Failure to sign the signature block below may result in the bid being declared non-responsive.*

Bidder _____
(Contractor's Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

By _____
(Printed Name, Signature, and Title of Person Authorized to Sign this Bid) (Date)

_____
(Person to be Contacted) (Telephone Number)

_____
(Email Address) (Fax Number)

THIS SECTION FOR GPO USE ONLY

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____
(Initials) (Initials)

EXHIBIT 1
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
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.

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;

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:

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:

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:

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.

GPO Exhibit 3
FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008

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.

GPO Exhibit 3
FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008

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

GPO Exhibit 3
FAQ Supplement to CMS Security Clause 09A-01
Date: April 4, 2008

fee at each of the regional PSC offices. PSC offices are located in downtown Federal buildings in 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.

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.

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.

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.

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.