Program 5515-S Contract Term: September 1, 2020 through August 31, 2021 plus four option

Title: RRB Rate Letters, Tax Statements, BA-6 Forms

ITEM	DESCRIPTION	BASIS OF AWARD	MPM Communications, LLC, Waldorf, MD		SourceLink, Miamisburg, OH		Specialty Print Communications, Niles, IL		Vision Direct, Indianapolis, IN		GPO Estimate Chicago, IL	
			UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST
I.	DESIGN, LAYOUT, AND COMPOSITION											
(a)	Envelope, per envelope version…..per side (inside or outside)	8	50.00	$400.00	$50.00	$400.00	$22.00	$176.00	15.00	$120.00	$50.00	$400.00
(b)	Forms (each version).....per side	30	$100.00	$3,000.00	$50.00	$1,500.00	$106.00	$3,180.00	$25.00	$750.00	$100.00	$3,000.00
II.	PROOFS:											
(a)	Digital Content Proof-Envelopes…per side, per version	5	$25.00	$125.00	$50.00	$250.00	$18.00	$90.00	$15.00	$75.00	$25.00	$125.00
(b)	Digital Content Proof-Forms…per side, per version	24	$25.00	$600.00	$50.00	$1,200.00	$25.00	$600.00	$15.00	$360.00	$25.00	$600.00
(c)	PDF Proofs…per side, per version	35	$25.00	$875.00	$50.00	$1,750.00	$15.00	$525.00	$15.00	$525.00	$25.00	$875.00
III.	AUTHOR'S ALTERATIONS:											
(a)	Author's alterations envelopes…per side	1	$25.00	$25.00	$25.00	$25.00	$0.00	$0.00	$10.00	$10.00	$25.00	$25.00
(b)	Author's alterations, forms…per side	33	$50.00	$1,650.00	$25.00	$825.00	$0.00	$0.00	$10.00	$330.00	$50.00	$1,650.00
IV.	PREPRODUCTION QUALITY CONTROL SAMPLES:											
(a)	Preproduction Quality Control Samples…per 100 sets	10	$250.00	$2,500.00	$100.00	$1,000.00	$340.00	$3,400.00	$50.00	$500.00	$250.00	$2,500.00
V.	PRINTING:											
(a)	Window Envelope….per version											
	(1) MAKEREADY AND/OR SETUP	6	$75.00	$450.00	$25.00	$150.00	$150.00	$900.00	$0.00	$0.00	$100.00	$600.00
	(2) RUNNING PER 1,000 COPIES	1,341	$21.00	$28,161.00	$24.28	$32,559.48	$24.00	$32,184.00	$25.16	$33,739.56	$18.00	$24,138.00
(b)	Rate Letters…per version											
	(1) MAKEREADY AND/OR SETUP	20	$75.00	$1,500.00	$25.00	$500.00	$150.00	$3,000.00	$50.00	$1,000.00	$100.00	$2,000.00
	(2) RUNNING PER 1,000 COPIES	535	$10.00	$5,350.00	$8.40	$4,494.00	$16.63	$8,897.05	$10.00	$5,350.00	$10.00	$5,350.00
(c)	Rate Letter Newsletters….per version											
	(1) MAKEREADY AND/OR SETUP	2	$75.00	$150.00	$25.00	$50.00	$150.00	$300.00	$75.00	$150.00	$100.00	$200.00
	(2) RUNNING PER 1,000 COPIES	525	$12.00	$6,300.00	$14.40	$7,560.00	$12.83	$6,735.75	$12.00	$6,300.00	$12.00	$6,300.00
(d)	Tax Statement Forms…per leaf - Citizen											
	(1) MAKEREADY AND/OR SETUP	1	$75.00	$75.00	$25.00	$25.00	$150.00	$150.00	$75.00	$75.00	$100.00	$100.00
	(2) RUNNING PER 1,000 COPIES	547	$22.50	$12,307.50	$20.96	$11,465.12	$17.71	$9,687.37	$22.50	$12,307.50	$22.50	$12,307.50
(e)	Tax Statement Forms…per leaf -NRA											
	(1) MAKEREADY AND/OR SETUP	1	$75.00	$75.00	$25.00	$25.00	$150.00	$150.00	$75.00	$75.00	$81.25	$81.25
	(2) RUNNING PER 1,000 COPIES	1	$22.50	$22.50	$480.00	$480.00	$284.00	$284.00	$22.50	$22.50	$202.25	$202.25
(f)	BA-6 Forms											
	(1) MAKEREADY AND/OR SETUP	2	$75.00	$150.00	$25.00	$50.00	$150.00	$300.00	$75.00	$150.00	$100.00	$200.00
	(2) RUNNING PER 1,000 COPIES	258	$27.00	$6,966.00	$20.96	$5,407.68	$18.04	$4,654.32	$24.50	$6,321.00	$27.00	$6,966.00
VI.	LASER IMAGING PERSONALIZATION, NCOA PROCESSING, INSERTING AND MAILING											
(a)	Imaging/Inserting/Mailing…											
	(1) MAKEREADY AND/OR SETUP	24	$150.00	$3,600.00	$50.00	$1,200.00	$200.00	$4,800.00	$100.00	$2,400.00	$150.00	$3,600.00
	(2) RUNNING PER 1,000 COPIES	1,340	$19.00	$25,460.00	$32.00	$42,880.00	$30.00	$40,200.00	$24.00	$32,160.00	$19.00	$25,460.00
(b)	CASS/NCOA Processing for BA-6 Forms only…per 1,000 addresses											
	(1) MAKEREADY AND/OR SETUP											
	(2) RUNNING PER 1,000 COPIES	650	$0.75	$487.50	$2.50	$1,625.00	$3.50	$2,275.00	$1.00	$650.00	$1.50	$975.00
(c)	Tax Statement (NRA Form)-Non-authomated: Gather and match 2-3 leaves….per 1,000 leaves											
	(1) MAKEREADY AND/OR SETUP											
	(2) RUNNING PER 1,000 COPIES	1	$150.00	$150.00	$500.00	$500.00	$740.00	$740.00	$200.00	$200.00	$19.00	$19.00
(d)	Hand Insert into envelopes….per 1,000 sets											
	(1) MAKEREADY AND/OR SETUP											
	(2) RUNNING PER 1,000 COPIES	1	$50.00	$50.00	$500.00	$500.00	$8.50	$8.50	$150.00	$150.00	$177.12	$177.12
	TOTAL OFFER:			$100,429.50		$116,421.28		$123,236.99		$103,720.56		$97,851.12
	DISCOUNT:		5.00%	$5,021.48	0.00%	$0.00	4.00%	$4,929.48	0.00%	$0.00		$0.00
	NET OFFER:			$95,408.02		$116,421.28		$118,307.51		$103,720.56		$97,851.12
			Awarded									

Prepared by: KD
Reviewed by: CS

U.S. GOVERNMENT PRINTING OFFICE
200 N. LaSalle St, Suite 810
Chicago, IL 60601

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

RRB Rate Letters, Tax Statements, BA-6 Forms

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

U.S. Railroad Board (RRB), Chicago, IL

Single Award

BID OPENING: Bids shall be opened at **2:00 P.M.** prevailing Chicago, IL time on

August 3, 2020.

at the U.S. Government Publishing Office, Chicago.
Due to the COVID-19 pandemic, this will NOT be a public bid opening.

BID SUBMISSION: Due to the COVID-19 pandemic, the physical office will NOT be open. Based on this, bidders MUST submit email bids to **bidschicago@gpo.gov** for this solicitation. See also "ADDITIONAL EMAILED BID SUBMISSION PROVISIONS" on page TBD.

No other method of bid submission will be accepted at this time.

The program number "5515-S" and bid opening date **"August 3, 2020"** must be specified in the subject line of the emailed bid submission. Bids received after **"2:00 p.m. Central**" on the bid opening date specified above will not be considered for award.

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 10 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.

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.

NOTE: Bidder must use the exact bid pages in "SECTION 4. – SCHEDULE OF PRICES," (pages 43-46) and MUST NOT substitute their own bid formatting in their submitted bid. Substitution may result in a determination of the bid as non-responsive.

CONTRACT TERM: The term of this contract is for the period **beginning September 1, 2020 and ending August 31, 2021, plus up to 4 optional 12-month extension period(s)** that may be added in accordance with the "Option to Extend the Contract Term" clause in this contract.

NOTE: Minor changes are scattered throughout. Bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding.

The GPO 910 "BID" Form is no longer required. Bidders are to fill out, sign/initial, as applicable, all pages of SECTION 4. – SCHEDULE OF PRICES.

INFORMATION: For questions about these specifications contact Chuck Szopo at 312-353-3916 x6 or cszopo@gpo.gov. Questions about these specifications should be forwarded at least 1 workday before the Bid Deadline, in order to be addressed prior to bid submission.

Email requests for new award information (available approximately 2 weeks after bid opening) to GPO Chicago Front Desk at kdodson@gpo.gov.

Doing Business with GPO Customer Services During the Coronavirus Pandemic:

Contractors should continue performance on contracts. Contractors must continue to fully comply with the terms and conditions of these contracts. Deliveries, proof approvals, and press sheet inspections for agencies may be impacted. It is requested that contractors contact a Government employee at the delivery location to confirm their availability to receive prior to shipping.

Schedules and other adjustments will be made in accordance with GPO Contract Terms. Caution should be used to safeguard all products should any delivery delays be imposed by the Government.

As a reminder, contractors must furnish contract compliance information required in accordance with GPO Contract Terms, Contract Clause 12: Notice of Compliance With Schedules.

Contractors should immediately contact your GPO contract administrator(s) and/or contracting officer(s) to identify impacted orders if any delay is anticipated, including temporarily closure of a production facility or the planned suspension of any services.

If you have any questions on a particular contract, please contact the Customer Services contract administrator and/or contracting officer for your contract (best method of communicating with them is via email). Office team e-mail addresses can be found at https://www.gpo.gov/how-to-work-with-us/agency/services-for-agencies/procurement-services-team.

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 1987 (Rev. January 2018) and GPO Contract Terms, Quality Assurance Through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (revised September 2019).

GPO Contract Terms, Forms and Standards information for contractors can be found on the GPO website at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards. The GPO Contract Terms publications noted above can be downloaded from the GPO website at the following: https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/contractterms2018.pdf and https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap-rev-09-19.pdf.

DOING BUSINESS WITH GPO: Contractors wishing to do business with the GPO are referred to the GPO web site http://www.gpo.gov/how-to-work-with-us/vendors/programs-for-vendors, where one can register as a GPO contractor using the **'GPO Contractor Connection'** link in accordance with the furnished instructions on this page.

NOTE: Prospective and existing GPO contractors are to note that as of January 1, 2008, all contractors seeking to do business with GPO must first complete and thereafter maintain the accuracy of their GPO Contractor Connection registration with the following mandatory taxpayer information boxes: "EIN/TIN #" Employer Identification Number of Taxpayer Identification Number): "Subject to Backup Withholding" (See IRS Form W-9, available for download at http://www.irs.gov/pub/irs-pdf/fw9.pdf.) GPO will withhold payment of invoices for work completed by any contractor who fails to provide this tax data in GPO Contractor Connection. Such invoices will be declared ineligible for payment until all requirements for payment, including providing this tax data in GPO Contractor Connection, have been satisfied.

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

Product Quality Level:
(a) Printing Attributes -Level III.
(b) Finishing Attributes - Level III.

Inspection Levels (from ANSI/ASQC Z1.4):
(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	O.K. Press Sheets/Imaging Inspections
P-9. Solid and Screen Tint Color Match	O.K. Press Sheets/Imaging Inspections

Special Instructions: In the event that the Government waives inspection of press sheets/imaging, the following listed alternate standards shall become the Specified Standards:

P-7. OK'd preproduction samples, OK'd proofs, average type dimension as typeset by contractor.
P-9. OK'd preproduction samples, Pantone Matching System, Government furnished swatch or sample.

SUBCONTRACTING: The predominant production functions are the coordination of the entire project *plus* either the laser imaging of the personalized (variable) information or the printing of the tax statement forms, the BA-6 forms and the rate letters (with newsletters). Contractors who do not provide either (a) the coordination of the entire project and the laser imaging of the personalized (variable information) or (b) the coordination of the entire project and the printing of the tax statement forms, the BA-6 forms and rate letters, will be declared not responsible. All other functions may be subcontracted.

TIME CRITICAL: The requirements under this contract are time critical. For the purposes of this contract, the provision in GPO Contract Terms Pub. 310.2 (Rev. 5-99) for schedule extensions does *not* apply. NO AUTOMATIC EXTENSIONS OF SCHEDULE WILL BE MADE. All bidders must commit to the final mail dates as specified on the print orders.

PREAWARD 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. As part of the financial determination, the contractor in line for award may be required to provide one or more of 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)
6) Letter of commitment from paper supplier(s)
7) Letter of commitment from any subcontractor

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.

During the Preaward Survey, the contractor will be required to provide documentation within 2 workdays of request to demonstrate compliance with the "SAFEGUARD MEASURES FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA" section of these specifications.

Documentation must include IT and security measures information in an in-depth manner similar to "ATTACHMENT A: Sample Enterprise Information Security and Privacy Policy". Contractor is guided to also see the "ADDENDUM Cybersecurity and Protecting Sensitive Information" starting on page 85.

Contractors who are unable to provide this documentation may be declared non-responsible.

Please see the URL links to the documents that describe the safeguard standards required:

NIST 800-53 Revision 4 https://nvd.nist.gov/800-53/Rev4

NIST 800-53A Revision 4 https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

Media Protection Security Family "MP-6 Media Sanitization" https://nvd.nist.gov/800-53/Rev4/control/MP-6

QUALITY CONTROL (QC): Production items should be produced in accordance with all established quality control checks and procedures to ensure that the imaged forms and letters are accurate. Any quality control checks and requirements established such as the use of review sheets, unique mark, tray checks, insertion checks and envelope sealing must be adhered to at all times.

Some or all of the following quality control measures may be required for each project:

- Quality Control (QC) Review Sheets: Upon Government request, the contractor must forward copies of the daily quality control (QC) documents used to verify accuracy during imaging (printing) and insertion. The QC documents must be securely transmitted, and supplied on a daily basis to the Government. Refer to sample copies provided entitled “Accuracy of Imaged Forms” and “Copies of Imaging, Mailing Receipts and Status Reports”.

- Unique Mark: To ensure that production will always begin at the top of the correct Tax Statement form, a unique mark will be placed on the top form of the Tax Statement. An approved form would then be placed on the laser printer with all measurements marked and the top of form mark indicated. This serves as a visual check for the printer operator and the inserter operator. If the operators do not see this mark, it will indicate that the piece was folded, inserted, or printed incorrectly. A missing unique mark requires that a supervisor be contacted to investigate the problem. This QC check must be included on the QC sheet in the area that indicates that the unique mark is being visually checked on a regular and ongoing basis by each operator. The unique mark is a blank square box located in the top left hand corner of each tax statement. The blank square box is imaged with a dot on the inside of the box to indicate the top of the tax statement.

- Tray Check: Tray checks must be used to ensure that the mailing operation is being performed correctly. A tray of mail will be inspected, counted and matched back to the presort listing. As the mail is being sorted, the operator will fan each handful to ensure that there are no empty envelopes being mailed, all envelopes are scaled, that there is a valid mailing address correctly shown head to head through each envelope window, and to check the top of form indicator in the window.

- Insertion Check: The inserter may have a sensor light that lights up if the thickness of an envelope is thicker or thinner than calibrated for a particular job. Because of the private information on the forms, extra precaution is required when setting the calibrator. Checks will be made over and above the standard. At all QC checks, the light (if present) will be checked to make sure it is working properly. QC will note all errors and corrections.

- Envelope Sealing: The inserter may have a valve that controls the water flow that is applied to the envelope flap. The operator controls this valve. The valve (if present) will be checked before beginning the insertion process to make sure it is working properly. A column should be included on the QC sheet so that at each QC check it will be indicated that the water flow has been checked and that it is working properly or the corrections were made. If a problem is found, the contractor will check each previous piece to find where the problem started and seal as needed.

Copies of Imaging, Mailing Receipts and Status Reports: Contractor is required to provide copies of all pages of all mailing receipts (GPO Form 712, PS Form 3600-R or equivalents) on a daily basis to the agency. Contractor is required to provide copies of the Quality Control (QC) review sheets on a daily basis to the agency (refer to the section entitled, Quality Control (QC) Review Sheets). Contractor is

required to establish an imaging and mailing schedule prior to imaging and mailing, and to provide a daily status report with the mailing receipts. The schedule and the daily status reports must include the number of statements imaged and the number of statements mailed by zip code ranges. These reports must provide the information for all forms imaged and mailed within the previous 24 hours. These should also include the target date that each group was to mail as well as the actual date mailed, quantity deemed unqualified for mailing with a separate description of problems making them unmailable, and quantities of statements requiring reprinting. Additionally, any other pertinent information should be provided or as requested by the Government.

CONTRACTOR MEETING WITH THE USPS: Contractor is required to meet yearly with the appropriate personnel of the Post Office where the mailings will be made. This meeting must be held and problems resolved before production begins.

Government permit imprint mailing allows mailed pieces to be mailed without the postage being deposited at the Post Office. However, an account must be established by the contractor at the Post Office. The cost to establish the Government permit imprint account will be borne by the agency.

Contractor may be required to bring preproduction samples for approval by the Post Office.

Contractor is responsible for reviewing all factors which could affect mail acceptance including ensuring that:

- The Post Office location for the mailings is familiar with Government permit imprint mail.
- Specific requirements for mail using a Government permit imprint are met, including requirements which may affect the wording of the permit imprint and/or requirements that require additional paperwork and account set up prior to the mailing being accepted by the Postal Service.
- Problems are resolved sufficiently before the start of mailing such that delays in mailing do not occur.
- Mail at the lowest automated barcoded first-class rates.

INSPECTIONS OF LASER PERSONALIZATION AND MAILING OPERATIONS: Onsite inspections of these operations by the agency may be required, or at the Government's option, contractor may be required to overnight or fax inspection samples to the Agency at the contractor's expense. At the Government's option, agency may conduct a phone inspection with the contractor concerning the contractor's operation.

Notification: The contractor must provide a ten (10) workday notification prior to the start of laser personalization and mailing operations. At that time, if requested, an inspection schedule must be furnished including contact names, street addresses, email addresses, and phone and fax numbers for all inspection locations. Restrictions regarding day and time of inspection are not applicable to these laser personalization and mailing operation inspections.

If the inspection is conducted at the contractor's plant, the inspection production sample will be produced by the contractor and reviewed onsite by the agency representative(s).

Laser image personalization inspections will include inspection of laser imaging of all forms. This will also include cutting (if applicable), folding, inserting, sealing, sorting, mailing prep (including bagging, traying, etc.) and inspection of the holding area to insure that forms are kept separate from other work in progress, safe, and secure.

The inspection production sample must be fully imaged. The Government may exercise the option to have the sample folded, inserted into envelopes, envelopes sealed and sorted for mailing. The Agency will inspect these samples from actual production to confirm that the variable information imaged is correct. THE CONTRACTOR MUST REGENERATE ALL FORMS SO THAT ALL RECIPIENTS WILL RECEIVE A MAILING.

Laser personalization and mailing operation inspections must be structured so that the Government representatives can spend the minimum amount of time at the inspection. The cutting (if required), folding, inserting, sealing, sorting, and preparation for mailing must be started as forms are being imaged so that these operations can also be reviewed the same day as the imaging inspections. These operations must be produced at the same plant as the imaging or at a plant that is within a 1 hour drive so that these inspections can be held the same day.

If the inspections cannot be completed within one day, per diem charges will be deducted from the contractor's voucher for the actual number of Government representatives up to a maximum of two, for each additional day spent. If there is a delay in excess of one day, the Government representatives may report back to their duty stations. The travel costs for the representatives to go back to the inspection as well as their per diem costs will then be deducted from the contractor's voucher.

Mailing must NOT proceed without the "OK to Mail" approval from the agency. An "OK to Mail" or "Hold" will be issued within 4 hours of the contractor's notification. Do NOT delay any other operations awaiting this OK.

GOVERNMENT IN-PLANT INSPECTIONS: The Government reserves the right to have Government representative(s) inspect any operation under this contract at the start of production and at any time during production. In addition to the inspections indicated, the Government reserves the right to inspect all stages of production.

Contractor must use the actual final live data for all personalization and mailing operation inspections and samples.

Notifications for Printing Press Inspections: Contractor must provide the Government with a 5-workday notification for all press inspections. These inspections must be held Monday through Friday, exclusive of Federal holidays, between the hours of 8 a.m. and 5 p.m.

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 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 periodic pricing revision.

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 **September 1, 2020 to August 31, 2021**, 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 **May 31, 2021**, 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.

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 other information pertinent to the particular order.

NOTIFICATION: The contractor may be notified on or before June 30 of each year of availability or non-availability of funds for subsequent periods. Cancellation may be effected if (i) the Contracting Officer notifies the contractor that funds are not available for the next year, or (ii) the Contracting Officer fails to notify the contractor that funds are available for the next year.

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 **September 1, 2020 through August 31, 2021**, 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” 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, 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.

OPTIONS: Whenever an option is indicated in the specifications, it is the Government's option, not the contractor's, unless it is specifically stated otherwise.

POSTAWARD CONFERENCE: At the Government’s option, immediately after award a postaward conference with contractor representative(s) may be held via telephone conference to discuss the requirements of the contract.

PRODUCTION CONFERENCES: Government representatives may, at agency’s option, conduct one or more production conferences each year with the prime contractor and all subcontractors. Meetings will either be held at a Chicago, IL location or via phone conference, at the Government’s option. The prime contractor and their subcontractors will be responsible for all costs related to attending such meetings, whether in person or by phone. Representatives at these meeting must be able to discuss ALL aspects of production from start to finish. Additionally, the contractor and their subcontractors must be able to provide technical support and assistance during the term of the contract. No additional charges will be allowed for such performance.

CONTRACTOR CUSTOMER SERVICE REPRESENTATIVE: Contractor must have a customer service representative for this account available between the hours of 9 a.m. to 5 p.m. prevailing Chicago, IL time. This person must be able to be accessed via phone, fax and e-mail. Representative must be able to address ALL aspects of the contract, including production status, as well as technical areas. Back up support to this representative must be available in the absence of the primary contact and to provide additional technical expertise. Government inquiries must receive a response within one hour.

CONFIDENTIALITY OF INFORMATION: Information regarding any individual is of a confidential nature and may be used only for the purposes of producing the requirements of this contract. All materials containing confidential information, including but not exclusive to Government furnished data, imaged forms, and scrap, must be handled so that information does not have any unauthorized use. All scrap generated with any information regarding any individual person must be shredded, incinerated, otherwise destroyed beyond recognition. Any media (files, disks, etc.) produced by the RRB and sent to the contractor MUST be returned to the RRB upon completion of the specific order. Contractor must return this material via an overnight delivery service to prevent theft or accidental use.

SAFEGUARD MEASURES FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA: Agency policies require documentation that PII data sent to contractor remains secure while projects are in progress and is eventually destroyed in such a way that it cannot be retrieved or restored after being deleted from the contractor's hard drives/systems.

Contractor is required to meet or exceed the following security measures, and provide documentation of ability to comply, see "PREAWARD SURVEY" for details.

Physical Access Policy

- All entry points and exits to and from the Production area are security controlled. Entry points include the front lobby and the employee entrance. The production area is under 24 hour surveillance (inside and outside the building). Any attempted physical access violations are investigated and appropriate action is taken when needed. If an employee is terminated their access is immediately made void and any access will be denied.

Production Area

All employees having access to RRB data must:

- Have been approved through a documented background security check.
- Are aware of the sensitive information involved.
- Are aware of the penalty associated with any criminal action.

Data Security

- Access to data is provided on a need-to-know basis, universal access is not granted.
- Data is protected through the use of profiles specifying who and what type of access is allowed.
- All computer monitors are password protected with a "strong" password. All passwords must expire and must be reset on a regular basis.
- Only approved company software is permitted on computers.
- Connection of non-approved devices to any workstation is prohibited.
- RRB processed data must be stored on the main frame and can only be accessed by authorized personnel.

The process from data receipt to deletion is:

- Data is received either electronically or on tape media.
- Any tape media is returned, after data is downloaded to the network.
- Data is processed and mailed per client instructions.
- Unless the client requests a different time span, data is retained for a period of no more than six weeks. This retention is to ensure that any questions resulting from the mailing can be answered by the contractor's team.
- At the end of this retention period the directory structure containing the data is deleted from the network.
- The space that is released from the deletion will be overwritten within 1 to 3 days.
- The process of overwriting the space that once held the deleted data starts immediately.
- No user is permitted to install software on either a server or their desktop, preventing any reconstruction software from being installed.
- The only users that have access to the areas of disk that houses the PIN data are all security cleared to the highest levels.

Data Security Reporting

Contractor must have software to generate reports, or equivalent procedures that include:

Server Encryption: Bitlocker Drive Encryption or similar. Additional enterprise server-based encryption measures may be implemented. Encryption measures should include all laptops or computers that will be removed from the facility.

Secure Data Transfer between Agency and Contractor: Data for the RRA Rate Letters and RRA Tax Statements is transmitted via secure FTP. Data for the RUIA forms BA-6 will be transmitted by tape cartridge due to its large file size, or at agency's option may be transmitted via secure FTP.

Complete Documentation of SourceLink IT and Security Policies: "Attachment A: Enterprise Information Security and Privacy Policy" is a sample of the type of complete documentation of IT and Security policies required for fulfillment of this contract. Please note the specific reference to Agency requirements: "Electronic storage media must be securely wiped by overwriting (i.e. DoD standard) or degaussing prior to disposal or reuse."

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. For "PRIVACY ACT" purposes, "agency" refers to the Railroad Retirement Board (RRB).

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.

FEDERAL TAX INFORMATION (FTI): Section 6103 of the Internal Revenue Code (26 U.S.C. §6103) requires that returns and return information must be kept confidential and may not be disclosed except as permitted by the Internal Revenue Code. The term "return" means any tax or information return, declaration of estimated tax, or claim for refund required by, provided for, or permitted under the Internal Revenue Code and filed with the Secretary of the Treasury. "Return information" is defined very broadly, and includes a taxpayer's identity, the nature, source, or amount of his income, payments, deductions, the existence or progress of an audit, or any other data provided to or collected by the Secretary with respect to a return or determining the existence of tax liability for any person under the Internal Revenue Code. However, return information does not include data in a form which cannot be associated with or otherwise identify a particular taxpayer. Collectively, the IRS uses the term "federal tax information" or FTI to refer to any return or return information received by the IRS or secondary sources, including any information created by a recipient that is derived from return or return information. The RRB receives FTI from the IRS under 26 U.S.C. §6103(h)(5) (permitting disclosure to enable the RRB to withhold tax

from Tier I benefits) and 26 U.S.C. §6103(l)(1) (permitting disclosure of taxes imposed by the Railroad Retirement Tax Act for purposes of the RRB administering the Railroad Retirement Act).

BREACH NOTIFICATION: The contractor is required to notify the RRB contracting officer's representative and GPO contract administrator within one hour of determination of any actual or potential breach of RRB data. The agency has an additional 30 minutes to prepare and submit the appropriate breach report to Department of Homeland Security, US-CERT. These requirements will be met at no additional cost to the Government.

BREACH RESPONSIBILITY: If it is determined that the contractor is responsible for a breach of RRB data, contractor shall be responsible for all breach related costs (notification, credit monitoring, legal settlements, etc.) The RRB shall determine if the contractor is responsible for any breach of RRB's data. These requirements will be met at no additional cost to the Government.

LIMITATION OF PERFORMANCE AND CONTRACTOR OBLIGATIONS:

(a) Funds are available for performance of this contract for the first program period only. The amount of funds available at award are not considered sufficient for performance required for any program year other than the first program year. When additional funds are available for the full requirements for the next succeeding program year, the Contracting Officer may (circumstances permitting), so notify the contractor in writing not later than 30 calendar days before the expiration of the program year for which performance has been funded (unless a later day is agreed to). Notification that funds are not available may effect cancellation of the contract.

(b) The Government is not obligated to the contractor for any amount over requirements for which funds have been made available and as obligated by each print order.

(c) The contractor is not obligated to incur costs for the performance required for any program year after the first, unless and until written notification is received from the Contracting Officer of an increase in availability of funds. If so notified, the contractor's obligation shall increase only to the extent contract performance is required for the additional option program year for which funds have been made available.

(d) If this contract is terminated under the "Termination for Convenience of the Government" clause "total contract price" in that clause means the amount available for performance of this contract, as provided for in this clause. The term "Work in Process" in that clause means the work under program period requirements for which funds have been made available. If the contract is terminated for default, the Government's rights under this contract shall apply to the entire multiyear requirements.

(e) Notification to the contractor of an increase or decrease in the funds for performance of the contract under another clause (e.g., the "option" or "changes" clause) shall not constitute the notification required by paragraph (a).

(f) This procedure shall apply for each successive program year.

USE OF THE SEAL OF THE RAILROAD RETIREMENT BOARD (RRB): Use of the seal of the Railroad Retirement Board is subject to the following permissions, procedures and penalties outlined in 20 C.F.R. PART 369 (as amended)—USE OF THE SEAL OF THE RAILROAD RETIREMENT BOARD, Title 20: Employees' Benefits.

PAYMENT: Submit 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 invoicing. 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.

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/vendors/how-to-get-paid.

Courtesy Copy of Invoice: Contractor is required to provide a copy of each print order invoice voucher (including postal statements) to the Chicago RRB within two workdays of fax submission to GPO FMCE.

U.S. Railroad Retirement Board
844 N. Rush Street
Chicago, IL 60611-2092
George.keesee@gpo.gov

RECEIPTS FOR DELIVERY: Contractor must furnish their own receipts for delivery, and postal statements for mailing, as suitable. These receipts must include the GPO jacket, program and print order numbers, total quantity shipped and/or delivered, number of cartons and quantity per carton; date delivery made; and signature of the Government agent accepting delivery. Original copy of these receipts or other acceptable proof must accompany the contractor's voucher for payment.

NOTE: Number of pieces listed on the postal receipts MUST match the number of recipients in the supplied distribution lists, with an accounting for undeliverables, etc.

CONTRACTOR'S INVOICE FOR PAYMENT MUST BE ITEMIZED IN ACCORDANCE WITH THE SCHEDULE OF PRICES. FAILURE TO ITEMIZE IN ACCORDANCE WITH THE SCHEDULE OF PRICES MAY RESULT IN DELAYED PAYMENT.

SECTION 2.- SPECIFICATIONS

SCOPE: These specifications cover the production of printed window envelopes, printed & personalized laser imaged forms, and printed & personalized laser imaged rate letters, and newsletters, requiring such operations as pick up and/or receipt of furnished materials, design, typesetting, proofs, preproduction quality control samples, inspection samples, printing in up to two colors of ink, cutting, perforating, folding, inserting printed items into and sealing envelopes, acceptance of Postal Service mailing permits, Postal Service sorting and barcoding to obtain the best possible First Class rates, conducting quality control reviews during production, mailing, providing and updating production and mailing status reports, and related operations.

TITLE: RRB Rate Letters, Tax Statements, BA-6 Forms.

Although this is an option year contract, all estimates, averages, etc., are based on one year's production. Quantities and/or items produced cannot guaranteed.

This contract is comprised of 3 different projects: Rate Letters, Tax Statements, and BA-6 Forms. Specifications apply to all projects unless stated otherwise in each individual project section.

Table of Contents:

FREQUENCY OF ORDERS: It is estimated that one Rate Letters project, one Tax Statements project, and one BA-6 Forms project will be placed per contract year.

QUANTITIES:

See the additional requirements for quantities in each project section.

All quantities are +/- NONE. 100% production is required. It is the contractor's responsibility to produce any additional quantities required for samples and spoilage.

NOTICE TO BIDDERS: The RRB will be converting to an online system (Paperless), where the RRB's customers can view and print their forms from their home computer. As of the publishing date of this solicitation, the RRB has not yet started the Paperless project. The RRB hopes to have a Paperless system implemented before the end of the base and all option periods of this contract. The Contractor "should" expect to see a decline in the quantities required in the latter option years when the Paperless project is completed and implemented.

THEREFORE, The Contractor is STRONGLY encouraged to contact GPO AND the RRB (at a minimum) annually to enquire about projected completion and implementation of the RRB's Paperless project AND the ESTIMATED quantities required prior to each phase being started by the Contractor.

GOVERNMENT TO FURNISH:

Non-variable text on forms and envelopes: It is anticipated that electronic files created in a PC-based program such as Microsoft Word or similar will be furnished. At the Government's option, camera copy, manuscript copy, or samples of previous printed pieces with corrections may be furnished. Rough page layouts may be furnished. Manuscript copy may be handwritten or typed. Combinations of the above may be furnished. Electronic files will be uploaded by the agency to the contractor's secure FTP site. At the Government's option, data files may be made available for pickup or e-mailed using secure encryption to the contractor as file attachments.

Variable data personalized information: Data files for the variable data personalized information will be furnished as ASCII files. Electronic files will be uploaded by the agency to the contractor's secure FTP site. At the Government's option, data files may be made available for pickup or e-mailed using secure encryption to the contractor as file attachments. If applicable, the data will be sorted as follows: (1) GEO code order – with records containing foreign addresses first; and (2) ZIP Code order.

Preproduction Quality Control Samples: Data files will be furnished for preproduction samples. These files will use actual data. Data files for preproduction samples will be furnished as ASCII files. Electronic files will be uploaded by the agency to the contractor's secure FTP site. At the Government's option, data files may be made available for pickup or e-mailed using secure encryption to the contractor as file attachments.

Furnished Fonts: Fonts provided, if any, (see "CONTRACTOR TO FURNISH") are the property of the ordering agency and are provided for use on this contract only. Using the furnished fonts for any job other than the one for which the fonts were submitted violates copyright law. All fonts should be eliminated from contractor archive immediately after completion of the production run.

GPO Form 2511 Print Order: Print orders will generally be enclosed with furnished materials or sent via email. At the Government's option, print orders may be furnished as a hard copy, a faxed copy, or by secure FTP. Contractor must be able to accept via email.

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 will be required to provide fonts as specified.

ELECTRONIC PREPRESS: Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure accurate output of the required reproduction image. Any errors, media damage or data corruption that might interfere with proper file imaging must be reported to the Agency and Chuck Szopo at 312-353-3916 x6 in sufficient time to comply with the shipping schedule. 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 Assurance Through Attributes Program (QATAP) quality level. Contractor must maintain the latest version of all programs and operating systems used in this contract as well as maintain backwards-compatibility.

TYPESETTING, LAYOUT AND PERSONALIZATION:

<u>See the additional requirements for typesetting, layout and personalization in each project section.</u>

For printed copy (not laser imaged personalized copy), contractor will be required to set type and create layouts as directed. Copy on both forms and envelopes is anticipated to have either minor or major changes every year. It is anticipated that yearly changes to the envelopes will be minor. Data boxes on the tax statement forms may change from year to year. The Government also has the option to entirely redesign the forms. Copy furnished on a disk or via email may need to be reformatted by the contractor. Contractor will be required to provide the correct fonts, formatting for columns, etc.

All imaged addresses must be complete and include the agency's encoded line, the recipient's name, and complete mailing address. Addresses in the United States or as otherwise applicable, must have the zip + 4 barcode. The address showing through the window must include a barcode. Contractor must use the largest type size that will fit in the window and still meet all Postal Service requirements. No other information other than what has been indicated can show through the window.

Contractor will be allowed to insert a matching code in the address block that shows through the envelope's window. The matching code must not interfere with any other information or affect the piece being accepted by the Postal Service. The size of the matching code must be inconspicuous and in a smaller typeface than the other information on the tax statement forms. Matching codes, if used, must appear on all Preproduction Quality Control Samples. Contractor must provide the agency with information as to the type of code to be used and what it indicates.

The agency retains the right as to the final decision as to the acceptability of the typefaces and sizes used. Once approved, contractor may not make revisions without written approval from the agency.

NOTE: When typesetting and creating layout designs, the contractor must remember all factors which will affect the final production of the forms. Fields which will be laser imaged must be designed with that in mind. Printed type must be positioned so that it will not show through the window and that all forms will meet the Postal Service tap test. Perforating and folding must be taken into consideration so that the forms will fold neatly and cleanly (on perforations when applicable), and be machine insertable.

ENVELOPE INVENTORY: If envelope copy is changed during the term of the contract, the contractor must comply with the new requirement, and cannot exhaust previous stock. The contractor must produce a new supply of envelopes using the current valid copy of the envelopes.

PROOFS:

See the additional requirements for proofing in each project section.

1-4 sets of proofs, in any combination of the proof types below, may be ordered for each version of any production item, as specified on the GPO Form 2511 Print Order or as otherwise directed by the agency. These proofs must contain all non-variable (but not the personalized) copy.

Digital Content Proofs (Black or Color): 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. Contractor must submit ink draw downs on actual production stock of Pantone color(s) used to produce the product.

"Press Quality" PDF "Soft" Proof (For Content Only): Must be created 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. Contractor must call agency point of contact to confirm receipt.

AUTHOR'S ALTERATIONS: Author's Alterations consist of all marks made by the author at variance with the original copy as submitted to the contractor, but do not include corrections marked by the agency due to the failure of the contractor to follow copy literally.

It is anticipated that proofs WILL NOT be "OK'd with Corrections" and that revised proofs will be required at all times for both Author's Alterations and Printer's Errors. No extra time in the schedule can be allowed for this reproofing; such operations must be accomplished within the original production schedule allotted in the specifications.

Occasionally, when Printer's Errors are minor on content proofs, and it is the Government's intent to order digital contract proofs next, contractor will be allowed to proceed to the next proofing stage. In such cases, the Government will pay for the contract proofs as the next proofing stage. Contractor, however, is not to proceed to this stage unless specifically authorized to do so by the Government.

Author's Alterations will be charged at the regular contract rates per the "Schedule of Prices." Charges for making AA's will not be honored unless the voucher that is submitted to GPO is supported by appropriate documentation.

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.

Contractor MUST NOT produce Preproduction Quality Control Samples until the "OK to Produce Preproduction Samples" is received.

PREPRODUCTION QUALITY CONTROL SAMPLES:

See the additional requirements for Preproduction Quality Control Samples in each project section.

Contractor to provide the number of Preproduction Quality Control Samples ordered on the print order or otherwise requested by the agency. Provide one imaged sample for each individual data file.

Preproduction Quality Control Samples must be printed, constructed, and laser imaged using the same copy, colors of ink, equipment, methods of production, and paper that will be used in the final products. These samples must be address-sorted using the same method as the final imaging and sorting. Preproduction Quality Control Samples must be representative of the final product in all respects and include both the printed information and the personalized information. Envelopes must be printed, converted and constructed (machine die-cut, folded and glued, including the poly insert) to be the same as the final product.

Preproduction Quality Control Samples may be required to be generated from a specific file for data files or may be required to be imaged using the final data files for actual imaging. If these samples are imaged from the final data, contractor will be instructed as to which files are to be used, e.g., the first 100 names from each file.

All Preproduction Quality Control Samples will be examined for quality, compliance with the file layout, correct variable data locations, dollar figure alignment on the decimal point, required information appears

in the envelope window no additional information appears in the envelope window, information is correctly suppressed, and similar.

The agency will approve, conditionally approve, or disapprove the samples. Approval or conditional approval shall not relieve the contractor from compliance 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, because of contractor's error, the samples are disapproved by the agency, the Government at its option may require the contractor to submit additional samples for inspection and testing or to make the changes on the next preproduction run. 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.

STOCK:

BIDDERS, PLEASE NOTE: GPO has issued a new *Government Paper Specification Standards, No. 13*, dated September 2019. Prospective bidders should carefully read this publication as the applicable standards within become an integral part of this contract. The document is posted at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards along with a list of major revisions and any amendments thereto.

Rate Letters, Newsletters, Tax Statements, BA-6 Forms: White Opacified Offset Book, basis size 25 x 38", 60 lbs. per 500 sheets, equal to JCP A80.

Window Envelopes: At contractor's option, either White Wove or Bleached White Kraft, basis size 17 x 22", 24 lbs. per 500 sheets, equal to JCP V20. Do NOT mix stocks. Use suitable clear poly insert for envelope window(s) in compliance with USPS requirements for OCR readability and all other USPS regulations and requirements.

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

BINDING OPERATIONS:

See the additional requirements for binding operations in each project section.

All cutting (if required due to contractor's method of operation), folding, inserting, sorting, traying, sacking, etc. must be done at a single location. These must be done at the same location as the imaging or within a one-hour drive of the imaging location.

PACKING: Bulk shipments must be packed suitably in shipping containers. Containers must be a minimum of 275 psi and must not exceed 45 lbs. when fully packed.

LABELING AND MARKING: Refer to Labeling and Marking Specifications (GPO Form 905). See GPO Contract Terms Booklet, Publication 310.2. for more information.

All expenses incidental to packing and labeling bundles and containers must be borne by the contractor.

SORTING, MAILING AND DISTRIBUTING IN ACCORDANCE WITH POSTAL SERVICE (USPS) REGULATIONS:

See the additional requirements for sorting, mailing and distribution in each project section.

All mailed pieces must meet all USPS requirements and must mail at the lowest First-Class rates for which they can qualify.

Address Sorting: CASS Certification is not required for the Rate Letters and Tax Statement Projects. The RRB shall provide the Contractor the CASS certification produced from the current address updates of its beneficiary records.

The Contractor shall do all sorting and CASS Certification for the BA-6 project to achieve the lowest automated, barcoded, First Class postage rates. Data files will NOT be supplied sorted in accordance with Postal Service requirements. Contractor must process all addresses at the highest sortation level (carrier route, etc.), add barcodes, and change addresses to meet Postal Service format requirements and CASS certify. However, contractor should make the minimum standardization change to addresses that would still be acceptable to the Postal Service for the most favorable rates.

(Note: The RRB does not rate letters and tax statement addresses changed based on Emergency/911 address changes applied to the rate letters and tax statements.)

NCOA Processing: Will not be required for the Rate Letters project or the Tax Statements project.

NCOA will be required for the BA-6 project.

USPS Addressing and Tap Test Requirements: The laser imaged copy in the address block must meet all USPS requirements including those for typography, print quality, reflectance, barcode location, clear zones, tap test, etc. The forms and envelopes must be produced so that all information required will appear through the window but that no extraneous copy will show. Confidentiality of the information on the forms must be maintained.

Postal Service Forms and Other Requirements: Contractor must generate all bag tags, tray labels, etc. They will be required to do all bagging, traying, sorting, etc. for this class of mail and level of sortation. Contractor must generate and accurately complete all required Postal Service forms.

Accuracy of Imaged Forms: A form must be produced for each data file. 100% of the records must be properly imaged and mailed. No improper forms may be distributed. No duplicate forms may be distributed. No damaged forms may be distributed. Contractor must guarantee 100% accuracy. Contractor must have a method for verifying that all records are correctly imaged and a plan for regenerating any that are incorrectly imaged, damaged, or destroyed. This must include methods for determining what records have been imaged to insure the imaging of all forms, tracking all forms, determining missing or damaged forms, insuring that damaged forms and test forms are not mailed, regenerating forms that are missing or damaged, and insuring that duplicate forms are not generated or mailed. Additionally, contractor must have a specific plan for guaranteeing that incorrectly imaged statements or duplicate statements, produced for whatever reason (tests, makeready, spoilage, etc.) are not mailed and are destroyed by a process that renders them unreadable, such as by shredding or incineration.

GPO "VERIFICATION OF DELIVERY": Contractor MUST email delivery verification information to VerifyChicago@gpo.gov WITHIN 24 HOURS OF DELIVERY. Enter Program and Print Order numbers in the subject line, and in the body of the message indicate the method of shipment and the delivery date. If a contract specifies a shipping method of **f.o.b. contractor city** (at government's expense), enter the date of shipment. If a contract specifies **f.o.b. destination** (at contractor's expense), enter the date of delivery. If a contract specifies a combination of both methods, include all shipping and

delivery dates. **Failure to provide this information for each print order may result in delayed payment of invoices.**

DISTRIBUTION:

See the additional requirements for distribution in each project section.

Mailing of any project must not commence until "OK to Mail" approval is given by the agency.

Deliver F.O.B. Destination (at contractor's expense) via traceable means, items such as samples and bulk shipments.

All pickups and deliveries must be made at the U.S. Railroad Retirement Board, 844 N. Rush Street, Chicago, IL 60611-2092. Specific room numbers will be provided on each GPO Form 2511 Print Order.

Mail F.O.B. Contractor's City all individual mail pieces. Contractor must mail all addresses within the same zip code on the same day. The mailing of the tax statements may be in batches.

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

All mailing must be made at the lowest first class, carrier route sorted, barcoded rates.

Use of Government postage and fees paid permit imprint (indicia): Contractor must mail using a Government postage and fees paid permit imprint (indicia) printed on the envelopes.

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 required by the USPS.

Contractor must guarantee 100% production of all data records. A properly personalized form must be produced and mailed for each individual record.

Damaged Forms: Contractor must maintain a record of all damaged imaged forms and a record of when these forms were regenerated. These records will be required to be provided to the agency upon request, and if not requested earlier, must be provided within one workday of the completion of the mailing. NOTE: ALL DAMAGED FORMS MUST BE REGENERATED AND MAILED WITHIN THE CONTRACT SCHEDULE.

Non-USPS Postage (Invalids): It is anticipated that a small quantity of mailings may contain mailing addresses deemed invalid (unqualified) by the U.S. Postal Service (may not qualify for the imprint). Contractor is required to apply the appropriate equivalent postage to Invalids. Contractor must notify the agency of any such non-qualifying pieces. At the Government's option, the contractor may be required to overnight these pieces to the agency at the contractor's expense.

- Contractor must mail the fully imaged mail pieces whose addresses are deemed invalid but have addresses that look like they can be mailed. This type of invalid address contains a name, street address, city, state, zip code and/or province and country.

- Contractor must return the fully imaged mail pieces to the agency when addresses are deemed invalid but do not look like they can be mailed (i.e., no address, incomplete address or nonsensical address).

- Contractor must provide two lists to the Government containing the claim numbers that have invalid mailing addresses. 1) Claim numbers with invalid addresses that were mailed by the contractor. 2) Claim numbers with invalid addresses that were not mailed but returned to the agency. The agency will use the files and lists to identify the claim numbers and correct the mailing addresses for future mailings.

Contractor will be reimbursed for Non-USPS postage by submitting a properly completed Postal Service form with invoice voucher.

All expenses incidental to overnight delivery services, picking up and returning materials, picking up and submitting proofs and preproduction samples, furnishing sample copies, furnishing supply of blank form and envelope copies, and providing all required receipts, records, etc., must be borne by the contractor.

SCHEDULE:

See the additional requirements for schedule in each project section.

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

No definite dates for placement of orders or pickup of material can be predetermined.

All pickups and deliveries must be made Monday through Friday, exclusive of Federal Holidays, before 3:30 pm local prevailing time.

Workdays and Calendar Days: Workdays are Monday through Friday, exclusive of Federal Holidays. Calendar days are actual calendar days. Schedules for BA-6 forms are entirely in workdays. Schedules for tax statements are in workdays for all production up to the QC Production Samples. The QC samples, production inspection samples, and all production imaging and mailing operations and related functions are computed based on actual calendar days, not workdays. Rate letters schedules are based on workdays. "Delivered by" dates are dates by which the items are actually received by the Agency. "Available for pickup" dates are dates by which the material is available for pickup by the contractor or the contractor's designated carrier. If the contractor picks up via an overnight carrier, they will not actually receive the returned items until the next day.

NOTE: For the purposes of this contract, if items are produced or reviewed in a lesser time than is required by the contract, the next production period will be based as to when that item is actually produced or reviewed, not the maximum amount of time that would have been allowed under the contract.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with each 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 MATERIALS: All furnished materials must be returned to the Agency at the address indicated in "Distribution". All expenses incidental to the pickup and return of all Government Furnished Material and furnished samples must be borne by the contractor.

RATE LETTERS PROJECT – Approximately 1 order per year.

The Rate Letter project consists of up to 21 different forms, two newsletter versions, and two different envelopes (the domestic and the airmail envelopes). Forms are printed and laser personalized.

QUANTITIES: Quantities indicated are estimated.

Item	Quantity (Domestic)	Quantity (Foreign)
Rate Letters		
(Face only, with newsletter insert)	(RL-6 newsletter insert)	(RL-6F newsletter insert)
Form RL-46 (1 version)	41,736	186
Form RL-47 (16 versions)	463,563	2,312
Form RL-48 (1 version)	352	15
Form RL-49 (1 version)	16,152	20
Subtotal of letters ordered:	522,803	2,533
Subtotal of face only pages invoiced:	522,803	2,533
(Face only, no newsletter insert)	(No newsletter insert)	(No newsletter insert)
Form RL-41 (1 version)	9,727	12
Subtotal of letters ordered:	9,727	12
Subtotal of face only pages invoiced:	9,727	12
Subtotal all letters ordered:	532,530	2,543
Subtotal of face only pages invoiced:	532,530	2,543
TOTAL of letters ordered:	535,075	
TOTAL face only pages invoiced:	535,075 (+20 (or 19) MR)	
Newsletters		
Form RL-6 (face and back)	522,803	0
Form RL-6F (face only)	0	2,533
Subtotal of face and back pages invoiced:	1,045,606	0
Subtotal of face only pages invoiced:	0	2,533
TOTAL of newsletters ordered:	525,336	
TOTAL newsletter pages invoiced:	1,048,139 (+2 MR)	
Rate Letter Envelopes		
Envelopes	532,663	0
Air Mail Envelopes	0	2,412
TOTAL of envelopes ordered:	535,075	
TOTAL envelopes invoiced:	535,075 (+2 MR)	

Beneficiaries will receive one of 20 (or 19) versions of the Rate Letter (based upon a 2-digit code on the file) along with a newsletter insert (Form RL-6 for beneficiaries residing in the United States or Form RL-6F for beneficiaries residing in foreign countries). There are 5 rate letter form numbers – one form number (RL-47) contains 16 different versions. The versions differ depending on the makeup of the annuity; the different annuity components. For example: one version may contain a Tier 1, Tier 2, and a Vested Dual Benefit amount. Another version may consist of a Tier 1 and Supplemental Annuity, etc.

Each Rate Letter for Forms RL-46, RL-47, RL-48 and RL-49 is to be enclosed in a separate envelope along with one newsletter insert. Each letter for Form RL-41 is to be enclosed in a separate envelope only (no newsletter enclosed). During non-cost of living increase years, Form RL-48 (reject rate notification letter) will not be used, reducing the number of letter versions from 20 to 19.

TRIM SIZES:

Rate Letters and Newsletters: 8-1/2 x 11".

Rate Letter Window Envelopes: Size 9-1/4 x 4-1/8" with 4-1/2 x 1-1/4" single window positioned 1/2" from the left and 5/8" from the bottom. Window must be large enough to accommodate all required information.

TYPESETTING, LAYOUT AND PERSONALIZATION:

Rate Letters (non-variable text): It is anticipated that Rate Letters will have minor to moderate wording changes each year. At the Government's option, Rate Letters may be fully redesigned in any given year. Agency-furnished electronic files must be reformatted by the contractor to meet supplied requirements. If provided, follow supplied samples for type size, style and layout. All columns of figures must align on the decimal point unless specifically indicated otherwise by the agency.

Rate Letters (variable data personalized information): Rate Letters will be personalized with customer name, financial data, mailing address and/or other information. Each form has approximately 60 different elements of variable data. Contractor will be required to create electronic overlays (similar to an AFP overlay) for each of the 20 (or 19) versions. Contractor will be required to provide any programming necessary to utilize furnished data files. Some data fields will be suppressed. Suppressed fields will be coded.

Data files for the variable data personalized information will be furnished sorted in the following order: 1) GEO code order with records containing foreign addresses first; 2) ZIP Code order. Each record in the file will contain a 2-digit code indicating which one of the 20 (or 19) versions of the Rate Letter is to be printed for the addressee.

Newsletters (Forms RL-6 and RL-6F): Contractor will be required to set type and layout all page elements to meet supplied requirements. It is anticipated that the newsletters will have minor wording changes each year, to each version.

Rate Letter Security Window Envelopes: It is anticipated that changes to the envelopes will be minor. Envelope is to be typeset with approximately 7 lines of type, logo and one rule, which represents the return address, import information statement, address service requested line, airmail designation on foreign version and indicia. Window must be large enough to accommodate all required information such as the recipient's name, mailing address, city, state, zip code, province; country; contractor's matching code; barcode; and any required endorsement line. No additional copy may appear through the window. The statement "IMPORTANT INFORMATION ENCLOSED" is to be printed to the right of the window in a location that does not interfere with USPS requirements for OCR readability. "Address Service Requested" line must be typeset in compliance with postal service requirements.

See "TYPESETTING, LAYOUT AND PERSONALIZATION" on page 16 for additional information.

PROOFS:

One to four sets of proofs may be ordered for each version of the Rate Letters, Newsletters and Envelopes, as specified on the GPO Form 2511 Print Order or as directed by the agency. These proofs must contain all non-variable (but not the personalized) copy.

Digital Content Proofs and/or PDF Proofs may be ordered. Proofs will not be returned. Approval or changes will be sent to contractor via email.

AUTHOR'S ALTERATIONS: Author's alterations (AA's) may occur during the proofing stage. At the Government's option, changes may be supplied by the Agency or requested from the contractor.

Author's Alterations (AA's) proofs shall be PDF proofs, provided via e-mail to one or more email addresses as provided by the Agency.

At the Government's option, Digital Content Proofs may also, or alternatively, be requested as AA's proofs.

Author's Alterations of the newsletters are to be provided as PDFs with the initial approximately 100 records, and as hard copies with the second test file of approximately 700 records.

AA's proofs will not be returned. Approval or changes will be sent via email.

See "PROOFS" on page 17 for additional information.

Contractor MUST NOT produce Preproduction Samples until the "OK to Produce Preproduction Samples" is received.

PREPRODUCTION QUALITY CONTROL SAMPLES: The contractor will be required to furnish two groups of Preproduction Quality Control Samples for the Rate Letters project. The first sample group will involve approximately 100 rate notices. Provide one imaged sample for each individual data file. The second (final) sample group will require approximately 500 to 700 rate notices, along with newsletter inserts and envelopes. The rate letter samples are to be printed, sorted, folded, inserted and sealed into the preproduction sample envelopes. The rate letter samples are to contain the proper newsletter sample, based upon the mailing address (domestic or foreign).

See "PREPRODUCTION QUALITY CONTROL SAMPLES" on page 18 for additional information.

Contractor MUST NOT proceed with printing until an "OK to Print" is received.

PRINTING:

Rate Letters (non-variable text): Print head to head. Follow the margins on the samples. No bleeds. There will be 20 (or 19) versions, each version has different copy. All versions print in black ink only.

Rate Letters (variable data personalized information): A process similar to an electronic overlay (Advanced Function Printing (AFP) overlay) should be used to print the non-variable text of the Rate Letters along with the variable data. Laser imaging is required. Other forms of imaging including ink jet, dot matrix, and line printing are NOT acceptable. All laser imaging must be done at a single location. Laser imaging must be in black. Each form has approximately 60 different elements of variable data.

Newsletters: Print head to head. Follow the margins on the samples. No bleeds. There are 2 versions, each version has different copy. Both versions print in black ink only.

Rate Letters Window Security Envelopes: Print on the inside and the outside in Pantone 287 Blue. **The outside must be offset printed.** For the outside, follow samples for margins, no bleeds. Either offset printing or flexographic printing is acceptable for the inside. The inside prints with a security pattern (agency logo security tint) consisting of a repeat pattern of broken lines, follow the sample for imposition. One Domestic version and one Air Mail version is required.

BINDING OPERATIONS:

Folding and Inserting: Fold Rate Letters and Newsletters and insert into contractor-produced envelopes specifically manufactured for those forms, with the applicable completed address block showing through the envelope's window. Recipient name, mailing address, encoded line, contractor's matching code, and postal barcode must show through the envelope's recipient window. A process similar to 2D bar coding should be used to ensure the finishing equipment inserts the correct notices into each envelope.

It is anticipated that these forms will be produced to fold in half and in half again so that they will be inserted with a closed end into the envelope. Contractor is required to determine the actual folding specifications for proper machine insertion.

Contractor must ensure that a properly imaged form is properly inserted into each envelope. Contractor must ensure that no blank forms are folded and inserted and that no envelopes are sealed empty. Rate Letters must be inserted so that the forms going to domestic destinations are inserted into domestic envelopes and those going to foreign destinations are inserted into the air mail envelopes.

Envelopes with Form RL-41 inserted will NOT also contain a Newsletter. For all other Rate Letter versions, newsletter Form RL-6 is to be additionally inserted one per envelope with domestic mail or newsletter Form RL-6F is to be inserted one per envelope with foreign mail.

Sealing: Envelopes must be securely sealed after forms are inserted. Contractor must use a method of sealing such that envelopes are securely sealed at the time of sealing. Methods that rely on the pressure of the other envelopes to seal the bond are not acceptable. Envelopes must be securely sealed when entered into the mail stream and must not open until opened by the recipient.

DISTRIBUTION:

Mailing must not commence until approval is given by the agency. The OK to commence mailing or to delay mailing will be given within 4 hours of the contractor's notification that they are ready to start mailing. Do not delay any operations awaiting this OK.

The rate letters are to be released and mailed all at once upon completion.

See "DISTRIBUTION" on page 21 for additional information.

Rate Letters Project Schedule:

1. GPO Form 2511 Print Order will be issued approximately mid-October. Agency will furnish the first Preproduction Quality Control Sample data file with the GPO Form 2511 Print Order. The first Preproduction Quality Control Sample data file will contain approximately 100 records.

2. Proofs must be delivered to the agency at the address indicated on the print order within eight (8) workdays of receipt the print order. Proofs must include all project elements and all versions – Rate Letters, Newsletters and Envelopes, and the output from the first Preproduction Quality Control Sample.

3. Reviewed proofs will be available for pickup by the contractor within three (3) workdays of receipt by the agency.

4. Revised proofs, if required, must be delivered within three (3) workdays of the reviewed proofs notification of availability for pickup by the contractor, and will be available for pickup by the contractor within three (3) workdays of their receipt by the agency.

5. The second (final) Preproduction Quality Control Sample data file will contain approximately 500 to 700 records. It is anticipated that the data file will be furnished to the contractor at the beginning of November. Samples must be delivered to the agency within eight (8) workdays of notification of availability of data files, and will be available for pickup by the contractor within three (3) workdays of their receipt by the agency.

6. Revised proofs, if required, must be delivered within three (3) workdays of the reviewed proofs being available for pickup by the contractor, and will be available for pickup by the contractor within three (3) workdays of their receipt by the agency.

7. The production file with live data will be available for pickup by the contractor approximately mid-December. Contractor will be allowed five (5) workdays for complete production, imaging, and mailing.

8. Contractor must not mail prior to receiving an "OK to Mail" at the imaging inspection, or at the Government's option, the contractor must securely transmit to the agency the first forms imaged for review and approval. A decision will be furnished within two (2) hours of receipt of the forms. Additionally, the agency may require that samples be provided at intermittent phases during the course of production.

NOTE: If a production phase is completed in a lesser time than required by the contract, the next production phase begins, such that overall production time is reduced. The maximum amount of time will not thus be allowable under the contract.

For example, if the contractor is allowed 10 workdays to provide proofs, the agency is allowed 5 workdays to review proofs, and the contractor is allowed 5 workdays to provide revised proofs. At the maximum schedule, if the print order is available for pickup September 6, 2020, proofs must be delivered by September 20, 2020 (10 workdays), and the agency must have the reviewed proofs available for pickup by the contractor by September 27, 2020 (5 workdays). The contractor must provide the revised proofs by October 4, 2020 (5 workdays).

If the print order is available for pickup September 6, 2020, and the proofs are delivered to the agency September 16, 2010 (2 workdays earlier than required), the agency must have the reviewed proofs available for pickup by the contractor by September 23, 2020 (5 workdays), not September 27, 2020. If the agency reviews the proofs within 3 workdays, by September 21, 2020, rather than the allowed 5 workdays, the contractor must provide the revised proofs by September 28, 2020 (5 workdays from when the proofs were available for pickup by the contractor).

TAX STATEMENTS PROJECT – Approximately 1 order per year.

The Tax Statement Project consists of two different forms (the Citizen and the NRA forms), and two different envelopes (the domestic and the airmail envelopes). Both the Citizen and NRA forms are printed and laser personalized.

QUANTITIES: Quantities indicated are estimated.

Item	Quantity (Domestic)	Quantity (Foreign)
Citizen Forms (Form RRB-1099/1099-R)	546,633	370
NRA Forms (Form RRB-1042S)	0	432
Domestic Envelopes	546,633	
Airmail Envelopes		802

TRIM SIZES:

Tax Statement Forms: 8-1/2 x 14" for Citizen; 8-1/2 x 11' for NRA. Must be clean edges or clean edge perforations, depending upon method of production.

Tax Statement Window Envelopes: Non-standard size of 3-7/8 x 9", open side, suitable seams, gummed flap, with one die-cut window. Window must be rectangular, with rounded corners, and a clear poly insert that meets USPS requirements for OCR readability.

Window for the Tax Statement Domestic envelope is 3-3/4" x 1-1/4" positioned 5/16" from the left and 1/2" from the bottom.

Window for the Tax Statement Air Mail envelope is 3-3/4" x 1-1/4" positioned 5/16" from the left and 1/2" from the bottom.

TYPESETTING, LAYOUT, AND PERSONALIZATION:

Tax Statements Forms (non-variable copy): It is anticipated that the Tax Statement Forms will have minor to moderate wording changes each year. At the Government's option, Tax Statement Forms may be fully redesigned in any given year. Agency-furnished electronic files must be reformatted by the contractor to meet supplied requirements. If provided, follow supplied samples for type size, style and layout. All columns of figures must align on the decimal point unless specifically indicated otherwise by the agency. Contractor will be required to set type and do the layout if camera copy is not furnished.

Each of the two Tax Statement versions has approximately 400 typelines including regular, italic and bold typefaces, plus rules and solids. After the initial typesetting of the face and back, it is anticipated that contractor will maintain the typeset file and only make required changes each year. Required changes are expected to include date changes to the face and back and other minor changes. Occasionally, boxes for data fields may be added or deleted. The Government reserves the right to make major changes or require complete redesign and re-typesetting of the forms each year.

Tax Statement Forms (variable data personalized information): Tax Statement Forms will be personalized with customer name, financial data, mailing address and/or other information. Each form has approximately 60 different elements of variable data. Contractor will be required to create electronic overlays (similar to an AFP overlay) for each of the two versions. Contractor will be required to provide any programming necessary to utilize furnished data files. Some data fields will be suppressed for certain individuals or for tax statement segments within the form. Suppressed fields will be coded.

If an entire Tax Statement segment is suppressed, contractor will be required to image **THIS FORM IS NOT REQUIRED FOR YOUR CURRENT YEAR TAXES** in the general area in which the variable tax information would appear, set in a large size, bold typeface. The furnished data files will NOT contain this typeline, which must be generated by the contractor. Contractor must image this information in the largest typeface that will fit and text must be easily readable.

For the Tax Statements, this matching code is comprised of the mail batch number and actual sequential number. For example, a matching code of "03 00011695" indicates that the tax statements is from the third mail/production batch (03) and is the 11,695th tax statement (00011695). If this matching code as described is revised, the contractor must provide the agency with information as to the type of code to be used and what it indicates. The Government reserves the right to be the final judge of the acceptability of the matching code including its locations.

Tax Statements Window Security Envelopes: It is anticipated that changes to the window envelopes will be minor. Both the Domestic and Airmail envelope versions will be typeset with approximately 11 lines of type, 1 logo and 1 ruled box, which represents the return address, important information statement, address service requested line and indicia. In addition, there will be an Airmail designation on the foreign envelope version. Window must be large enough to accommodate all required information such as the recipient's name, mailing address, city, state, zip code, province, country, contractor's matching code, barcode and any required endorsement line. No additional copy may appear through the window. The statement "IMPORTANT TAX RETURN DOCUMENT ENCLOSED" is to be printed to the right of the window in a location that does not interfere with USPS requirements for OCR readability. "Address Service Requested" line must be typeset in compliance with postal service requirements.

Contractor must create the security pattern for the inside of each envelope version. The security pattern consists of broken lines. The security pattern is the same for all versions.

See "TYPESETTING, LAYOUT AND PERSONALIZATION" on page 16 for additional information.

PROOFS:

See "PROOFS" on page 17 for additional details.

One to four sets of proofs may be ordered for each version of the Tax Statement Forms and Tax Statement Window Envelopes, as specified on the GPO Form 2511 Print Order or as directed by the agency. These proofs must contain all non-variable (but not the personalized) copy.

Tax Statement Mailers: Digital Content Proofs and/or PDF Proofs will be required.

Tax Statement Envelopes: Digital Content Proofs showing Pantone 287 Blue text will be required.

Proofs will be returned, or at Agency's option proofs will be held and approval or changes will be sent to contractor via email.

AUTHOR'S ALTERATIONS: Author's alterations (AA's) may occur during the proofing stage. At the Government's option, changes may be supplied by the Agency or requested from the contractor.

Tax Statement Mailers: Digital Content Proofs and/or PDF Proofs will be required.

Tax Statement Envelopes: Digital Content Proofs showing Pantone 287 Blue text will be required.

Proofs will be returned, or at Agency's option proofs will be held and approval or changes will be sent to contractor via email.

Contractor MUST NOT produce Preproduction Quality Control Samples until the "OK to Produce Preproduction Samples" is received.

PREPRODUCTION QUALITY CONTROL SAMPLES: It is anticipated that three different groups of samples will be required for the Tax Statements project. Different data files will be furnished for each group of samples. Two separate data files, one each for the Citizen and NRA forms, will be furnished. A record layout will be furnished for the first group. The data files for these groups may have place holders (such as alpha characters and numbers), actual data, or a combination. Characters such as "%" with a tax rate and "( )" enclosing negative numbers will also be used. Negative numbers must align on the decimal point with numbers in other fields.

(Note: RRB uses three data files: Citizen –Domestic/CASS, Citizen – Foreign address, and NRA)

However, based on the amount of time left in the schedule, at the Government's option, the third stage samples might not be requested.

At the Government's option, separate data files may be furnished for the Preproduction Quality Control Samples or contractor may be required to produce those from the final production data files.

If preproduction samples are to be imaged from the final data, contractor will be instructed as to which files are to be used, e.g., the first 100 names from each file. Contractor must ensure that these names are not deleted from the final production run and that the all intended recipients will receive a Tax Statement.

Contractor must furnish the full quantity of samples ordered. It is anticipated that contractor will be required to furnish from 50 to 200 sets *of each* of the two different Tax Statement forms and envelopes at each stage. These items are NOT included in the quantity ordered and must be furnished and delivered at no additional cost to the Government.

See "PREPRODUCTION QUALITY CONTROL SAMPLES" on page 18 for additional information.

Contractor must not proceed with printing until an "OK to Image (Print)" is received.

ADDITIONAL SAMPLE COPIES OF THE TAX STATEMENTS AND ENVELOPES: After the "OK to Image (Print)" of the printed portion of the tax statement forms and envelopes (usually after the first set of Preproduction Quality Control Samples), contractor must provide agency with 600 printed but unimaged (not personalized) copies of each of the Citizen and the NRA statements and 100 copies each of the domestic and air mail envelopes. These must be delivered within **5 workdays** of this OK to the address noted in "DISTRIBUTION". These copies are NOT included in the quantity ordered and must be furnished and delivered at no additional cost to the Government.

PRINTING, INK AND MARGINS:

Tax Statements (non-variable text): Print head to head. Follow the margins on the samples. No bleeds. There will be two (2) versions, each version has different copy. Both forms print in two colors on the face and a single color on the back. The back color will be one of the face colors. Colors may change during the term of the contract.

Citizen Form (RRB-1099/1099-R) prints in Pantone 287 Blue and Pantone 348 Green on the face, and Pantone 287 Blue on the back. NOTE: This form is anticipated to be 1 leaf.

NRA Form (RRB-1042S/1099-R) prints in Pantone Black and Pantone 348 Green on the face, and Pantone Black on the back. NOTE: This form is anticipated to be 2-3 leaves.

At the contractor's option, the non-variable portion of the face and the back of the Tax Statements may be digitally imaged in lieu of printing. However, contractor must meet the same QATAP standards as for printed forms and the required Pantone colors must be matched. Additionally, both forms contain several large solids with fine knock-out type on the face.

Tax Statements (variable data personalized information): A process similar to an electronic overlay (Advanced Function Printing (AFP) overlay) should be used to print the non-variable text of the Tax Statements along with the variable data. Laser imaging is required. Other forms of imaging including ink jet, dot matrix, and line printing are NOT acceptable. All laser imaging must be done at a single location. Laser imaging must be in black.

Tax Statements Window Security Envelopes: Print on the inside and the outside in Pantone 287 Blue. The outside must be offset printed. For the outside, follow samples for margins, no bleeds. Either offset printing or flexographic printing is acceptable for the inside. The inside prints with a security pattern (agency logo security tint) consisting of a repeat pattern of broken lines, follow the sample for imposition. One Domestic version and one Air Mail version is required.

The statement "IMPORTANT TAX INFORMATION ENCLOSED" is to be printed in bold type to the right of the window for both envelope versions. The phrase is to be printed in the middle of the blank area to the right of the envelope window and under the permit imprint box. The preprinted phrase may change during the term of the contract. Placement shall not interfere with USPS requirements for readability.

Both envelope versions must have one window. Window must be large enough to accommodate all required information such as the recipient's name, mailing address, city, state, zip code, province; country; contractor's matching code; barcode; and any required (not optional) endorsement line. No additional information may appear through the window.

BINDING OPERATIONS:

Perforating:

Citizen Form: Full horizontal printed perforations are required after the second and third Tax Statement segments. These are located approximately 7" and 10-1/2" from the top of the forms. Folds will be on these perforations. Exact placement of the perforations may require adjustment based on copy, variable imaging, and folding requirements. Note that although the form is also folded after the first Tax Statement segment, that area is not perforated.

NRA Form: Full horizontal printed perforations are required after the second and third Tax Statement segments. These are located approximately 3-5/8" and 7-1/4" from the top of the forms. Folds will be on these perforations. Exact placement of the perforations may require adjustment based on copy, variable imaging, and folding requirements. Note that although the form is also folded after the first Tax Statement segment, that area is not perforated.

Gather and Match: Anticipated to apply to NRA Form only. Gather and match 2-3 leaves, may require non-automated processing, at contractor's option.

Folding and Inserting: Fold Tax Statements and insert into contractor-produced envelopes specifically manufactured for those forms, with the applicable completed address block showing through the envelope's window. Recipient name, mailing address, encoded line, contractor's matching code, and postal barcode must show through the envelope's recipient window. Tax statement forms must NOT have any folds within any of the individual statement segments. Contractor must ensure that folds are between the tax statement segments and on the printed perforations where the form is perforated. There are 4 tax statement segments on the face of each form, each approximately 3-1/2" in depth. It is the contractor's responsibility to determine the actual folding specifications for proper machine insertion.

Hand Inserting: Anticipated to apply to the NRA Form only. May require hand insertion, at contractor's option.

Contractor must ensure that a properly imaged form is properly inserted into each envelope. Contractor must ensure that no blank forms are folded and inserted, and that no envelopes are sealed empty. Tax Statements must be inserted so that the forms going to domestic destinations are inserted into domestic envelopes and those going to foreign destinations are inserted into the air mail envelopes.

Sealing: Envelopes must be securely sealed after forms are inserted. Contractor must use a method of sealing such that envelopes are securely sealed at the time of sealing. Methods that rely on the pressure of the other envelopes to seal the bond are not acceptable. Envelopes must be securely sealed when entered into the mail stream and must not open until opened by the recipient.

See "BINDING OPERATIONS" on page 19 for additional information.

INSPECTIONS OF LASER PERSONALIZATION AND MAILING OPERATIONS:

See "INSPECTIONS OF LASER PERSONALIZATION AND MAILING OPERATIONS" on page 6 for additional information.

Prior to a laser image personalization inspections of the tax statement forms, the Government will provide a list of 30 to 50 claim numbers from throughout the nonresident alien (NRA) live production file. The numbers will come from the front, middle and end of each file. The list of claim numbers will be provided at the same time as the production files are sent to the contractor and no later than 24 hours prior to the date of inspection.

The contractor will be required to provide the NRA and Citizen Statements with these claim numbers to the RRB representative at the inspection, or at the Government's option, overnight or fax these to the RRB at the contractor's expense. It will be at the Government option to determine if these tax statements should be inserted and sealed in the appropriate envelopes. The RRB will inspect these statements from actual production to confirm that the variable information imaged on the tax statements are correct. THE CONTRACTOR MUST REGENERATE THESE STATEMENTS SO THAT ALL RECIPIENTS WILL RECEIVE THEIR TAX STATEMENTS.

Laser personalization and mailing operation inspections must be structured so that the Government representatives can spend the minimum amount of time at the inspection. The laser personalization of both tax statement forms must be held the same workday. Usually, this is done by personalizing the smaller NRA quantity first and then starting the Citizen forms. However, at the contractor's option, they can personalize a portion of each.

DISTRIBUTION:

Mailing of the Tax Statements must not commence until "OK to Mail" approval is given by the agency.

The tax statements must be mailed in batches on a daily basis.

See "DISTRIBUTION" on page 21 for additional information.

SCHEDULE:

See "SCHEDULE" on page 22 for additional information.

It is anticipated that the Tax Statements print order will be placed in October of each year with all shipping/mailing/delivery completed in January of the following year.

Contractor is bound by the mailing date on the GPO Form 2511 Print Order. Additional proofs or Preproduction Quality Control Samples required due to additional proof stages, author's alterations, or printer's errors, or any other delays, problems, or contract requirements will NOT be a cause for delay in the schedule. All mailing must be completed by the scheduled date.

Agency and contractor are required to send all proofs and Preproduction Quality Control Samples via overnight delivery the day before the due date. For example, the proofs or samples should be sent via overnight delivery on Monday if the proofs or samples are due the next workday on Tuesday.

Tax Statements Project Schedule:

Typesetting, Design, and Proofs

1. Proofs must be received by the agency within ten (10) workdays of agency notification of material availability for contractor pickup.

2. Proofs will be held a maximum of five (5) workdays from date of receipt by the agency.

3. Additional proofs required due to author's alterations, printer's errors, or for any other reason, must be received by the agency within five (5) workdays of agency notification of material availability for contractor pickup.

4. Additional proofs will be held a maximum of three (3) workdays from receipt by the agency.

1st Stage Preproduction Quality Control Samples

1. 1st stage preproduction samples must be received by the Government within eight (8) workdays of when the "OK to Produce 1st Stage Preproduction Samples" is given to the contractor.

2. Reviewed 1st stage preproduction samples will be available for pickup by the contractor within five (5) workdays from receipt by the agency.

3. Corrected 1st stage preproduction samples, if required, must be received by the agency within three (3) workdays from when the reviewed 1st stage preproduction samples are available for pickup by the contractor. At the Government's option, corrections may be allowed to be made on the 2nd stage preproduction samples.

4. Reviewed corrected 1st stage preproduction samples will be available for pickup by the contractor within three (3) workdays from receipt by the Government.

2nd Stage Preproduction Quality Control Samples

1. 2nd stage preproduction samples must be received by the Government within five (5) workdays of when the "OK to Produce 2nd Stage Preproduction Samples" is given to the contractor.

2. Reviewed 2nd stage preproduction samples will be available for pickup by the contractor within five (5) workdays from receipt by the agency.

3. Corrected 2nd stage preproduction samples, if required, must be received by the agency within three (3) workdays from when the reviewed 2nd stage preproduction samples are available for pickup by the contractor.

4. Reviewed corrected 2nd stage preproduction samples will be available for pickup by the contractor within three (3) workdays from receipt by the agency.

The "OK to Print the Tax Statements" and the "OK to Print the Envelopes" will be given sometime between the OK of the 2nd preproduction sample and two weeks prior to the start of the final stage of imaging and mailing.

It is the agency's intention to give approval to print as soon as the printed material is acceptable ***and*** the agency is able to determine a close estimate as to the quantities that will be required. Approval to print may be given at different times for different items (domestic envelopes, NRA envelopes, Citizen forms and NRA forms). However, the Government will not guarantee that the approval to print will be prior to two weeks before the final stage. Note, however, the Government will not be responsible for approval to print being given after that time if delayed due to printer's errors. It is not anticipated that any approval to print will be given until at least the approval of the first set of preproduction samples. Contractor may check at various times during the schedule with the RRB to see if quantities have been determined and the "approval to print" can be issued.

3rd Stage Preproduction Quality Control Samples

In this stage of production, schedule is based on calendar days NOT work days. **All calendar days including Saturdays, Sundays, and Federal Holidays (except Christmas and New Year's Day) are counted in the schedule.**

1. Contractor will be notified at least ten (10) calendar days prior to the date the live production data files and Preproduction Quality Control Sample data files (if separate files) will be available for pickup. The agency will inform the contractor if a Third Stage sample will be necessary. If the agency decides to run a Third Stage sample, the required date for the production of the Third Stage samples will be included at this time. The agency may have previously furnished a schedule with

these dates. If so, that schedule will serve as notification unless the dates have been changed.

2. Contractor will be required to pickup the live production data files Third Stage sample data files (if separate) on the date the agency specified they will be available for pickup.

3. At the Government's option, Third Stage samples may be sent to and reviewed at the RRB or may be reviewed at the contractor's plant.

   - Review at RRB: QC preproduction samples must be delivered to the RRB **within three (3) calendar days** from when the data files were available for pickup. Approval/disapproval will be furnished within **one (1) calendar day.**

   - Review at Contractor's Plant: QC preproduction samples must be available for review **within two (2) calendar days** from when the data files were available for pickup. Approval/disapproval will be furnished within **one (1) calendar day.**

   - If the Third Stage sample was sent to the agency, corrected samples, if required, must be received by the agency within **one (1) calendar day** from when the reviewed samples are available for pickup by the contractor.

   - If the Third Stage sample is being reviewed by the agency at the contractor's plant, corrected samples, if required, must be received by the agency on the **same calendar day** as the disapproval by the agency.

4. Contractor may process the live production data files while the Third Stage samples are being produced and reviewed. However, contractor may NOT start any actual imaging until the OK is given by the agency.

Inspection Samples from Production

At the Government's option, agency representative(s) may be sent to the contractor's plant(s) for review of inspection samples and operations, or contractor may be required to have the inspection samples delivered via overnight delivery or faxed to the RRB for review.

1. Review at RRB: Inspection samples must be delivered **within one (1) workday** from when the data files were available for pickup. Approval/disapproval will be furnished within **one (1) calendar day.**

   Corrected inspection production samples, if required, must be available on the **same day**, or sent overnight delivery for the next **calendar day**.

   The "OK to Image (Print)" the production file will be given upon approval of the inspection production sample by the agency.

2. Review at Contractor's Plant: The agency representative(s) will conduct an **onsite inspection** at the contractor's plant **one (1) workday** after the data files were available for pickup. Approval/disapproval will be furnished the **same day.**

   Corrected inspection production samples, if required, must be available on the **same day**.

The "OK to Image (Print)" the production file will be given upon approval of the inspection production sample by the agency.

Imaging, Inserting, and Related Operations

1. Laser imaging personalization, cutting, folding, inserting, envelope sealing, sorting for mailing, and related operations must start by the calendar day following the "OK to Image (Print)" approval of the inspection production sample.

2. Mailing of the Tax Statements must not commence until "OK to Mail" approval is given by the agency. An "OK to Mail" or "Hold" will be issued within 4 hours of the contractor's notification that they are ready to start mailing. Do NOT delay any other operations awaiting this OK.

3. All postal mailing receipts, status reports and QC review sheets should be sent to the Agency on a daily basis.

4. Final production, imaging, folding, inserting, sealing and mailing must be completed **within ten (10) calendar days** from when the live production files were transmitted. Other items that must be completed include: returning Tax Statements with invalid mailing addresses to the agency, sending the required mailing receipts, status reports and QC sheets to the agency and/or GPO, and the regeneration and mailing of any forms due to spoilage.

BA-6 PROJECT – Approximately 1 order per year.

The BA-6 project consists of a single sheet form laser imaged with personalized data. There is one version of the BA-6 Form and two versions of the BA-6 envelope.

QUANTITIES: Quantities indicated are estimated.

Item	Quantity (Domestic)	Quantity (Foreign)
Printed and laser imaged BA-6 Form	258,000	100
BA-6 Domestic Envelopes	258,000	
BA-6 Airmail Envelopes		100

TRIM SIZES:

BA-6 Forms: 8-1/2 x 14". Must be clean edges or clean edge perforations, depending upon method of production.

(Note: RRB may re-size the BA-6 Form to 8-1/2 x 11" during the course of the contract).

BA-6 Envelopes: Non-standard size with window, 3-7/8 x 9", open side, suitable seams, gummed flap, with one die-cut window. Window must be rectangular, with rounded corners, and a clear poly insert that meets USPS requirements for readability.

Window for the BA-6 Domestic and BA-6 Air Mail envelopes is 3-7/8" x 1-3/8", positioned 1/2" from the left and 7/8" from the bottom.

TYPESETTING, LAYOUT, AND PERSONALIZATION:

BA-6 Form (non-variable copy): It is anticipated that the contractor will be required to typeset approximately 60-115 typelines plus rules for the BA-6 Form, following the layout furnished with the order. It is anticipated that the balance of the form content (approximately 88-100 typelines) will be furnished in an electronic file (anticipated to be Acrobat PDF). It is anticipated that the BA-6 Form will have minor to moderate wording changes each year. At the Government's option, the BA-6 Form may be fully redesigned in any given year. Agency-furnished electronic files must be reformatted by the contractor to meet supplied requirements. If provided, follow supplied samples for type size, style and layout. All columns of figures must align on the decimal point unless specifically indicated otherwise by the agency.

BA-6 Form (variable data personalized information): The BA-6 Form will be personalized with customer name, financial data, mailing address and/or other information. Each form has approximately 60-92 different elements of variable data. Contractor will be required to create electronic overlays (similar to an AFP overlay) for each of the two versions. Agency will provide a data layout with all fields numbered that coincides with a sample variable data filled form. Contractor will be required to provide any programming necessary to utilize furnished data files.

Some data fields will be suppressed for certain individuals or for some segments within the form. Suppressed fields will be coded. If an entire segment is suppressed, contractor may be required to image dashes in the field. The furnished data files may not contain these dashes.

This matching code is comprised of the mail batch number and actual sequential number. For example, a matching code of "03 00011695" indicates that the form is from the third mail/production batch (03) and is the 11,695th form (00011695). If this matching code as described is revised, the contractor must provide the agency with information as to the type of code to be used and what it indicates. The Government reserves the right to be the final judge of the acceptability of the matching code including its locations.

BA-6 Security Window Envelopes: It is anticipated that changes to the envelopes each year will be minor.

The Domestic envelope will be typeset with approximately 11-15 lines of type, 1 logo and 1 ruled box, which represents the return address, important information statement (2 lines), address service requested line and indicia.

The Airmail (foreign) envelope will be typeset with approximately 11-18 lines of type, 1 logo and 1 ruled box, which represents the return address, important information statement (2 lines), address service requested line and indicia, plus Airmail and International designations.

The "IMPORTANT INFORMATION" statement is to be printed to the right of the window for both versions in a location that does not interfere with USPS requirements for readability. "Address Service Requested" line must be typeset in compliance with postal service requirements.

Window must be large enough to accommodate all required information such as the recipient's name, mailing address, city, state, zip code, province, country, contractor's matching code, barcode and any required endorsement line. No additional copy may appear through the window.

Contractor must create the security pattern for the inside of each version. The security pattern consists of broken lines. The security pattern is the same for all versions.

See "TYPESETTING, LAYOUT AND PERSONALIZATION" on page 16 for additional information.

PROOFS:

One to four sets of proofs may be ordered for the BA-6 Form and each version of BA-6 Envelopes as specified on the GPO Form 2511 Print Order or as directed by the agency. These proofs must contain all non-variable (but not the personalized) copy.

Digital Content Proofs and/or PDF Proofs will be ordered. Proofs will be returned, or at Agency's option proofs will be held and approval or changes will be sent to contractor via email.

AUTHOR'S ALTERATIONS: Author's alterations (AA's) may occur during the proofing stage. At the Government's option, changes may be supplied by the Agency or requested from the contractor.

Author's Alterations (AA's) proofs shall be PDF proofs, provided via e-mail to one or more email addresses as provided by the Agency.

At the Government's option, Digital Content Proofs may also, or alternatively, be requested as AA's proofs.

Proofs will be returned, or at Agency's option proofs will be held and approval or changes will be sent to contractor via email.

See "PROOFS" on page 17 for additional information.

Contractor MUST NOT produce Preproduction Quality Control Samples until the "OK to Produce Preproduction Samples" is received.

PREPRODUCTION QUALITY CONTROL SAMPLES: Different data files will be furnished for each set of preproduction samples. A record layout will be furnished for the first group. The data files for these groups may have place holders (such as alpha characters and numbers), actual data, or a combination. Characters such as "%" with a tax rate and "( )" enclosing negative numbers may also be used. Negative numbers must align on the decimal point with numbers in other fields.

At the Government's option, separate data files may be furnished for the Preproduction Quality Control Samples or contractor may be required to produce those from the final production data files.

If preproduction samples are to be imaged from the final data, contractor will be instructed as to which files are to be used, e.g., the first 100 names from each file. Contractor must ensure that these names are not deleted from the final production run and that the all intended recipients will receive a BA-6 mailing.

Contractor must furnish the full quantity of samples ordered. It is anticipated that contractor will be required to furnish 100 Preproduction Quality Control Sample sets of BA-6 Forms. The BA-6 forms must be printed and laser imaged, sorted, folded and inserted into the sample envelopes. These items are NOT included in the quantity ordered and must be furnished and delivered at no additional cost to the Government.

See "PREPRODUCTION QUALITY CONTROL SAMPLES" on page 18 for additional information.

Contractor must not proceed with printing until an "OK to Image (Print)" is received.

PRINTING, INK AND MARGINS:

BA-6 Forms (non-variable text): Print head to head. Print face and back a single ink color of Pantone 287 Blue. Color may change during the term of the contract. Follow the margins on the samples. No bleeds. Layout may contain large solids with fine knock-out type. BA-6 forms must be addressed in one location that will show through the envelope's window.

At the contractor's option, the non-variable portion of the forms may be digitally imaged in lieu of printing. However, contractor must meet the same QATAP standards as for printed forms and the required Pantone color must be matched. Personalized data must align with the applicable printed data.

BA-6 Forms (variable data personalized information): A process similar to an electronic overlay (Advanced Function Printing (AFP) overlay) should be used to print the non-variable text along with the variable data. A letter must be produced for each data file. 100% of the records must be properly imaged. Laser imaging is required. Laser imaging must match Pantone 287 Blue or the current single ink as ordered by the agency. Other forms of imaging including ink jet, dot matrix, and line printing are NOT acceptable. The imaged area of the BA-6 form should match the rest of the form as close as possible unless indicated otherwise by the Government. Samples will be furnished to the awarded contractor as a guide.

BA-6 Security Window Envelopes: Print on the inside and the outside in Pantone 287 Blue. The outside must be offset printed. Either offset printing or flexographic printing is acceptable for the inside. The inside prints with a security pattern (agency logo security tint) consisting of a repeat pattern of broken lines, follow the sample for imposition.

One Domestic version and one Air Mail version is required. Both envelope versions have one window. Window must accommodate all required information such as the recipient's name, mailing address, city, state, zip code, province; country; contractor's matching code; barcode; and any required (not optional) endorsement line. No additional information may appear through the window.

BINDING OPERATIONS:

Folding and Inserting: Parallel fold each BA-6 Form in half twice, with the address block visible. It is anticipated that these forms will be produced to fold in half and in half again so that they will be inserted with a closed end into the envelope.

Insert each folded form into a contractor-produced custom envelope, with the address block showing through the envelope's window. Recipient name, mailing address, encoded line, contractor's matching code, and postal barcode must show through the envelope's recipient window. It is the contractor's responsibility to determine the actual folding specifications for proper machine insertion.

Contractor must ensure that a properly imaged form is properly inserted into each envelope. Contractor must ensure that no blank forms are folded and inserted, and that no envelopes are sealed empty. BA-6 Forms must be inserted so that the forms going to domestic destinations are inserted into domestic envelopes and those going to foreign destinations are inserted into the air mail envelopes.

Sealing: Envelopes must be securely sealed after forms are inserted. Contractor must use a method of sealing such that envelopes are securely sealed at the time of sealing. Methods that rely on the pressure of the other envelopes to seal the bond are not acceptable. Envelopes must be securely sealed when entered into the mail stream and must not open until opened by the recipient.

SORTING, ADDRESSING, AND MAILING IN ACCORDANCE WITH POSTAL SERVICE (USPS) REGULATIONS:

All mailed forms must meet all USPS requirements, and industry standard best practices for optimal readability and usability. Return address block on envelopes must be typeset in compliance with all postal service requirements. Recipient address block on letter must meet all USPS requirements including those for typography, print quality, reflectance, barcode location, clear zones, tap test, etc. Contractor is responsible for reviewing all factors which could affect mail acceptance.

NCOA processing is required: The agency will supply input and output lists. Contractor will be required to copy these lists and NCOA process to obtain the change of address. Do not alter the original files. The level of processing will be specified by the Government at the time the list is supplied. At the minimum, these must be processed for an individual move. It is anticipated that the lists will also be required to be processed for a family move. After processing, the contractor must provide a listing of all the addresses changed with their NIXI codes and number of hits matched. These must be cross referenced by the contractor with other references that are on the files, such as an agency code. Additionally, an output tape must be supplied of all the updated addresses. These may need to also be cross referenced by the contractor with the original addresses.

The address files requiring NCOA processing will be furnished prior to any material furnished for the printing or other personalization. However, at the agency's option, a smaller, sample test file may be furnished for processing and contractor would be required to provide a sample NCOA processed reply file. The sample test file would be used to determine the level of processing required and to verify contractor understanding of all the agency requirements.

See "SORTING, MAILING AND DISTRIBUTING IN ACCORDANCE WITH POSTAL SERVICE (USPS) REGULATIONS:" on page 19 for additional information.

DISTRIBUTION:

Mailing of the BA-6 Forms must not commence until "OK to Mail" approval is given by the agency.

At the contractor's option, the BA-6 forms may either be mailed on a daily basis or upon completion.

See "DISTRIBUTION" on page 21 for additional information.

SCHEDULE:

It is anticipated that the BA-6 print order will be placed in February or March of each year with all shipping/mailing/delivery completed in June.

Contractor is bound by the mailing date on the GPO Form 2511 Print Order. Additional proofs or preproduction samples required due to additional proof stages, author's alterations, or printer's errors, or any other delays, problems, or contract requirements will NOT be a cause for delay in the schedule. All mailing must be completed by the scheduled date.

Agency and contractor are required to send all proofs and preproduction samples via overnight delivery the day before the due date. For example, the proofs or samples should be sent via overnight delivery on Monday if the proofs or samples are due the next workday on Tuesday.

BA-6 Project Schedule:

Note: The schedule for BA-6 forms is entirely in workdays – not calendar days.

NCOA Processing

1. Agency will notify contractor of the availability of the GPO Form 2511 Print Order and the data files for NCOA processing. NCOA processing must be completed and all revised files and reports delivered within ten (10) workdays. If a sample test file is furnished for NCOA processing, the reply file must be completed and delivered within five (5) workdays.

Typesetting, Design, and Proofs

1. There may be a time gap between the completion and approval of the NCOA Processing phase of production and the beginning of production of the BA-6 Forms and Envelopes. No specific time frame can be furnished from the NCOA processing until the start of the proof cycle. It is anticipated that the proof cycle will start in March, April, May or June.

2. Agency will notify contractor of the availability of materials and instructions for production of the BA-6 Forms and Envelopes Proofs. Once notification is made, proofs must be received by the agency within eight (8) workdays.

3. Agency will hold proofs a maximum of five (5) workdays from date of receipt.

4. Revised proofs, if required, must be delivered within five (5) workdays of the reviewed proofs being available for pickup by the contractor.

5. Agency will hold revised proofs a maximum of five (5) workdays from date of receipt.

Preproduction Quality Control Samples

1. Preproduction Quality Control Samples must be received by the Government within seven (7) workdays of when the "OK to Produce Preproduction Samples" is given to the contractor.

2. Agency will review Preproduction Quality Control Samples within five (5) workdays from date of receipt.

Contractor must not proceed with printing until an "OK to Print" is received.

Live Data and Completion of Production

1. Within ten (10) workdays of approval of the Preproduction Quality Control Samples, agency will notify contractor of the availability of live data for production of the BA-6 Forms and Envelopes.

2. Contractor must not mail until they receive an "OK to Mail" at the imaging inspection, or at the Government's option, the contractor must fax or transmit by the requested means to the Agency the first forms imaged for the Agency to check and "OK." A decision will be furnished within 2 hours of receipt of the forms. Additionally, the RRB may require that samples be sent to them at intermittent phases during the production time.

3. Contractor must complete production, imaging, and mailing within ten (10) workdays, or by the ship/delivery date on the 2511 Print Order.

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 requirements 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) 8
(b) 30

II. (a) 5
(b) 24
(c) 35

III. (a) 1
(b) 33

IV. (a) 10

		(1)	(2)
V.	(a)	6	1,341
	(b)	20	535
	(c)	2	525
	(d)	1	547
	(e)	1	1
	(f)	2	258

		(1)	(2)
VI.	(a)	24	1,340
	(b)	650	
	(c)	1	
	(d)	1	

SECTION 4.- SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city for mailed shipments and f.o.b. destination to Chicago, IL.

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.

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.

The contractor is cautioned not to perform any operation(s) or produce any product(s) for which a price has not been offered under the contract. Further, the contractor is not to accept print orders which are outside the scope of the contract. Any changes made to the print order MUST be confirmed in writing by the Contracting Officer, Chicago GPO. If such orders are placed by the agency, and no Modification is received from the Chicago GPO, the contractor is to notify GPO Chicago immediately. Failure to do so may result in nonpayment.

CONTRACTOR MUST INVOICE IN ACCORDANCE WITH SCHEDULE OF PRICES. FAILURE TO ITEMIZE IN ACCORDANCE WITH THE SCHEDULE OF PRICES MAY RESULT IN DELAYED PAYMENT.

All billing 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. DESIGN, LAYOUT, AND COMPOSITION: Only one per side charge per order will be allowed for the inside security pattern since the same pattern is used for all envelopes.

(a) Envelope, per envelope version ……..... per side (inside or outside) …… $_____

(b) Forms (each version) ……. per side ……..…… $_____

_____
(Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

II. PROOFS:

(a) Digital Content Proof – Envelopes……per side, per version…….$_____

(b) Digital Content Proof – Forms……..per side, per version……..…$_____

(c) PDF Proofs……..…….per side, per version……..$_____

III. AUTHOR'S ALTERATIONS: Author's alterations charges will be allowed only for changes at variance with the original copy. No charges will be allowed for printer's errors. All author's alteration charges must be supported by documentation submitted with the contractor's invoice voucher.

(a) Author's alterations, envelopes…….....per side……..…$_____

(b) Author's alterations, forms……per side……..$_____

IV. PREPRODUCTION QUALITY CONTROL SAMPLES:

(a) Preproduction Quality Control Samples……per 100 sets……$_____

V. PRINTING: Contractor will be allowed a separate "Makeready and/or Setup" charge for each form version. Printing face only or face and back must be included in one charge as applicable. For each window envelope version, all inside and outside printing must be included in one charge. Only one "Makeready and/or Setup" charge will be allowed per version regardless of the quantity run.

	MAKEREADY AND/OR SETUP (1)	RUNNING PER 1,000 COPIES (2)
(a) Window Envelope ……..... per version ..…….....	$_____	$_____
(b) Rate Letters …….... per version …..……..	$_____	$_____
(c) Rate Letter Newsletters …. per version ……...	$_____	$_____
(d) Tax Statement Forms …..... per leaf ……..... (Citizen, 8-1/2 x 14")	$_____	$_____
(e) Tax Statement Forms …..... per leaf ……..... (NRA, 8/12 x 11")	$_____	$_____
(f) BA-6 Forms ……...…….…….…….	$_____	$_____

_____
(Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

VI. LASER IMAGING PERSONALIZATION, NCOA PROCESSING, INSERTING AND MAILING: Contractor will be allowed a separate "Makeready and/or Setup" charge for imaging each of the different versions of forms. Only one "Makeready and/or Setup" charge will be allowed per form version regardless of the quantity imaged. No extra charges allowed for inserting and mailing in different types of envelopes to domestic and foreign destinations. All costs for computer programming, data processing, cutting (if required), folding, sacking, bagging, traying, completion of all required forms, delivery to the Post Office, and all related operations from imaging to the final mailing must also be included in the costs except that a separate charge is allowed for CASS/NCOA processing of BA-6 forms.

	MAKEREADY AND/OR SETUP (1)	RUNNING PER 1,000 COPIES (2)
(a) Imaging/Inserting/Mailing……..……...…..	$_____	$_____
(b) CASS/NCOA Processing for BA-6 Forms only…..…per 1,000 addresses…..$_____		
Tax Statement (NRA Form) - Non-automated:		
(c) Gather and match 2-3 leaves…….per 1,000 leaves…….....$_____		
(d) Hand insert into envelopes……...per 1,000 sets……...$_____		

_____
(Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

LOCATION OF POST OFFICE: All mailing will be made from the _____

Post Office located at Street Address_____,

City_____, State_____, Zip Code_____

Phone_____, Contact Person_____, Fax_____.

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent, _____calendar days. See Article 12 "Discounts" of Solicitation 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 points(s), in exact accordance with specifications.

NOTE: Failure to provide a 60-day bid acceptance period may result in expiration of bid prior to award.

CONTRACTOR'S NAME AND SIGNATURE: Fill out and return one copy of all pages in "Section 4. - Schedule of Prices," initial or sign each in the space provided. Additionally, see Page 1.

Contractor _____

_____
(Street Address) (City – State – Zip)

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

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

_____
(Email Address) (Contractor's Code No.)

THIS SECTION FOR GPO USE ONLY

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____

be Contacted) (Telephone Number)

_____
(Email Address) (Contractor's Code No.)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

5515-S ATTACHMENT A

[SAMPLE]
Enterprise Information Security and Privacy Policy

Table of Contents

- **Introduction**

This document is designed and implemented to provide the specific instructions and references for behaviors of employees with regard to the appropriate handling and processing of "Contractor" information assets and information resources. The use of information assets and information resources is in most cases an integral component of every job function at "Contractor", therefore requiring controlled business processes to ensure that the confidentiality, integrity, availability, and accountability of "Contractor" data is maintained throughout its lifecycle.

This Policy applies, and provides the minimum baseline standards, to all "Contractor" information technology ("IT") resources and information/data assets. This Policy also provides the minimum baseline standards for "Contractor" Units for the development of their respective Agreed Upon Procedures and Standard Operating Procedures documents for management of their customer data, and network IT resources and information/data assets.

- **General Information Security Principles**

A key input for the "Contractor" information security program is a set of accepted Information Security Principles. The information Security Principles are a statement of fundamental value, a rule, or belief, which are pervasive and contribute to the organizations entity-level control environment. An Information Security Principle provides enterprise-wide guidance and must be universally applied and enforced. The broadest of constituents must understand them and they must have applicability to that broad base. The Information Security Principles define the philosophy of the organization that in turn influences the definition of the security policies. The main purpose of the Information Security Principles is to inform Executives of the potential IT security risks, document the corporate commitment to managing risks, and measure the security programs effectiveness. The Information Security Principles provide the security decision anchor for subsequent security strategies, architectures, policies and processes. The following are "Contractor" Information Security Principles.

1. *Individual accountability and responsibility for information security shall be clearly and consistently defined, communicated, and acknowledged.*
2. *The organization will treat information as a critical resource and ensure that completeness and accuracy of information is maintained and known at all times.*

3. *The privacy and confidentiality of information in all forms, whether created by "Contractor" or entrusted to us by our customers, partners, or suppliers, will be safeguarded and comply with applicable laws and regulations.*
4. *Information has value and shall be used and administered in an ethical way.*
5. *Information security controls shall be proportionate to the risks of modification, denial of use, or disclosure of the information.*
6. *All parties, including but not limited to information owners and information security practitioners, with a need to know should have access to available principles, standards, convention, or mechanisms and training for the security of information and information systems, and shall be informed of applicable threats to the security of information.*

- **Risk Assessment and Scope of This Policy**

Risk management is the process of minimizing the impact of information asset loss. Understanding the risk of assets loss, the vulnerabilities associated with managing the asset, and the cost of safeguards allows management to make informed decisions about security recommendations for implementing appropriate and cost-effective safeguards. The process defines the value of the asset, derived from its confidentiality, integrity and availability. It then assesses the risk to that asset based on a series of threats, each with a likelihood of occurrence, and vulnerability within the asset that triggers the impact. The following conceptual equations illustrate the calculation of risk.

Risk = Value x Threat & Likelihood x Vulnerability

Residual Risk = Risk – Mitigation Strategy Effectiveness

The risk management process balances risks with controls. This process reinforces the awareness of the risks and provides an understanding of controls to limit residual risks to an acceptable level.

Risk assessments are performed to enable "Contractor" to continue to perform to the level of customer expectations and within the contractual requirements established by Service Level Agreements.

- ***The Process***

The risk assessment process includes four steps:

1. ***Scope*** – What is going to be protected as determined by the Data Classification Policy;
2. ***Threat Assessment*** - What to protect against and documenting the consequences of a threat;
3. ***Risk Assessment*** - Determining whether existing safeguards are satisfactory and, where appropriate, implementing additional controls; and
4. ***Evaluation*** – Periodic monitoring to ensure safeguards are in place, effective in minimizing known risks and, existing classifications for data, applications, systems and servers are appropriate.

- **Compliance**

The IT Administrators and other operational management personnel will implement this policy to ensure that the spirit of the policy, to appropriately manage user access privileges to the information systems and processing facilities, is followed. Information Systems Security Office ("ISSO") will enforce this policy through regular audits in coordination with Human Resources and the Information Security Assurance & Compliance ("iSAC") office to ensure ongoing compliance. Failure to comply with this policy may result in reduction of access privileges, and/or termination of employment.

"Contractor" has aligned its Information Security Program with the ISO/IEC 27002:2005 Code of Practice for Information Security Management. In addition, "Contractor" has adopted the Information Systems Audit and Control Association's (ISACA®) Control Objectives for Information and Related Technologies (COBIT®) as its IT Governance Controls Framework.

- **Enforcement**

Protection of "Contractor" information is the responsibility of every employee. Therefore, every employee has a responsibility to be aware of and understand "Contractor"'s policy program. As well, all employees are required to remain in compliance with policy at all times. Failure to do so may result in disciplinary action, up to and including termination of employment.

This policy applies to all employees, contractors, and vendors accessing "Contractor" data, and IT processing facilities.

- **Exception Process**

The EISPP Steering Committee shall approve any exemptions to this policy. Exemption requests to this policy must satisfy the following criteria:

- The committee must be provided with the problem and a resolution scenario;
- The scenario must be justified with a business need and practical; and
- It must have signoff from the business area impacted.

- **Ownership & Management**

  This enterprise policy is owned, managed, and maintained by the CIO, in cooperation with the EISPP Steering Committee, and iSAC office.

- **Review Cycle**
  The policy owner will review this policy at planned intervals (i.e. annually at minimum) or when significant changes have occurred within the business or the operating environment of the business. These reviews will ensure that the policy is suitable, adequate and effective. Where a policy requires review and updating, the current policy shall be effective until the new policy is approved and distributed. The policy owner shall be responsible for the dissemination of the new policy to the user community.
  The review cycle will include the following considerations:
  - Changes to the operating environment (i.e. legislative/regulatory, technology, etc.);
  - Policy review by independent parties;
  - Management reviews; and
  - Changes to the Information security threat landscape.

- **Terms and Definitions**

The authoritative reference for information security terms will be the NIST IR 7298 Glossary of Key Information Security Terms. The NIST portal (http://csrc.nist.gov/) will be referred for updates to this glossary of terms and definitions for information security.

- **Policy Descriptions and Policy Number References**

Throughout this policy document, and available information security domains, there will be a table of Policy Descriptions and associated Policy Numbers for currently established procedures at the various operational locations for performing the stated information security policy domain. These procedures include defined standards of operations for the control, and may be associated with published Standard Operating Procedures.

Information Security Governance Structure

- ***Overview***

Information security administration and governance is performed by different roles within an organization. Consistency in the responsibilities and approach to administration and governance is required to ensure that risk is properly managed. Confirmation of the responsibilities in a policy will facilitate alignment of these responsibilities across departments and external organizations as applicable. Personnel are important and strategic assets and "Contractor" needs to ensure they are appropriately organized, and understand their roles and responsibilities in maintaining the overall security of information assets and resources.

- ***Purpose***

It is a requirement to ensure that employees, contractors and third parties are aware of their overall responsibilities to comply with all "Contractor" policies and applicable regulations and laws. In addition, individuals shall consult their Manager and/ors Human Resources personnel regarding specific security responsibilities related to their role or function. The policy goal is to ensure information security responsibilities are consistently applied, administered, and monitored in response to business conditions.

- ***Policy***

"Contractor" will maintain information security governance and administration functions to manage the security components, processes and procedures within each area of responsibility. Various groups are involved in the development, review, recommendations, approval, implementation, monitoring and management of the information security policies. The following outlines the responsibilities of the various groups involved in information security governance and administration.

- ***Board of Directors***

The Board has ultimate responsibility for corporate risk and management oversight of the company. The Board shall review and approve this information security management policy annually, as a component of the general compliance program. The Board shall also maintain a general understanding of the scope of this policy and, where required, make inquiries of responsible senior officers with respect to this policy. Additionally, the

Board shall review the outcome of significant information security events and the resulting action plans for preventing recurrence of the incident, or problem.

- ***"Contractor" Units Operations Management***

The following is a list of activities this group will engage and be responsible for:

- Participating in the Information Security Steering Committee;
- Integrating Corporate Security Policies into the Business Unit security program (i.e. AUP/SOP);
- Providing recommendations for corporate information security policies, as required;
- All business and support functions including technology groups ensuring compliance with all information security policies, standards and requirements, including applicable regulatory requirements within the jurisdictions they operate;
- Ensuring that every employee, contractor, or third party understands their responsibilities and accountabilities for information security;
- Establishing and implement appropriate business unit level procedures and practices that comply with this policy, and applicable regulations for the safeguarding of information in the business' possession;
- Ensuring escalation processes and controls exist to identify and resolve any breach of security over information; and
- Maintaining adequate documentation for compliance to this policy.

- ***Information Security Steering Committee***

This committee is composed of the Operational and Technology Management team for each of the "Contractor" Units (i.e. VP Operations, and Director of IT), the "Contractor" CIO, and the iSAC Office Director. This committee will endorse and champion information security, and provide counsel on the development and implementation of information security strategies, policies, and practices. This committee shall:

- Consider and recommend changes to the security policies and standards;
- Review and update Information Security Standards;
- Define Information Security Policy documentation ownership and maintenance;
- Incorporate the Information Security Principles and management requirements into the Information Security Policy Framework;
- Champion the deployment of Corporate Programs for Information Security Policies and Issue-Specific Security Standards with the Lines of Businesses;
- Measure the effectiveness of the security policies; and
- Maintain adequate documentation for compliance to this policy.

- ***Information Security Assurance & Compliance Office (iSAC)***

This corporate-level management office is responsible for coordinating general information security assurance and compliance activities and processes within the "Contractor" Units. This office will work directly with the "Contractor" Units, via their local Information Systems Security Office ("ISSO") representative, to coordinate customer audit activities, internal information security initiatives, and internal and external audit compliance reviews. Also, iSAC will assist the "Contractor" Units with their business continuity management ("BCM") programs to ensure compliance with "Contractor" information security policy, and customer requirements. This office shall also be responsible for performing objective assessments of information security control effectiveness through scheduled reviews and independent audits.

- ***Information Systems Security Office (ISSO)***

This function is a component of each respective "Contractor" Unit Operations with a specific responsibility for coordinating information security standards and security incident management and investigations. The ISSO will coordinate with, and receive assistance from, the iSAC office to ensure that corporate standards for information security are deployed and maintained as required. The ISSO is also responsible for ensuring that information technology security measures are applied, administered, and monitored in response to business conditions. In general, the ISSO shall be responsible for:

- Investigating internal and external incidents or breaches in security;
- Ensuring chain of custody and due care is applied to breaches, as required;
- Providing recommendations where appropriate on security policies and practices for the safeguarding of information assets;

- Providing a forum and senior management council on strategy, policies and practices related to customer and employee privacy matters and compliance to relevant privacy legislation or regulatory requirements; and
- Maintaining adequate documentation for compliance to this policy.

- ***Human Resources***

This function will engage and be responsible for:

- Reviewing information security policies for personnel expectations and security requirements in roles and responsibilities;
- Ensuring due care is applied during the hiring process according to the information security policies;
- Providing recommendations on policy content, as required;
- Managing records of attestation; and
- Maintaining adequate documentation for compliance to this policy.

- ***Employees***
  - Must be aware and knowledgeable of the "Contractor" Information Security Policies, Standards, and Procedures.
  - Understand "Contractor"'s commitment to Information Security.
  - Understand their role and responsibility in protecting "Contractor" data/information assets and IT resources.
  - Acknowledgment of policies through an annual attestation process.
  - Attend annual information security awareness training.
- ***External Contractors***
  - Must be aware and knowledgeable of "Contractor" Information Security Policies Standards, and Procedures.
  - Understands their obligations to comply with "Contractor" information Security Policies as a requirement in continuing their contract with "Contractor".

Policy Descriptions and Policy Number References

Information Asset and Resource Management

- ***Overview***

Information can exist and be communicated in many forms. It can be printed and faxed, stored electronically and transmitted using various electronic means or spoken in conversation. It is the responsibility of every employee, contractor, or third party, to protect "Contractor" data/information assets. This extends to using approved or accepted means for communicating that information. As with all forms of technology, it is imperative that we adequately protect, preserve and take care in transmitting all controlled "Contractor" data and/or information. This policy sets out those accepted circumstances under which various forms of electronic communication may be used for purposes of "Contractor" business.

- ***Purpose***

This policy sets out those acceptable electronic mechanisms for undertaking related business communications and the security practices that shall apply to transmitted and stored information. When using any form of electronic communications device, users must reference and acknowledge the classification of the information assets accessed during this transaction to ensure that sufficient controls are in place to maintain the security requirements based on its classification. Electronic communication includes, but shall not be limited to, data created and sent or received via the following systems or services:

- Internet;
- Email;
- Facsimile transmission (manual or automated);
- Text messaging (IM, SMS, etc.);
- Cellular/iDEN/PCS/VoIP telephones – voice, messaging, mobile browsing;
- Pagers;
- Smartphone and mobile computing devices; and
- Video.

- ***Policy***

All users of the "Contractor" network environment must be familiar with and acknowledge the risks associated with the use of electronic communications, and exercise due care and good judgment in communicating controlled "Contractor" data and/or information.

- **Acceptable Use of Assets**
- ***Internet***

Employees are permitted to use the Internet, where necessary, to carry out job responsibilities as well as maintaining currency in profession specific fields. Using Internet communication to carry out personal responsibilities is permitted as long as it does not negatively impact job performance, the efficiency and security of "Contractor" information systems, and "Contractor" reputation. The use of this technology will be monitored to ensure compliance with policies. Viewing, downloading, generating, possessing or distributing inappropriate or offensive materials from the Internet is not considered acceptable use of resources and is therefore subject to disciplinary action. Inappropriate or offensive material includes sites, material or activity that is/has:

- Sexually oriented content, text or graphic, including jokes and cartoons;
- Gambling of any nature;
- Illegal/Questionable Conduct, including sites that promote crime, unethical or dishonest behavior;
- Hacking, including sites providing information on or promoting illegal or questionable access to information systems. (*The exception to this requirement is for use in information security research by the IT department and iSAC as part of the vulnerability management program, and similarly related information security management programs*);
- Racism/Hate, including sites that promote the denigration or superiority of any racial or identifiable group;
- Violence, including sites that promote violent activity or behavior; and
- Or any other site where content is not deemed to be reasonable or appropriate in a professional work setting.

- ***Email***

Email facilities provided by the "Contractor" corporate network environment shall only be used for "Contractor" business communication. Internet email shall not be considered a secure method for business communication and all business communications transmitted via Internet email is subject to the Data Classification Policy and shall be encrypted, as required, according to encryption policy and standards. All employees who have an email identity are responsible for any and all actions associated with this identity and must use it responsibly. Employees are responsible for any access or use of their account and email ID and shall ensure such use conforms to this policy. When using email, all employees shall ensure that precautions are in place to protect "Contractor" systems, and data/information from risk of exposure, tampering or abuse.

When email attachments are necessary for sending out to a customer or third party it must be first determined if the attachment contains Personally Identifiable Information (PII), Electronic Protected Health Information (EPHI) or otherwise contains Restricted or Confidential information that if the document is inappropriately disclosed can breach compliance requirements, and/or be harmful to "Contractor", customer, or another third party. Examples of PII information as defined by the U.S. Office of Management and Budget (described in detail below):

- Full name (if not common);
- National identification number;
- IP address (in some cases);
- Vehicle registration plate number;
- Driver's license number;
- Face, fingerprints, or handwriting;
- Credit card numbers;
- Digital identity;
- Birthday;
- Birthplace; and
- Genetic information.

"Contractor" information/data can be defined as: **Restricted** or **Confidential** which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause irreparable harm to the organization. If the attachment does contain PII, EPHI, or other Restricted or Confidential company data/information, then the person sending the attachment must encrypt the data before sending. If encryption technology is not available, or technically feasible, then at a minimum the attachment should be compressed using commercially available software, and created with a password/passphrase to decompress and unlock the document. The password/passphrase will not be emailed along with the attachment, but must be communicated using an out-of-band method, such as verbal communication to the receiving party via telephone or in person.

- ***Facsimile Transmission***

All employees are required to ensure that when using technology care is taken to protect "Contractor" information/data assets. Using a facsimile machine to transmit information/data must be bound by the same scrutiny that we use in other methods of electronic transmission. Communications marked Restricted or Confidential shall be sent using secure transmission or alternative methods that have adequate controls to ensure adequate protection of the confidentiality and integrity of the communication.

- ***Mobile Computing Devices and Communications***

Mobile devices used for accessing the "Contractor" IT environment for office productivity services shall employ similar access controls mechanisms consistent with computer workstations. As indicated in this policy, users must be familiar with and acknowledge the risks associated with the use of mobile computing devices, and exercise due care and good judgment in handling and communicating controlled "Contractor" data and/or information on these devices.

Handling and communications involving data/information classified Restricted or Confidential must be encrypted or have appropriate compensating controls in place to protect its confidentiality and integrity.

Mobile storage devices are not to be used for the copying, or processing of customer data, or any other data classified as Restricted or Confidential. These devices include thumb drive memory sticks, and other non-volatile-based write/read-many type data storage devices.

- **Data Classification**

Data classification provides the preliminary mechanisms for the protection of data. The purpose of this data classification policy is to provide a system for protecting information that is critical to "Contractor". The scope of this policy includes all personnel who have access to any "Contractor" data in any form. All "Contractor" employees (including contractors and third party vendors with access to "Contractor" data) are responsible for the protection of "Contractor" data. Three levels of classification are in place. These are:

1. *Restricted or Confidential;*
2. *Internal Use Only; and*
3. *Public.*

Restricted or Confidential data is intended for use within the organization and represents the highest security level. Unauthorized disclosure could adversely impact the organization, its employees and its business partners. Examples include mailing schedules, mailing list data (addresses, names, etc.), company financial data, and vendor contracts (such as Equifax), customer client lists, and customer data including EPHI and PII. Restricted or Confidential data requires confidentiality controls for transmission and storage of this data where technically feasible. Controls can include, but are not limited to, encryption, read access privileges, and access monitoring. Specific requirements include:

1. "Contractor" client data classifications must default to Confidential or Restricted unless specified otherwise by the client;
2. Data must be destroyed in accordance with the "Contractor" *Data Management Policy;*
3. Must have signed 'Non-disclosure Agreements' for each user with access;
4. Data must not be posted on any publicly accessible page of a website;
5. Data must be stored on a secure server and not a local workstation/laptop using strong encryption (i.e. PGP/GPG);
6. Data stored on backup media such as CDs/DVDs, flash drives or tape must be encrypted or stored in a facility with controlled physical access; and

7. This data (including printed spoiled material) must be shred for secure disposal. If offsite shredding is provided by through a 3rd party, a certificate of destruction must be obtained and filed.

Internal Use Only data shall be protected from unauthorized access, modification, transmission, storage or other unauthorized use. Examples include "Contractor" company directories, employment data, customer price sheets, and vendor price sheets. Internal Use Only data requires confidentiality controls for transmission and storage outside of the "Contractor" IT infrastructure. Controls can include, but are not limited to, encryption, read access privileges, and access monitoring. Specific requirements include:

1. Data must be protected against loss, theft, unauthorized access and/or unauthorized disclosure;
2. Data must have access granted to authorized "Contractor" employees and contractors;
3. Data must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent unauthorized disclosure) when not in use;
4. Data can only be posted on a controlled website by authorized personnel, with approvals to do so;
5. Printed matter shall be shredded when no longer needed. Storage media shall be destroyed by shredding or by another process that renders the data beyond either recognition or reconstruction. Destruction records shall be maintained for future reference; and
6. Electronic storage media must be securely wiped by overwriting (i.e. DoD standard) or degaussing prior to disposal or reuse.

Public data is open and does not require confidentiality controls.

"Contractor" and customer data must be reviewed annually and reclassified, if required. The classification level and associated protection of replicated data must remain consistent with the original data.

- ***Roles & Responsibilities***

It shall be the responsibility of Managers and Human Resources to ensure that all employees, contractors and third parties have access to all relevant policies and procedures associated with adhering to this policy. This does not negate the responsibility of all employees, contractors and third parties to ensure that they understand and abide by their responsibilities in relation to the acceptable use of electronic communications.

- **Policy Descriptions and Policy Number References**

Policy No.	**Description of Policy**
P600.1	"Contractor"'s data classification policy has been designed to support the practice of "need to know", so that information will be protected from unauthorized disclosure, use, modification, and deletion.
P600.2	Any physical or logical collection of data must be classified as a whole at the highest data classification level within the collection.
Policy No.	**Description of Policy**
Classification	
601.1	Data that has not yet been classified must be treated as Confidential. For example, newly created documents must be stored on secure server network drives.
601.2	All "Contractor" data must be classified as "Public", "Internal Use Only", "Confidential", or "Restricted".
601.3	Classifications assigned to "Contractor" data must be reviewed at least once every three (3) years and reclassified based on changing usage, sensitivities, regulations, or legislations. For example, data currently classified as private may be elevated to confidential with the passing of new state or federal laws.
601.4	Data must be protected in accordance with the security controls (Data Classification Levels) specified for the classification level that it is assigned.
601.5	The classification level and associated protection of replicated data must remain consistent with the original data [e.g. (i) confidential HR data copied to a CD-ROM, or other removable-media (e.g. floppy disk or thumb-drive), or from one server to another, retains its confidential classification; (ii) printed copies of confidential data also remain confidential.
G601.7	Inventory of computer assets used to store sensitive data.
Internal Use Only Safeguards	
602.1	Data must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
602.2	Data must have access granted to authorized "Contractor" employees and contractors.

602.3	Data must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
602.4	Data can only be posted on a website by authorized personnel.
602.5	Data must be properly destroyed when no longer needed subject to the "Contractor" Data Management Policy.
Internal Use Only Destruction Methods:	
603.1	Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
603.2	Electronic storage media must be sanitized appropriately by overwriting or degaussing prior to disposal.
Policy No.	**Description of Policy**
[Confidential] - Data Safeguards	
604.1	"Contractor" client data classifications must default to confidential unless specified as Restricted by the client.
604.2	Data stored in an electronic format must be protected.
604.3	Data access is granted based on the user's role/job responsibility.
604.4	Data must not be disclosed to parties without explicit management authorization.
604.5	Data stored in areas with access controls in accordance with *Physical Access Policy.*
604.6	Data must be destroyed in accordance to the "Contractor" *Data Management Policy.*
G605.7	Employees must sign confidentiality and security agreement for handling of sensitive information.
G605.8	Service providers' non-disclosure agreements requires the company to ensure that service providers maintain safeguards for handling sensitive information.
[Confidential] - Data Destruction Methods:	
605.1	Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
605.2	Electronic storage media must be sanitized appropriately by overwriting or degaussing prior to disposal.
[Restricted] - Data Safeguards:	
606.1	Data stored in an electronic format must be protected.
606.2	Data must be encrypted when stored on servers.
606.3	Must have signed 'Non-disclosure Agreements' for each user with access.
606.4	Data must be stored in areas with access controls in accordance with *Physical Access Policy.*
606.5	Data must not be posted on any public website.
606.6	Data must be stored on a secure server and not a local workstation/laptop.
606.7	Data must be destroyed in accordance to the "Contractor" *Data Management Policy.*
606.8	Data classified 'Restricted' must be encrypted using strong encryption (ie.PGP/GPG) when stored on the "Contractor" network. Data stored on electronic media such as CDs/DVDs, flash drives or tape must be encrypted.
[Restricted] - Data Destruction Methods:	
607.1	"Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
607.2	Electronic storage media must be sanitized appropriately (i.e. overwriting, secure delete or degaussing) and data must not be retrievable prior to disposal.
Policy No.	**Description of Policy**
Hardware	
1001.1	Connection of non-"Contractor" provided devices to any "Contractor" provided device is prohibited without written permission from IT Management. This includes but is not limited to- Music Players (iPods etc.), printers, scanners, cameras, cell phones, and Personal Digital Assistants (PDA) and external storage devices (USB drives/thumb drives, portable hard drives, and CD/DVD burners.
1001.2	All users will use approved/standard computing hardware to access the corporate network unless

	approved by management. This includes company approved models and manufacturers.
1001.3	Hardware is to be purchased by the company through standard company procurement channels only. It is not acceptable to purchased company hardware through retail channels unless approved by management.
Applications	
1002.1	Users will only use approved company software. Loading or installing software that is non-company approved onto company equipment is prohibited.
1002.2	Applications are to be purchased by the company through standard company procurement channels only. It is not acceptable to purchased company software through retail channels unless approved by management.

Human Resource Security

- ***Overview***

Personnel are important and strategic assets for securing information resources and assets and "Contractor" must ensure that employees, contractors, and third party users understand their role and responsibilities.

- ***Purpose***

It is a requirement that employees, contractors and third parties are aware of their responsibilities to minimize risk and ensure compliance to all policies and applicable regulations and laws. Human error and omissions are inherently weak components of an organization's defense strategy for information resources and assets. In addition, individuals shall consult their Manager and Human Resources personnel regarding specific security responsibilities related to their role or function. The policy goal is to ensure information security responsibilities are consistently applied, administered, and monitored in response to business conditions.

- ***Policy***

All personnel shall abide by "Contractor" security policies and procedures and ensure compliance to specific security practices that apply to individual roles or functions. All personnel shall annually acknowledge and attest, as part of the annual acknowledgement process with HR, to having read and understand "Contractor" policies.

- ***Conditions of Employment***

All personnel, at the time of accepting a position, and annually, shall attest to:

- Conforming to "Contractor" security policies and procedures;
- Maintaining the confidentiality of "Contractor" and customer related data/information;
- Having an obligation to report any security incident, improper or unethical practice, whether actual or suspected;
- Being aware of the consequences of intentional violations, negligence, errors or omissions; and
- Completing the "Contractor" Information Security Awareness Training.

Human Resources shall maintain the signed annual attestation record, and record of attendance for the Information Security Awareness Training.

- ***Background Checking and Security Clearance***

Appropriate background checks, and security clearance checks as required, shall be undertaken for all employees and contractors commensurate with the risks involved in the job function. All roles within the organization shall be defined based on the type of information that is accessed and handled as part of day-to-day functions and, an appropriate screening or security process shall be implemented. Required security clearance checks shall be advised to the employee, contractor or third party in advance. Independent and qualified individuals shall perform security clearance checks, and only the results advised to the relevant Manager. Any information collected, during or obtained as a result of the security clearance process, shall be treated as Restricted under the *Data Classification Policy* and handled accordingly.

- ***Employment Transfers***

The terms and conditions of all employees transferring or undertaking promotion shall be reviewed and revised, as required, to ensure changes to security responsibilities are appropriately administered. Where changes are required, and the following are deemed necessary, the employee shall undertake the annual attestation again and any additional security screenings required prior to commencing in the new position.

- ***Information Security Awareness, Education, and Training***

All employees and contractors accessing "Contractor" IT network resources and information/data assets shall, at a minimum, complete the annual information security awareness training or equivalent, and review and adhere to any security communication updates provided by "Contractor".
It shall be the responsibility of Managers to ensure that, where required, employees and contractors undertaking roles or functions requiring heightened levels of security training are appropriately trained and regularly tested for competency appropriate to the role or function.

- ***Roles & Responsibilities***

Human Resources shall define the roles and responsibilities of all employees, contractors and third parties, including the requirement to adhere to management policies, procedures, codes of conduct, and any applicable professional practices. The terms of conditions of all employment contracts shall define the employee's responsibility for information security and incident management. Employees, contractors and third parties are responsible for adherence to and compliance with this policy and other applicable "Contractor" policies. Any case of unauthorized access to "Contractor"'s information shall be immediately reported to the appropriate party and, if needed, escalated to higher levels for investigation and resolution.

- **Policy Descriptions and Policy Number References**

Policy No.	Description of Policy
Communication	
G1101.1	Training of employees to maintain security, confidentiality, and integrity of sensitive information
G1101.2	Regular reminders and security awareness to employees - Regular communication to employees regarding company policy and legal requirement to keep sensitive data secure and confidential.
G1101.3	Advising employees of new security risks or possible breaches.
Security Response	
G1102.1	The security SOP manual outlines the steps in responding to security breaches. Includes: notification for customers, businesses, law enforcement, and consumers as required by contracts, regulations, and state laws

Physical and Environmental Security

- ***Overview***

Assets are strategic in nature and as such their security is critical for effective and continued operations. Appropriate physical security control measures shall be established for facilities to ensure confidentiality, integrity and availability of information resources and assets. Where assets are located in public areas, they shall be appropriately protected to prevent or deter loss or damage from theft or vandalism. Physical security is the frontline of protection for "Contractor"'s employees, facilities and information resources and assets. All "Contractor" employees (including contractors and third party vendors with access to "Contractor" facilities) are responsible for adhering to this policy.

- ***Purpose***

This policy shall provide direction for the level of physical security required to protect "Contractor" assets commensurate with the classification of the asset, and provide adequate preventive controls, by means of a stable and secure base for the operation of the business systems. This policy establishes a standard for creation of secure workplaces and server rooms that will ensure the protection of employees, property and "Contractor" data.

Specific purposes of this policy include the following components:

- Mechanisms to prevent unauthorized physical access, damage, and interference to "Contractor" properties and assets;
- Mechanisms to prevent loss, damage, theft or compromise of assets and interruption to "Contractor"'s business activities;
- Physical security requirements for data in all forms (I.e. electronic, hard copy, etc.);
- Facility security requirements that host data and information technology infrastructure;
- Direction for users' handling and access of systems, networks and associated data;
- Clear desk policy requirements; and
- Definition of user responsibility for maintaining physical security.

- ***Policy***

Appropriate physical security shall be implemented to maintain an adequate level of access control to "Contractor" assets.

- ***Risk Assessment***

Physical security of assets is largely dependent on the nature of the asset and the environment in which it resides and is used. To appropriately assess and determine the physical security requirements a risk assessment shall be undertaken to determine value and evaluate known threats and vulnerabilities.

- ***Perimeter Security***

Perimeter security shall be well defined with controlled entry points to include monitoring of all access. The entry controls shall include alarm systems, card controlled entry gates (or similar positive authentication mechanisms such as guard stations, or recognition authentication) and surveillance cameras. All these controls and barriers must be consistently applied.

- ***Physical Entry Controls***

Classified or Restricted areas within "Contractor" shall be protected by appropriate entry controls and mechanisms to ensure that only authorized personnel are allowed access, and where applicable, third party users and contractors may also be granted specific access. Access rights shall be audited, reviewed and updated on a regular basis to detect any unusual activity and also to maintain users' accountability.

- ***External and Environmental Threats***

Appropriate physical protection against natural or man made events such as fire, flood, ice storm, earthquake, explosion and others shall be designed and implemented, as feasible. Where applicable, there may be a need to design a backup system that will provide continuity of services in the event of a disruption to normal operations. It is important that the backup systems are stored securely at an offsite location and are well protected from similar external and environmental threats that may affect the primary facility. The backup systems must be tested on a regular basis to ensure the systems will operate effectively when required.

- ***High Security Areas***

Where heightened risk has been identified, "Contractor" shall install additional monitoring devices (i.e. surveillance camera equipment, motion sensing equipment, etc). Users shall be advised of any monitoring activities, and be made aware of their rights and responsibilities working in these secure areas.

- ***Delivery and Loading Areas***

Appropriate security and monitoring services shall be implemented in shipping and receiving areas where high value assets are received, shipped, and/or stored, and where open access poses a risk to the security of the facility. Physical access control mechanisms shall include automated controls such as card access controlled doors, or similarly authenticated access control mechanisms (i.e. recognition authentication, guard station), and registering and inspecting all incoming, and outgoing material.

- ***Equipment Location and Protection***

Equipment must be protected from physical and environmental threats that may compromise the security of the asset, and data. Protective measures shall be commensurate with the criticality of the equipment and risk attributes of data associated with it. Access to highly sensitive information processing facilities shall be limited only to designated individuals, and these facilities shall be monitored. Access to these facilities will also employ controlled access mechanisms. Users must be aware at all times when accessing secured facilities to ensure that tailgating does not occur.

- ***Workstation Environment***

  Users of remote mobile computers, while working in high risk or public facilities, shall physically secure their computers by means of a security cable or similar locking mechanism if they intend to be absent from their computer during their session. This is not necessary if they plan to be with their computer on a continuous basis. When mobile workstations are transported in a vehicle, and away from the person, care must be taken by the employee to secure the mobile workstation in a lockable trunk. If a lockable trunk is not available, the mobile workstation must be concealed from view by passersby and/or physically secured to the vehicle, with a locking cable, if possible. Alternatively, the employee can also carry the mobile computer with them if no reasonable facility is available for storage.

- ***Server Environment***

  Servers shall be located in physically secure and controlled access facilities. These facilities shall be considered data centers or raised floor environments with specific and specialized access permissions.

Access to these facilities will be limited to individuals assigned the role of system maintenance and administration, or equivalent.

- ***Equipment Maintenance***

Qualified parties shall ensure the proper functioning of equipment in accordance with the manufacturer's specifications by performing regular scheduled maintenance procedures. Where high value or sensitive assets are impacted, additional precautions shall be considered including physically escorting maintenance personnel, as needed.

- ***Secure Disposal or Re-Use of Equipment***

All information and equipment shall be disposed of or reused in a secure manner according to the identified classification of the material. All information system devices capable of storing information (i.e. hard drives, removable media, etc.) shall be either destroyed or wiped of their data contents. Equipment destined for recycling and reuse, shall be wiped of any data prior to reissue. Data removal will follow similar standards and procedures required for disposal of information systems equipment and/or media devices. Auditable records shall be maintained in all circumstances.

- ***Removal of Property***

Assets normally resident in the office environment of "Contractor" shall not be removed from the premises without prior authorization. IT equipment removed shall be recorded for audit purposes to ensure accountability to the assets' owner. Where cases of theft are suspected, designated individuals under the guidance of Human Resources shall perform spot checks.

- ***Emergency Services***

A detailed plan for access to emergency services and reporting incidents shall be made available to all staff working or accessing "Contractor" facilities. Emergency service plans shall be reviewed and tested annually as part of the Disaster Recovery Plan for each "Contractor" operating Unit.

- ***Parking***

Where parking facilities are available for staff, efforts shall be made to ensure the safety of staff transitioning in and out of these facilities. Additional precautions shall be considered for staff working outside of normal business hours and those potentially at greater risk of harm.

- ***Roles and Responsibilities***

Maintaining the security of assets is a key component of mitigating risks in the organization. Every asset owner has responsibility in determining and enforcing access to their assets. The asset owner is responsible for assigning value to the asset and classifying it according to its sensitivity and criticality. This shall be reviewed on a regular basis and the asset shall be re-classified, as circumstances require. The asset owner must authorize access to the asset as needed. The asset owner must ensure that the appropriate controls are in place commensurate with the risk level. The asset owner must investigate any reports of unauthorized access. It is the responsibility of each employee of the organization to ensure that there is no unauthorized access to the premises, assets and information. Consistent with the "defense in depth" strategy, all employees must be aware of, and challenge unfamiliar individuals to a location (i.e. those not wearing a visible identification badge or access card), to ensure access is authorized.

Responsibility for any of the above may be delegated where appropriate but the accountability remains with the asset owner.

- **Policy Descriptions and Policy Number References**

Policy No.	Description of Policy
P500.1	The issuance of ID badges allows for the safeguarding and tracking of "Contractor" employee access to facilities and information resources.
P500.2	"Contractor"'s business requires that contractors, vendors and clients may need access to "Contractor" facilities and tracking/logging of such access.
P500.3	Access to restricted areas such as server rooms are limited to authorize personal and tracked when entering or exiting secure locations.
P500.4	Surveillance video provides monitoring of entry points and restricted areas.
Policy No.	**Description of Policy**
Badges	
501.1	Badges must not contain identifying information other than photo, employee name, Identifying

	number and “Contractor” logo.
501.2	Badges must not be shared or loaned out except for authorized personnel.
501.3	Badges must be visible or available upon request at all times.
501.4	All employees of “Contractor” are assigned a badge that grants access to their work area only. All other access is granted on an ‘as needed’ basis.
501.5	Designated manager i.e. Human Resources/Office Manager or will create the employee’s badge upon receiving a request from the employee’s manager.
501.6	Requests for badges must be kept on file for a period of one year.
501.7	Badge access rights reviewed on a quarterly basis.
501.8	Inactive badges reviewed on a quarterly basis.
501.9	Badges must be turned in and deactivated upon the termination, lost / stolen, or departure of an employee.
501.10	A service charge may be assessed for cards that are lost, stolen or not returned.
501.11	Temporary Employee ID can be issued by HR or mgmt upon request.
Visitors and Logs	
502.1	Contractors, vendors or guests that do not have authorized access must sign-in at the front desk upon arrival at “Contractor”.
502.3	Contractors, vendors, or guests will be issued a temporary guest identification tag.
502.4	Contractors, vendors or guest must have their guest identification tag visible or available upon request.
502.5	Contractors, vendors or guests that do not have authorized access must be escorted at all times while in restricted areas
502.6	Contractors, vendors or guests must turn in their guest identification tag and sign-out at the end of each day.
502.7	Guest logs will be reviewed daily to ensure that each guest identification tag is returned.
502.8	Access to “Contractor” facilities must be logged, reviewed, and kept for a minimum of one year.
Server Room Access	
503.1	Access to the server room must be submitted in writing and approved by the ISSO manager or of a similar level. All requests must be kept on site for a period of one year.
503.2	Access lists to the server room must be reviewed and signed-off on a quarterly basis.
503.3	Employees may not “Tailgate” another employee through ANY entryway.
503.4	Contractors, vendors and guests must be escorted at all times while in the server room.
503.5	Everyone entering the server room must login and logout upon entry and exit.
503.6	The server’s function or IP address must not be displayed openly on or near the server.
Policy No.	**Description of Policy**
Cameras, Alarms, and Motion Sensors	
504.1	All entry points to the server room must be monitored via video camera.
504.2	Surveillance video must be maintained for a minimum period of one month and be stored in a secure location.
504.3	Remote monitoring must be utilized in the server room for after hours monitoring.
504.4	Each entry point to a “Contractor” facility, that can be opened, must be alarmed (e.g. doors, windows, etc.).
504.5	Each external entry point to a “Contractor” facility must be monitored via video camera.
504.6	Loading dock doors must remain closed when not in use.
504.7	Alarm codes must be changed when any employee with knowledge of the code leaves the company.
Environmental Controls	
505.1	HVAC system to control temperature and humidity.
505.2	Functioning Fire suppression system in data center.
505.3	Physical security systems must meet all local regulations, including, but not limited to building and fire codes.
Background Check	
506.1	Individuals must be made aware of the background check procedures during the application process. Appointment to or continued employment in a specified position is contingent upon an acceptable

	background check, and any written offer of employment must contain notice of this contingency.

Operations Management and Security

- ***Overview***

The protection of information in networks and the protection of supporting networks are complementary to the information security controls executed by staff and processes, and support the defense-in-depth strategy. The network infrastructure provides the next layer of control over the people and processes by integrating security into the infrastructure to fortify with network-based controls and security of network services. This policy will provide the direction required to ensure that infrastructure design considers and integrates security controls (i.e. confidentiality, integrity, and availability).

- ***Purpose***

"Contractor" employs a defense-in-depth strategy for managing information security across the systems and network infrastructure components within the enterprise. Access to information resources and assets are controlled by multiple security mechanisms and/or processes to ensure that access is both legitimate and controlled. For the defense-in-depth strategy to be successful, the implemented security processes and technology must be consistent with the security strategy and program to ensure that the individual components of the security strategy and program "fit" correctly and work effectively. This policy provides the direction to ensure that a common approach and policy toward information security is applied to the systems and network infrastructure for a good "fit".

This policy will apply enterprise-wide to include all IT infrastructures responsible for supporting the business processes of the organization. The policy goal is to provide the basis for reliability and availability of these resources in providing continuous support of business processes. Key elements of this policy include:

- Security controls for availability, integrity and confidentiality of IT infrastructure components and supporting network services;
- Physical design requirements for infrastructure zoning and segmentation to ensure adequate controls over access to IT resources; and
- Controlled access to data and systems depending on authorizations prescribed by the classification of the data and system, and criticality of infrastructure in supporting critical business processes.

- ***Policy***

To maintain the overall security of information resources, equipment shall be situated and designed for protection from logical, physical and environmental threats. Security shall be designed into the lifecycle of equipment to ensure that secure procedures for design, development, implementation, operations, and disposal exists. These controls shall also apply to ensure the availability of supporting utilities and facilities, such as the electrical supply and cabling infrastructure. The network infrastructure shall provide separation of networks to allocate higher sensitivity devices and resources to strongly controlled segments of the network. The allocation of devices and resources accessing the network will depend on the classification of the data residing on the devices and resources, provided by the *Data Classification Policy*.

- **Protection Against Malicious and Mobile Code**

To address the potential impact of malicious and/or unauthorized software, a protection program shall be maintained that will prevent, detect, and correct against malicious software (i.e. antivirus, antimalware, and antispyware software or network scanning devices). Only authorized software is to be used on "Contractor" IT infrastructure and equipment. Malicious and unauthorized software detection processes shall be utilized in the operation of the IT infrastructure systems. Malicious software is any software that can negatively impact or cause harm to IT systems, information or networks. There are several forms of malicious or unauthorized software and methods by which they can cause harm. Malicious or unauthorized software are at best a nuisance requiring time and effort to deal with, and in the worst-case have the ability to damage or destroy information or systems and require extensive reconstruction and recovery. A malicious or unauthorized software protection system includes, but is not limited to:

- The scanning of storage devices with up-to-date scanning software;
- Implementation of a malicious software removal and recovery process when they are encountered;
- The maintenance of a corporate security awareness program;
- The utilization of a malicious software detection system as a component of normal systems operations; and
- The protection environment including centralized reporting of malicious and unauthorized software.

- ***Controls against Malicious Software***

Malicious software includes viruses, worms, Trojan horse, Spyware, and other software designed for malicious intent.

- Antivirus protection facilities will be implemented at the desktop level that must not be disabled by the user.
- Antivirus protection facilities will be implemented at the network gateway (i.e. perimeter) to monitor and scan all incoming data packets for malicious software.
- Virus scanning tools and software will be made available and maintained by the business unit support groups.
- Software patches, updates, and releases must be screened and managed for distribution based on necessity and criticality.
- Software patches, updates, and releases shall only be accepted from authorized vendor sources. These updates shall be obtained on a regular basis as suggested by the software vendor and distributed consistent with change management and release management processes.
- The designated business support unit shall maintain secure storage for original software in the event a product needs to be recovered or reinstalled.
- It is the users' responsibility to notify the Service Desk if a virus is encountered or suspected.
- Any notification of virus information received via messages must be communicated to the IT Department. Messages concerning viruses must not be forwarded to other users.
- Third-party connections will be authorized and controlled consistent with information security policies to prevent malicious software introduction.
- Teleworking for remote users using non-"Contractor" workstations will implement controls for malicious software consistent with this policy.

- ***Desktop Image***

It is the responsibility of all employees to ensure that the "Contractor" standard desktop image in use by them is not tampered with in any way from its original configuration. Users are not to install additional software on "Contractor" workstations unless they have approval to do so.

- **Network Security Management**

Mechanisms shall be implemented to monitor ongoing security of the IT infrastructure. These mechanisms will provide management reports to ensure that the network security controls are consistent with information security policy. Specific items to monitor may include:

- Non-standard and unauthorized software;
- Abnormal network activity;
- Unauthorized/brute force attack signatures from the respective gateways;
- Unauthorized/brute force attack activities from within the "Contractor" IT infrastructure;
- Existence of unidentified and/or rogue network devices; and
- Unauthorized system changes, based on event logs and standard configuration records.

These mechanisms will also provide the following preventive and detective controls:

- Antivirus; and
- Tools for performing automated penetration and vulnerability testing.

- ***User Authentication for External Connections***

External connections made either by third parties, contractors, or remote employees must follow the Access Control policy for authenticating and authorizing users and their equipment. Connections involving non-"Contractor"-owned equipment will not be treated as trusted connections and will employ secure interfaces with the "Contractor" IT infrastructure. This secure interface will include the installation of a firewall and antivirus, at the "Contractor"-side of the connection. Mobile computing and teleworking infrastructure will employ secure infrastructure to authenticate users to the corporate environment according to the principle of need-to-know as defined by the Access Control Policy. Connections made by users must, at all times, conduct themselves in accordance with "Contractor" policies.

- ***Capacity Management***

Network resources shall be monitored for performance and peak load to ensure that availability of information assets and other supported resources are maintained at acceptable levels. Preventive, detective, and corrective

controls shall be designed and implemented to proactively and retroactively manage the infrastructure to ensure maximum availability of network services.

- ***Security of System Documentation***

Network configuration and design documentation shall be secured and maintained as Internal Use Only documents to ensure that documentation is current, secured, and readily available on a need-to-know basis.

- ***End-Point Security***

Network and desktop security strategy requires that appropriate security monitoring and compliance mechanisms be implemented at the end-point devices that connect to the "Contractor" IT infrastructure. End-point devices that are not recognized as authorized end-point devices, shall be denied access.

- ***Network Controls***

"Contractor" network device logging must be enabled. All logs must include information that is sufficient to support audits of overall effectiveness and compliance with security policies. The ISSO, or delegate, on a quarterly basis, must review logs that contain notification alarms. The system administrator is responsible for providing the logs to ISSO who must sign each log report that is reviewed. Each completed log report must be stored and kept for a period of six months.

For systems that process customer data, secure logging must be deployed to ensure that the source logs are reliable. A secure log server may be deployed in the production environment to consolidate log files from defined servers for evaluation and monitoring.

The network administrator must scan the network for open ports and known vulnerabilities defined in the *Security Scan procedures document* according to the following schedule:

- Internal Scan – every 6 months; and
- External Scan – every 3 months.

A network intrusion detection system shall be in place to alert the IT Administrator and ISSO of potential or occurring attacks.

- **Exchange of Information**

File Transfer Protocol is permitted to exchange information between the respective "Contractor" Unit and customer IT facilities. Where available, secure FTP, or other similar secure transmission protocol, shall be used to exchange information.

- **Data Backup**

"Contractor" data will be archived for the purposes of continuity of services resulting from an unplanned disruption of normal business operations. Data will be retained in accordance with business requirements for operational data, and regulatory requirements.

A formal backup procedure will be established and documented to ensure a consistent approach to the backup process. Data archiving will be performed on a regular basis and include daily incremental backups, and monthly full backups. Scheduled offsite backup media must be stored in a secure location with controlled access. Backup media must be stored in a fireproof facility rated for media and encrypted as part of the backup process. Chain of custody shall be maintained for all offsite transport of backup media. Backup media that contain customer data shall include confidentiality controls such as encryption for media archived onsite, as well as offsite.

Back-up data for customers must be assigned a specific agreed upon retention period. The backup administrator and IT management shall be notified when a retention period is ending. In all cases the back-up data must be destroyed after the assigned retention period has ended.

- **Third Party Policy**

As business relationships increase in complexity through outsourcing internal processes, there is a need to apply due diligence in managing these relationships to ensure the organization can continue to meet its business obligations. The result is that requirements of the organization now extend to the third party; however responsibility remains with "Contractor" to ensure continued compliance with their obligations.

All third parties, and their sub-contractors, servicing "Contractor" through an outsourcing arrangement will be subject to defined Information Security questionnaire and audit based on the services they provide to "Contractor". For third parties that have access to "Contractor" IT resources and information assets/data, "Contractor" will regularly assess the effectiveness of the information security control measures in place and maintained by the third

party and its applicable sub-contractors. This policy sets out the over-arching security requirements for third parties (including sub-contractors), non-employees, or business partners who access "Contractor" IT resources and information/data assets during the course of conducting business with "Contractor".

- ***Third Party Contractual Agreement***

Third party arrangements shall be documented in a formal service level agreement, subject to the following:

- Reviewed by a Legal representative of "Contractor";
- Where necessary, there shall be confidentiality agreements and non-disclosure agreements between the third party and "Contractor" when access to "Contractor" IT resources and information assets/data is involved in the services being provided;
- A listing of all sub-contracted entities of the third party involved in the provisioning of services provided to or on behalf of "Contractor";
- All applicable "Contractor" policies, standards, and procedures to which the third party, and its sub-contractors, are obligated to adhere to;
- Obligation for security awareness training for third party employees involved in the provision of services to "Contractor" must be demonstrated to be consistent with "Contractor"'s security awareness program when access to "Contractor" IT resources and information assets/data is involved in the services being provided;
- Applicable security clearance checks when access to "Contractor" IT resources and information assets/data is involved in the services being provided;
- Applicable business continuity and disaster recovery requirements;
- Measurement mechanisms to ensure ongoing compliance with contract obligations; and
- Completion of the Third Party Compliance Program information security questionnaire with satisfactory assessment results.

- ***Third Party Compliance***

Service level agreements shall identify specific information security related activities, such as right to audit, that will be conducted by "Contractor" or their designate, at their discretion, to test compliance with "Contractor" information security policies by the third party and their applicable sub-contracted entities involved in the provision of services, or handling of "Contractor" IT resources and information assets/data. Third party service level contracts will specify that the third party and/or applicable sub-contracted entities shall demonstrate compliance with defined criteria by providing operational performance reports.

- ***Roles & Responsibilities***

Network assets shall be designated an owner who shall be responsible for defining and periodically reviewing access restrictions, monitoring, and maintenance. The owner may delegate this responsibility to another associated member of his/her department; however, responsibility will still reside with the owner.

While incident response and monitoring remain the responsibility of the IT Department, the protection of information assets against malicious or unauthorized software is the responsibility of every employee, contractor and third party and shall be incorporated into the normal work environment. It is a management responsibility to ensure that incidents are dealt with on an efficient and timely basis.

- **Policy Descriptions and Policy Number References**

Policy No.	Description of Policy
P700.1	Full Data Backup on a monthly basis and incremental daily backups.
P700.2	Backup Hierarch & Retention schedule.
Policy No.	Description of Policy
Backups	
701.1	System administrator maintains documented backup process for ease of recoverability and audit.
701.2	Scheduled offsite backup media must be stored in a safe and secure location extraneous to the location of the backed up systems. Backup media must be stored in a fireproof safe rated for media and is encrypted as part of the backup process.
Media Destruction	
702.1	Any data classified as Restricted (including printed spoiled material) must be shred. If offsite shredding through a 3rd party a certificate of destruction must be provided and filed.
702.2	*Public Data Destruction Methods*: Can be disposed of in normal trash receptacles.

702.3	Before disposal or reuse erasing / expunging restricted data, a separate program performs a secure delete (if retrievable by common methods) is required to ensure the data is not retrievable.
702.4	Back-up data for "Contractor" clients must be assigned a specific agreed upon retention period. The backup administrator and IT management should be notified when a retention period is ending. In all cases the back-up data must be destroyed after the assigned retention period has ended.
G702.5	Requires designation of a records retention manager to supervise the disposal of records containing sensitive information.
Encryption Key Management	
703.1	**Key Generation:** Keys must be generated using an approved key generation method specified by the "Contractor" ISSO, or IT Manager of a similar level. Only key owners who have the necessary security authorizations and have received proper training must perform key generation functions. Keys must be changed on a regular basis depending on the nature of the critical operations they protect.
703.2	**Key Distribution:** is performed manually, where the key is brought to the employee and programmed at that time.
703.3	**Key Storage:** Unique/protected and private keys, which have a longer life than session keys, must be stored in a protected area.
703.4	**Key Storage**: When magnetic media are used to store keys, the media must be stored in a locked safe, vault, or an area where access is restricted to a limited number of personnel who are authorized by "Contractor"'s ISSO, or IT Manager of a similar level.
703.5	**Key Storage:** IT Manager of a similar level, will have documentation that includes the locations where keys are stored; protected methods to store magnetic media; proper authentication methods to prevent unauthorized access to computer and encryption software; and responsibilities of authorized personnel.
703.6	**Key Destruction**: The magnetic media must also be destroyed to ensure no data residue can be recovered. Encryption software can be used to automatically destroy keys and to produce audit reports (i.e., event logs) with information on time/date, type of actions, and user identification.
703.7	**Key Maintenance:** The key storage devices (e.g., vault, safe, etc.) must be protected with adequate physical security controls (e.g., badge access, keypad, or keys) so that the keys are not disclosed, modified, or replaced without the approval of the key owner.
Policy No.	**Description of Policy**
P800.1	"Contractor" performs logging and event trigging of events on its network All logs include information that supports audits and is in compliance with "Contractor" security policies.
P800.2	Logs subject to review follow notification and escalation procedures.
Policy No.	**Description of Policy**
Network Segmentation	
801.1	**Administrative Segment** - This segment has the lowest level of security and can be accessed by all "Contractor" personnel.
801.2	**Production Segment** – This segment is considered high-security and is isolated from any outside network (Internet).
801.3	**Data Services Segment** – This segment is considered high-security to limit access to "Contractor" customer data.
801.4	**DMZ Segment –** The Demilitarized zone segment is to isolate traffic from connecting to the internal network.
Network Security Logging Policy	
802.1	"Contractor" network devices must be enabled to perform logging of events (i.e. secure FTP) on a daily basis. All logs must include information that is sufficient to support audits of the effectiveness of and compliance in accordance with "Contractor" security policies.
802.2	Logs that contain Notification Alarms must be reviewed by the ISSO, or IT Manager of a similar level, on a quarterly basis. The system administrator is responsible for providing the logs to the ISSO, or IT Manager of a similar level.
802.3	The ISSO, or IT Manager of a similar level, must sign each log report that is reviewed. Each completed log report must be stored and kept for a period of six months.
Network Vulnerability Scanning	

803.1	The network administrator at each "Contractor" location must scan the network for open ports and holes defined in the *Security Scan procedures document* according to the following schedule: • Internal Scan – every 6 months, • External Scan – every 3 months.
G803.2	Use of a network intrusion detection system to create an alert about attacks.
Policy No.	**Description of Policy**
P900.1	Provide secure B2B FTP transmission moving files to a secure area once received.
P900.2	Logging / event trapping of all FTP traffic.
P900.3	Decryption of files is performed on an internal secure server within the "Contractor" secure network.
Policy No.	**Description of Policy**
FTP, Web-Upload, Email	
901.1	"Contractor" must provide FTP services through a dedicated FTP server located in "Contractor"'s public DMZ.
901.2	FTP accounts are recommended to be assigned to individuals and not to groups.
901.3	FTP must have tracking and audit logs enabled to track sending and receiving IP addresses.
901.4	For Restricted Data a Secure FTP server is scanned at timed internals for new files which are automatically moved to a secure internal server.
PGP and GPG Encryption	
902.1	Transmission of PGP/GPG data should use public keys.
902.2	Decryption of files is performed on an internal secure server within the "Contractor" secure network.
903.3	Public key encryption is used when emailing attachments that contain sensitive information between "Contractor" locations.

Access Control and Privilege Management

- ***Overview***

Information technology and information are strategic assets and therefore it is crucial to properly control access in order to minimize the security risks to the organization. As such, access management is equally crucial as a primary line of defense to prevent unauthorized access and protect the integrity, availability, confidentiality and privacy of information/data assets. The objective of this policy is to provide effective access management policies as the basis for managing information system resource privileges based on the principle of "need-to-know".

- ***Purpose***

This policy is aimed at providing direction regarding the secure design and implementation of information system access control mechanisms and requirements. A formal and consistent approach for managing access privileges is a necessary component of an overall information security program to ensure privileges are consistent with business and security requirements.

Some specific components of this policy include:

- Proof of identity;
- Recording of accountability of actions which can be used for audit purposes;
- Management control over access to data and systems depending on authorization prescribed by the classification of the data and system, and defined privileges of the user role;
- User access management (addition/change/removal of access privileges);
- Segregation and appropriateness of access control, prescribed by Management, for the Development, Acceptance Test, and Production environments; and
- Periodic review of access controls.

- ***Policy***

Appropriate and adequate security measures shall be in place to maintain the confidentiality, integrity, availability, and privacy of information. The level of security required shall be commensurate with the risk level of the information asset. Logical access shall be restricted by implementing adequate authentication and authorization mechanisms, with access rules based on defined roles. Procedures shall also be in place to keep authentication and access mechanisms effective (e.g. regular password changes).

- **Business Requirement for Access Control**

Access to information/data, IT facilities, and business processes shall be based on business need. Access control mechanisms and processes shall be balanced to permit appropriate access to employees, contractors, and third party users to perform their duties.

- **User Access Management**

A formally coordinated process shall be implemented to manage the lifecycle of user access rights based on their defined function. Rights to information assets shall be authorized by the asset owner, or designate, as part of the formal access management processes at user registration, modification, and deregistration. The asset owner is responsible for ensuring that access is granted on the principle of need-to-know and necessary for the individual to perform their job function. Access rights shall be carefully and regularly monitored and users shall be held accountable for their actions.

When access is no longer required, rights shall be immediately revoked to prevent unauthorized access to "Contractor"'s information assets. Upon termination of employment or contract, employees, contractors and third party users shall have their accounts immediately disabled. As employees are transferred or are assigned new responsibilities, their job functions may change requiring modification of their access rights, based on their new security responsibilities and job role.

Audit trails and logs shall be used to detect any suspicious activities that may indicate unauthorized access attempts to "Contractor" information systems. A record of all privileges allocated, and a log of the audit trails, shall be maintained for future reference.

- ***User Registration***

There shall be a formal user registration, management, and de-registration process in place assigning unique user IDs. Users will be given a written document stating their access rights and responsibilities, a signed copy of which shall be securely retained.

A Generic ID is a shared ID that various users make use of directly. Generic IDs shall be issued on an as needed basis and must be accompanied by an approved business justification, along with limitations on the credential distribution, duration and privileges.

Emergency IDs are those issued to and used by system administrators, or systems support personnel and can only be used once. These IDs must be appropriately controlled and distributed. Issuance of Emergency IDs must be accompanied by an approved business justification, along with limitations on the credential distribution and privileges.

Access rights shall be assigned to defined roles, with users belonging to various roles within groups. Requests for account creation, modification, or removal are provided in writing by the employee's supervisor via an email to the IT Administrator. Access rights will be based on the employee's documented job role and responsibility. The IT Administrator will compare the access request against the roles and responsibility matrix to ensure the access request is appropriate based on the defined job function. Any deviation from the defined job function is to be justified by business need and approved by the ISSO. This request and approval will be recorded and retained in the employee file.

- ***User Password Management***

A secret password is a key component of the logical access control mechanism. With the correct username and password, a user can have access to assigned information assets and resources. Thus, it is crucial that passwords are properly managed by keeping passwords confidential, performing regular password changes, and using quality passwords.

Temporary passwords are those issued to users that must be changed at first logon. These shall be issued at account creation.

User IDs will be created using a defined format of the user's first initial and last name. In cases where there is a duplicate ID, the employee's middle initial will be used (e.g. Brian E. Jackson would be *bjackson*; Brian E. Jackson, Jr. would be *bejackson*). Requests for access shall follow the defined formal access management process to require the request submitted electronically or in writing and include:

- Employee name;
- Job title;
- Manager's name;
- Access rights requested; and
- Appropriate approvals.

- ***Review of User, System and Application Access Rights***

The business manager, or designate, shall review user access rights at the system and application levels on a quarterly basis, using a formal process to ensure that access privileges are appropriate. A record attesting to this review shall be maintained. The employee's supervisor must notify Human Resources of any changes in the employee's job responsibilities. A request for changing existing user accounts or access rights (position or responsibility change) must be coordinated with Human Resources and the IT Administrator for the employee role change. Dissemination of the user ID and an initial temporary password must be communicated to the user in person by their immediate supervisor or via the telephone if the employee and their immediate supervisor are in separate locations. The IT Administrator must acknowledge their receipt and approval of the access request form through a signature, or email confirmation. This record will be included in the formal User Request Record. User requests must be kept on file along with the employee file maintained by Human Resources.

The employee's supervisor must notify Human Resources of the employee's intent to leave if the departure is voluntary. For terminations, the employee's supervisor, IT Administrator, and Human Resources will coordinate the account closure time and date in coordination with the employee's final day. The employee's supervisor or Human Resources must submit a request electronically or in writing for the removal of the access rights to the appropriate IT Administrator with the last date of access documented. The IT Administrator must remove all access to files on the date specified on the request. The IT Administrator must acknowledge through a signature, or reply email once the request is completed. This request and record will be submitted for retention in the employee file with Human Resources. On a quarterly basis, the Human Resources master list of employees who have left the company must be compared against the access rights list to ensure that terminated employees no longer have active accounts. Any access that is deemed inappropriate must be updated, disabled and/or removed immediately.

- **User Responsibilities**

Users shall be made aware of their responsibilities in contributing to the security of the information assets and their accountability for the use of their electronic identity and password. This awareness shall be provided as part of a formal user awareness program.

- ***Clear Desk and Clear Screen***

A clear desk involves securing sensitive material, regardless of the form in which it exists (for example paper or electronic), from the desk so that it is not accessible to unauthorized parties. Documents and other information materials shall be organized on the desktop to ensure that its security is maintained and only visible to authorized entities.

Based on a similar strategy, a clear screen entails locking the computers, with a screen saver for example, when away from the computer for a period of time. Other measures include standing next to the printer while sensitive material is being printed, and storing critical information assets in safes or other forms of secure storage.

The clear desk practices shall be followed to ensure that information assets and customers information is kept private and confidential, as required by "Contractor". Customer data is never to be copied to portable storage devices for convenience. Customer data only resides on secure servers when in use, and encrypted backup media when in archive. Customer data shall not be exposed on the desktop environment at any time without supervision.

- ***Passwords***

Passwords are considered confidential information and users are responsible for their protection. Strong passwords are to be used. Parameters for strong passwords include:

- Relatively easy to remember;
- Not based on something someone could easily guess or obtain using personal information (e.g. birth date, telephone numbers, names, etc.);

- Of sufficient length to require significant brute force effort to guess;
- Not vulnerable to dictionary attacks; and
- Free of consecutive identical, all-numeric or all-alphabetic characters.

All passwords, excluding service accounts (e.g. printer controllers), or accounts that have non-expiring passwords will be set to expire every 90 days. Vendor supplied default passwords must be changed. A password must be changed immediately if there is a suspicion it has been compromised. Users must change their password when signing onto a system for the first time. Screen savers with password protect must be enabled and set to lock computers that have been inactive for a maximum of 30 minutes. User accounts will be locked after 3 consecutive failed logon attempts within a 30-minute wait period. An audit trail providing the date of the last successful user logon must be recorded. Password history is set to remember the last 8 passwords.

- **Network Access Control**

Access to both internal and external networked services shall be controlled. The following controls and mechanisms shall be implemented to prevent compromise of network services and information assets:

- Design and configuration of secure interfaces between the "Contractor" network and other networks to which it is connected (e.g. public networks such as the internet);
- Implementing the proper authentication mechanisms for both users and their equipment;
- Controlling and monitoring access to, and availability of, information assets;
- Special controls shall be established to safeguard the confidentiality and integrity of data passing over public accessible networks according to their classification. Refer to the *Data Classification Policy* for details on the necessary controls according to classification; and
- Appropriate logging and monitoring shall be designed and implemented to enable recording of security-related actions.

- ***Cabling Security***

Power and telecommunications cabling carrying data or supporting information services shall be protected from compromise to the security of the transmissions due to threats such as interception or damage. Specifically for infrastructure cabling, the following shall be implemented:

- Network cabling shall be protected using a conduit or by avoiding routes through public areas;
- Utilize good housekeeping practices to ensure that cables are clearly identifiable and equipment markings are used to minimize handling errors, such as accidental patching of wrong network cables; and
- Disabling of access points when not in use or authorized for use.

- ***Equipment Identification in Networks***

Unique identifiers (i.e. asset tags, serial number, MAC addresses, etc.) shall be assigned to, or recorded from, each information processing, storage, and computing asset. This identifier will be used to verify the identity of the equipment to ensure only authorized equipment can connect with "Contractor" IT resources using current connection protocols. The use of automated tools to identify equipment shall be considered as a means to monitor and authenticate connections from specific equipment, or defined locations within the various facilities.

- ***Segregation in Networks***

The network infrastructure shall be designed and configured into separate network domains, each with its own security boundary. Access controls can then be defined for the network domains at a more granular level to further refine the network security rules, e.g. accessible only to the HR department or available to all employees. Users will be granted access to those domains based on business requirements. Segregation of the network into domains shall be based on business needs. If a given domain contains sensitive information, then it shall be protected from other users to reduce security risks, based on the need-to-know principle. The following domains have been defined.

Administrative Segment - This segment has the lowest level of security and can be accessed by all "Contractor" personnel.
Production Segment – This segment is considered high-security and is isolated from any outside network (e.g. Internet).
Data Services Segment – This segment is considered high-security to limit access to "Contractor" customer data.
DMZ Segment – The Demilitarized zone segment is to isolate traffic from connecting to the internal

network

- ***Perimeter Security***

Firewalls protect segments of the network such as DMZ and Data Services. Using firewalls as part of the internal network security solution provides additional layers of access control and containment. Adding firewalls to the information technology infrastructure enables enterprises to protect specific resources. This occurs by forcing traffic to authenticate as they move from segment to segment. In addition to user containment, internal firewalls add attack containment to the network to prevent damages from spreading.

Remote access to the "Contractor" network requires VPN technology and client software. Requests for VPN access shall follow the standard access control process to include authorization by IT and requesters supervisor, and kept on file. The VPN connection must be used for business purposes only. Users must have virus protection, spy ware protection, and a personal firewall enabled on the desktop/laptop that will be used to remotely access the network. The user will be automatically disconnected from the VPN after 30 minutes of inactivity and must login again to connect. Access rights to the VPN will be reviewed on a quarterly basis to ensure appropriateness.

Reconfiguration of a remote user's equipment for the purpose of split-tunneling or dual homing is not permitted. User must use the appropriate VPN Client software provided by "Contractor".

- **Operating System Access Control**

The IT facilities shall be secured to restrict access to the operating systems from unauthorized users by utilizing strong authentication. Systems must also retain a record of user activity to include successful and failed logins, and the use of any privileged access rights. Alarms must be raised when security has been breached. Where deemed appropriate, connection times of users may be restricted, as set by the access control policy. Refer to system access control standards for further detail on specific logon procedures, logging and detective control mechanisms.

- ***User Identification and Authentication***

There must be a suitable authentication method in place at the network entry point (i.e. network perimeter) to verify the identity of the user. The type of authentication method used shall be commensurate with the criticality of the information asset to be accessed and in accordance with the Access Control Policy.
Systems containing information that is classified as Restricted requires multi-factor authentication systems.

- ***Use of System Utilities***

Certain system software is capable of overriding the system and application controls in place and represents a potential threat to the security of information assets. Therefore their use shall be strictly controlled and monitored. A record of all system utilities installed shall be kept, and a log of their use shall also be maintained. Only approved system utilities shall be used when authorized to do so, and they must be removed or disabled once they are no longer required.

- ***Session time-out***

To prevent unauthorized access to unattended equipment, a time-out control will be implemented into consoles to deactivate the session after idle time. The user will then need to complete the authentication procedure again to gain access to the system. The time-out delay will depend on the security risks of the area, the sensitivity of the information and application being used, and the risks to the users of the equipment. Thus, in high-risk locations, the time-out period would be shorter.

- ***Roles & Responsibilities***

Designated owners shall own Information/data assets and be responsible for defining, and periodically reviewing, access restrictions and classifications, taking into account applicable access control policies and standards. The owner may delegate this responsibility to another associated member of his/her department; however, responsibility still resides with the owner. The designate assumes the role of custodian in this context. The owner, or designate, is then responsible for determining who should be authorized to have access to the information asset based on its classification, see *Data Classification policy*, and job role of the individual user and/or group. This shall be reviewed on a regular basis and the information shall be re-classified, as circumstances require. The information owner must authorize access to the information on a need-to-know basis. The information owner must ensure that the appropriate controls are in place to protect the information and that they are commensurate with its classification level. The owner must investigate any reports of unauthorized access or modification.

- **Policy Descriptions and Policy Number References**

Policy No.	Description of Policy
P100.1	Requests for access are provided in writing by the employee's supervisor. Access rights will be based on the employee's documented job role and responsibility
P100.2	User IDs are unique and follow the "Contractor" naming standards.
P100.3	Each request for the creation, modification or removal of a user ID or access is in electronic format and originates from employee's supervisor.
P100.4	All changes are tracked and kept on file for one year
Policy No.	**Description of Policy**
Creation of User IDs or Access	
101.1	User IDs will be created using a set format of the user's first initial and last name. In cases where there is a duplicate ID, the employee's middle initial will be used (e.g. Brian E. Jackson would be *bjackson*; Brian E. Jackson, Jr. would be *bejackson*). Each user ID must be unique. Access rights will be based on the employee's documented job role and responsibility.
101.2	Requests for access must be submitted electronically or in writing and include the required information: Employee name, job title, manager's name, access rights requested, and appropriate approvals.
101.3	User access rights cannot be modeled after any other user. They may be modeled after a department template.
101.4	User IDs of contractors and temp employees must have an end date specified within their user data.
101.5	Dissemination of the new ID and an initial password must be communicated to the user via the phone only if the user and IT Administrator are offsite.
101.6	IT Administrator must sign the request once the request has been completed.
101.7	User requests must be kept on file for a minimum period of one year.
101.8	The creation of shared IDs for user accounts is prohibited unless appropriate compensating user controls have been implemented and "Contractor" management has provided approval in writing. An example of a compensating control is when the network is segmented so that the user account would not have access to restricted data.
Modification of User IDs or Access	
102.1	The employee's supervisor must notify Human Resources of any changes in the employee's job responsibilities.
102.2	A request for changing user access rights (position or responsibility change) must be submitted electronically or in writing by employee's supervisor to the IT Administrator. Access rights will be granted based upon the new job responsibilities.
102.3	IT Administrator must sign the request once it has been completed.
102.4	User requests for modification must be kept on file for a minimum period of one year.
102.5	A request for changing a User ID (i.e. name change) must be submitted electronically via email or in writing by employee's supervisor to the IT Administrator.
Removal of User IDs or Access	
103.1	The employee's supervisor must notify Human Resources of the employee's intent to leave.
103.2	The employee's supervisor or Human Resources must submit a request electronically or in writing for the removal of the access rights to the appropriate IT Administrator with the last date of access documented.
103.3	The IT Administrator must remove all access to files on the date specified on the request.
103.4	Administrator must sign the request once completed.
103.5	Requests for removal must be kept on file for a minimum period of one year.
103.6	On a quarterly basis, the Human Resources master list of employees who have left the company must be compared against the access rights list to ensure that the employees no longer have access. Any access that is deemed unnecessary must be removed immediately.

Policy No.	Description of Policy
P200.1	"Contractor" employs monitoring software to ensure the guidelines are being followed.
P200.2	Passwords are considered confidential information and users are responsible for the protection of their passwords at all times.
P200.3	In order to protect client data and "Contractor" property '*Strong Passwords' are used*. These passwords and not easily cracked by tactics such as a brute force attack, social engineering or network sniffing.
Policy No.	**Description of Policy**
Creation of Passwords	
201.1	All passwords must be strong passwords with a minimum of 7 characters and contain 3 of the following: uppercase, lowercase, numbers and symbols/special characters. (e.g. s0urc3l1nk!). For example, the password of 'livefish' could be created as 'L1v3f!5h.
201.2	Passwords must not be displayed or stored in clear text.
201.3	Passwords must not be inserted into email messages or other forms of electronic communication, unless encrypted.
201.4	Passwords must be kept secure and never shared.
Password Expiration	
202.1	All passwords, excluding service accounts (e.g. printer controllers), or accounts that have NEP non-expiring passwords i.e. FTP) will be set to expire no less frequently than 45 days.
203.1	Vendor supplied default passwords must be changed immediately unless part of a compensating control.
203.2	A password must be changed immediately if there is a chance it has been compromised.
203.3	Users must change their password when signing onto a system for the first time.
Lockout	
204.1	Screen savers with password protect must be enabled and set to lock computers that have been inactive for a maximum of 30 minutes. Unless other compensating controls have been put in place such as floor production systems.
204.2	User accounts will be locked after 3 consecutive failed logon attempts within a 30-minute period.
History & Logging	
205.1	An audit trail providing the date of the last successful user logon must be created.
205.2	Password history is set to remember the last 8 passwords.
Policy No.	**Description of Policy**
P300.1	Systems containing information that is classified as Restricted cannot be accessed without multi-factor authentication systems.
Policy No.	**Description of Policy**
301.1	Remote access to the corporate network connectivity is via VPN. Utilized between the client software, and VPN firewall.
301.2	Transaction based i.e. credit card communication will use: Public key certificate (or identity certificate - VeriSign): A certificate which uses a digital signature to bind together a public key with an identity The certificate will be used to verify that a public key belongs to an individual or system.
Policy No.	**Description of Policy**
P400.1	Remote access is limited to authorized employees by their supervisor and must be approved by the Information Systems Security Officer (ISSO).
Policy No.	**Description of Policy**
401.1	Requests for VPN access must be electronically requested or in made in writing, must be authorized by IT and requesters supervisor and kept on file for a period of one year.
401.2	Only the user granted access may use the VPN Connection.

401.3	The VPN connection must be used for business purposes only.
401.4	Users must have virus protection, spy ware protection, and a personal firewall enabled on the desktop/laptop that will be used to remotely access the network.
401.5	The user will be automatically disconnected from the VPN after 30 minutes of inactivity and must login again to reconnect.
401.6	Access rights to the VPN will be reviewed on a quarterly basis to ensure accuracy.
401.7	Employees connecting via VPN: must connect using one of the following methods. If connecting via VPN from Corporate equipment: • Must connect using "Contractor" approved VPN software If connecting via VPN from personal equipment: • Must connect using "Contractor" approved VPN software connecting to a specified corporate desktop for remote control of that desktop.
401.8	Reconfiguration of a remote user's equipment for the purpose of split-tunneling or dual homing is not permitted.
401.9	User must install and configure the appropriate VPN Client software provided by "Contractor".
401.10	VPN access will be controlled using a password and login ID. This password will be changed following the password policy.

Information Systems Acquisition, Development, Change, and Maintenance

- ***Overview***

As part of its information security program and/or strategy, the appropriate IT solutions need to be identified, developed or acquired, as well as implemented and/or integrated into the business processes and infrastructure in a secure and managed way. Information systems and infrastructure shall be developed and maintained in a manner that will ensure the accuracy, completeness, timeliness and overall security of the system or infrastructure component. This policy is in place to provide direction to the development and maintenance of secure information systems and infrastructure.

This policy applies enterprise-wide to include all IT areas responsible for supporting business processes of the organization. IT infrastructure includes shared information technology services, application servers and network devices. The policy goal is to provide the basis for IT resource development, change management and security to ensure ongoing reliability and security of these resources in providing continuous support of business processes.

- ***Purpose***

This policy provides direction for integrating security controls in Service Delivery activities to promote long-term planning and security into IT service provisions and alignment with project management office systems development lifecycle (SDLC) methodology. Security shall be a requirement at the early design stage because it is more cost effective to do so at that phase of the change management process as part of the system development life cycle of the service. These controls are required to maintain the confidentiality, integrity, availability and privacy of information, commensurate with the risk to the information assets. Some specific purposes of this policy are:

- Prevent errors, loss, unauthorized modification or misuse of information in applications;
- To ensure the security of system files;
- To ensure that security criteria for integrity and confidentiality of information technology infrastructure components, applications and network devices are in place;
- To ensure that adequate quality assurance reviews are performed for application code to detect vulnerabilities;
- To ensure that security criteria for the acquisition and/or development of applications are in place;
- To ensure that change management requirements for development and maintenance of IT infrastructure components, applications and network devices are considered;
- To control access to development and production data and systems depending on formal change management procedures;

- To ensure integration of information security process into Systems Development Lifecycle ("SDLC");
- To ensure security considerations are integrated into current "Contractor" processes; and
- To ensure security controls over use of production data in development/test environment are in place.

Third party partners/service providers must demonstrate a consistent and compliant SDLC methodology. The policy goal is to ensure that security requirements are included in all system acquisition, development and maintenance on a consistent and reliable basis.

- ***Policy***

As part of the business requirements, security shall be integrated into the design and implementation of information systems. This means that security shall be a critical component of consideration whenever "Contractor" acquires, develops and maintains its information system infrastructure. All security requirements, security criteria, risk management processes, and industry best practices for application development shall be defined and considered at the design of a project and justified, agreed and documented as a component of the business justification for the information system. Security considerations and criteria shall follow each stage of the development lifecycle as part of the quality assurance review process to ensure adequate integrity and access controls are considered.

- **Change Management**

Changes to existing systems shall be carefully monitored through the use of a formal change control process in order to minimize the risks of disruption to internal processes or the integrity of data and processing systems. Any additions or changes to the existing systems shall follow a formal process of documentation, specification, development, testing, quality control, and managed implementation. The process shall include security controls that are implemented to ensure that developers are given access only to those parts of the system required for their work, and that a formal agreement for any change has been reviewed and approved. Separate environments will also be established to ensure the control of development and test code/data for promotion to production. Application and source code will be promoted among the development, test, UAT, and production environment via a managed process that controls promotion to each of the environments. Promotion of application and source code must be approved prior to promotion to each environment involved in the SDLC.

- ***Testing of System***

Whenever there are changes to systems, these changes shall undergo a technical risk review as part of the change record to ensure that they are functioning as expected and that the security controls that are currently in place have not been affected by the change. This post-implementation review shall include a testing of the change for implications to information security as well as functional impacts. This testing can be performed as part of the user acceptance testing, or a specific post-implementation test of the security controls. The results of this test will be documented in the change record testing section.

- ***Outsourced Software Development***

Outsourced software development shall be controlled according to change control standards to ensure that "Contractor" information security policies and business requirements are being met. The software development and maintenance practices of the Third Party software developer shall meet "Contractor" standards and policies for secure systems development. A controls and process review shall be conducted against the Third Party software developer's systems development and maintenance processes to ensure consistency with "Contractor" policies and standards. Refer to *Third Party Policy* for further details.

- ***Release Management***

Changes to information systems services must be coordinated to ensure that all aspects of a service release are considered to address the impact to the organization, both from a technical and non-technical perspective.

- ***Documentation***

Adequate systems design and configuration document must be maintained. This documentation must be kept up to date to accurately reflect the design and configuration of "Contractor" systems. It will be the responsibility of the application owner to ensure that supporting documentation is kept current.

- ***Emergency Changes***

Changes to software and network devices that arise from an immediate need to prevent security vulnerabilities or threats will be expedited based on the severity of the need. The standard change control will apply to this change, as it would for a normal change event. In this case, the formalities of change records will be made after the change has been implemented and the immediate danger has passed. The change will be recorded in the change management system and appropriate approvals will be confirmed in the record along with event results.

The change will follow standard change management process to include testing, and promotion to production in a controlled fashion.

- **Correct Processing in Applications**

Appropriate controls shall be designed and implemented in applications to ensure the reliable processing of data. This shall ensure the integrity of input, internal processing and output data through the effective deployment of application integrity control standards documentation for input validation, internal processing, and output validation controls. The integrity of these controls and features are tested during post-implementation evaluations to determine that the application design is consistent with the requirements definition and reliable. Post-implementation testing requires the validation of expected output from the new system with actual output from the new system. Procedures will be defined to perform this as a component part of the SDLC process.

- **Security of System Files and Production Data**

Access to system files and program source code shall be strictly controlled to maintain the integrity of the system. Special care shall be taken to avoid exposing sensitive and/or production data to the test environment to prevent corruption or inadvertent disclosure. Production data in native form used in the User Acceptance Testing or Development environments shall be protected at the same level as the Production environment. Test data that has been sanitized or scrubbed to render the data anonymous does not require the same level of protections as the Production environment.

- **Cryptographic Controls**

Encryption is one of the most widely used mechanisms to protect the confidentiality of information. Cryptography is the science of scrambling messages or information into generally unreadable code or ciphers such that only those with the correct "key" have the ability to decode the message. The underlying principle supporting cryptography is the use of a secret key that is shared among the limited parties involved in the sharing of confidential information. Only these parties have access to the shared secret "key" that is needed to both encode the message and then decode the message. This technology ensures that only those parties that have the secret key are able to read the coded message and therefore maintain the confidentiality of the message among the privileged parties. Encryption employs the use of cryptographic algorithms to scramble the message or information. The process for determining whether encryption is an appropriate control mechanism for protecting the confidentiality of information or data lies with the information owner's classification (based on direction from the Data Classification policy). The security requirements, which are based on the sensitivity of data, where it resides, and how it is transmitted for both the internal and external domains, will use the encryption standard defined. The use of encryption technologies to encode and decode messages and information is a necessary component of a security program/strategy to ensure compliance with regulatory, legislative requirements, and corporate objectives.

On any platform or environment that a cryptographic key is required, all symmetric and private asymmetric keys must be kept secret. All key management procedures must be fully documented and rigorously followed. All keys must have a finite lifetime. Various criteria can be used to determine how often a key should be refreshed. The boundaries of the application of the policy incorporate rules for keys and good key management, including the following aspects:

- The key length must provide the necessary level of protection;
- Keys must always be securely stored and transmitted;
- Keys must be randomly generated, unpredictable and use the full spectrum of the key space;
- Keys lifetime must consider the sensitivity of the data that it is protecting (i.e. the more sensitive the data, the shorter the key lifetime should be);
- Key lifetime must consider the frequency of key use;
- All Master Keys must be securely backed up or escrowed in case of emergencies; and
- Keys must be properly destroyed at the end of their use.

- ***Policy***

Information, when stored or transmitted, shall be encrypted, as required, according to the requirements of its information classification and/or owner needs. All encryption products and processes must be configured to "Contractor" standards prior to use. For information classified as Restricted, that is backed-up onto electronic storage media for off-site storage, the entire electronic storage media must be encrypted before sending off-site.

- ***Key Management***

All shared secret or private encryptions keys shall be keep confidential and protected from unauthorized access by the individuals assigned the keys. Each cryptographic key must have an identified owner, with individuals within that business unit identified to authorize use and management of the key. Cryptographic keys must be classified according to Key Classification standards, which define their confidentiality, integrity and availability requirements. No sharing, copying or using of these keys is allowed by anyone other than those assigned responsibility for the keys. The keys shall at all times be protected from unauthorized access or use. Any and all transfer of keys will be accomplished using authorized and secure methods.
The use of asynchronous key encryption technologies and mechanisms will be governed by an identified *Certification Practice Statement* (CPS) and applied using a defined *Certificate Policy* (CP), as required.

- ***Encryption Algorithms, Encryption Key Size, and Change Frequency***

Only approved cryptographic algorithms and associated size of the encryption keys shall be used. Frequency of key changes shall be consistent with the key size. Larger key sizes do not require as frequent a key change as a smaller key size. Key change frequency will be consistent and in compliance with the data classification and resulting security requirements. Additionally, key change frequency will also be consistent and in compliance with the legislative or regulatory needs that the data supports or is party to. All keys must have a predefined lifetime and must be changed according to the defined change frequency. A key must be replaced with a new key within the time deemed feasible to determine the old key (for example, within the time to perform a successful dictionary attack on the data enciphered under the key).

- ***Generation***

An independent party (e.g. Audit) must be present to verify the procedures are followed when master/root encryption keys are generated/loaded as part of the initialization of an encryption system. Secret/private keys must be generated using a process such that it is not possible to predict any resultant value or to determine that certain values are more probable than others from the total set of all the possible values. When generating public/private key pairs for individual users, distinct sets of public/private key pairs must be generated for different business functions. When generating public/private key pairs for system components, separate sets of public/private key pairs must be generated for different business activities. Key components must be generated in a secure location using a secure hardware device approved by current industry standards.

- ***Distribution / Activation When Received***

For symmetric encryption keys that are distributed manually to facilitate subsequent transmissions of an encrypted message, the following controls are required when handling cleartext encryption keys:

- Encryption keys must be split into separate key parts;
- Manual distribution and input of key parts must conform to principles of dual control and split knowledge; and
- Key parts must be distributed over a channel that is different than the channel used for transmitting information protected under the encryption key.

A mechanism must exist which will verify accurate key entry when a key is entered manually. "Contractor" must retain sole custody of the following keys, and they must never be distributed to an external entity, including business partners:

- "Contractor" Master Keys;
- "Contractor" Private Signing Keys; and
- "Contractor" Customer PIN Generation/Verification Keys.

- ***Storage / How Authorized Users Gain Access***

Private asymmetric keys and symmetric keys shall only exist in the following secure forms:

- As cleartext inside the protected memory of a tamper-resistant cryptographic device;
- As ciphertext outside the protected memory of a tamper-resistant cryptographic device;
- As cleartext outside the protected memory of a tamper-resistant cryptographic device as long as it is composed of two or more key components and is managed using the principles of dual control and split knowledge; and
- Plaintext secret/private keys whose compromise would affect more than one party must exist only within a secure cryptographic device. Plaintext secret/private keys whose compromise would affect only one party must exist only within a secure cryptographic device, or a physically secure environment operated by, or on behalf of, that party.

Cleartext key components must be physically managed according to Safekeeping Standards and Procedures.

- ***Use***

- A key must be used for one specific cryptographic purpose only.
- A cryptographic key must be used only for the purpose for which it was originally intended.
- Cryptographic keys must not be shared. That is, apart from public keys, an instance of a cryptographic key must be used only by one business area and for only one role within that business area.
- Production keys must never be used in test or development.

- ***Dealing with Compromised Keys***

- Use of a key must cease when its compromise is known or suspected. Such a key must be changed immediately and a new key generated.
- A process must exist for emergency changes of cryptographic keys, which fail or have been exposed or otherwise compromised. If a key cannot be changed immediately, the service it protects must be suspended.
- Cryptographic keys encrypted under or derived from a compromised key must be changed immediately.
- A compromised key must not provide any information to enable the determination of its replacement.

- ***Destruction***

- Printed plaintext key components, printed key cryptograms and delivery envelopes that are no longer required must be destroyed immediately by crosscut shredding, burning or pulping.
- Plaintext key components and key cryptograms stored on other media must be destroyed such that it is impossible to recreate them by physical or electronic means.

- ***Logging / Auditing Key Activities***

Systems must implement a mechanism that detects and logs, for periodic review, any unauthorized attempt to access, modify or destroy a cryptographic key or key part.

- ***Key Escrow and Retention***

All utility keys used for encryption/decryption shall be escrowed to allow read access to information and data. All third party providers that employ encryption technologies in the processing of "Contractor" data must provide all utility keys used for encryption and decryption of this data to "Contractor" for storage and archiving. Key escrow does not apply to signing keys used for digital signatures. "Contractor" will be the owner of all keys in Escrow that are used to manage "Contractor" data. Encryption keys shall be retained for the duration consistent with the data it is used to decrypt.

- ***Roles & Responsibilities***

Secure system development and maintenance is crucial in minimizing risks associated with systems integrity and availability. It is the responsibility of each asset owner to determine and enforce the security requirements of their assets and systems, based on the organizational security policy.

Responsibility for any of the above may be delegated where appropriate but the accountability remains with the information owner.

Incident Management

- ***Overview***

To respond effectively to unintended events an information security incident response and monitoring capability must be in place. This function detects and responds to events that are not planned and may affect "Contractor"'s ability to perform normally. Since unintended events may have a material impact on operations, it is essential to ensure that incidents, irrespective of their importance, are properly detected, reported, recorded, and responded to.

- ***Purpose***

This policy establishes the requirements for incident response and monitoring and forms a strong component of the information security program/strategy in detecting and reacting to security breaches or other events impacting information assets or resources. This policy will:

- Ensure that events and/or detected weaknesses associated with information systems are communicated promptly such that corrective action is taken in a timely manner;

- Ensure a consistent and effective approach is applied to the management of information security incidents;
- Require centralized reporting of security incidents;
- Provide the definition of roles and responsibilities for responding to and managing incidents;
- Identify the requirement for monitoring capabilities;
- Outline the appropriate communication of information, lessons learned, and other inputs to the continuous improvement effort following a security incident; and
- Outline the responsibility for maintaining exposure metrics and/or criteria for assessing impact of incidents.

This policy will apply enterprise-wide and integrate into existing business and information technology processes, as well as, user awareness and education programs.

- ***Policy***

The policy goal is to ensure the impact of a security breach or other unplanned event is minimized, contained, and appropriate steps are efficiently taken to restore services to normal operation in a timely and predictable manner.

- **Reporting Information Security Events and Weaknesses**

Employees, contractors and third party users shall be aware of the incident reporting procedures in place at "Contractor", and "Contractor" shall train employees and contractor users on the proper procedures to follow for incident detection and reporting. Training content will allow the individual to recognize an incident, and contain the incident by responding accordingly. This training and education will be provided as part of the information security awareness training. Third party users must demonstrate annually that a similar process exists within their respective organization, consistent with the "Contractor" program.

- **Management of Information Security Incidents**

Reported incidents shall be managed through a centralized process that incorporates classification of the incident, response (containment, chain of custody, investigation and examination), monitoring, evaluating, escalation, and overall incident management. This process shall be designed to ensure that the admissibility and weight of evidence rules are applied. For additional information on admissibility and weight of evidence rules, please refer to local *Collection of Evidence* resources. A repository shall be maintained to ensure accurate capture, review and reporting on incidents.

- ***Monitoring Capabilities***

Automated or manual detective control mechanisms shall be integrated into processes to allow for proactive monitoring capabilities for incidents that may occur as part of normal business operations. These mechanisms will provide the required information for the incident response process to record and respond in a timely manner to maintain normal business operations.

- ***Impact Analysis***

The management of information security incidents will involve a process to assess the impact of the incident against normal operations to qualify and/or quantify the potential for loss. This information will be reported by the incident response team as part of the incident management process to justify the response plan and for future reference.

- ***Incident Analysis***

The management of information security incidents will involve a process to analyze and catalogue events for correlation against past events. This information will be used to identify recurring or systemic issues with current information security controls.

- ***Roles & Responsibilities***

The protection of information assets is the responsibility of every "Contractor" employee, contractor and third party and shall be incorporated into the normal work environment. It is a management responsibility to ensure that incidents are dealt with, on an efficient and timely basis. A formal incident response contact list will be provided in the incident response program and process that will be kept current by performing quarterly validation of the individuals and their contact details. This list will also be present in the BCP and DR documents for escalation purposes, where appropriate.

Business Continuity Management

- ***Overview***

Management must prepare, periodically update, and regularly test a business continuity plan that specifies how alternative facilities will be provided so the business can continue operations in the event of an unplanned interruption.

A business contingency plan deals with facilities and other business matters including computers and communications systems. A computer and communications contingency plan is considerably narrower in scope. This policy is intended to supplement the disaster recovery plans because the business facilities will be necessary if the organization is going to remain operational. The workers who create business contingency plans are often not the same as those who are responsible for systems contingency planning. For example, physical security specialists may create business contingency plans, while information systems technicians may be focusing on system contingency planning. Nonetheless, a policy requiring business contingency planning is needed, especially where subsidiaries and other decentralized management structures prevail.

Refer to the formal Disaster Recovery Plan document for the individual contingency planning for each "Contractor" facility.

Compliance Management

- ***Overview***

Compliance with information security policies is a requirement of an effective information security program/strategy to ensure that risks are managed effectively and appropriately, and legal, statutory, regulatory and contractual obligations are met. It is the responsibility of management to ensure that its personnel, contractors and third parties are following its policies and procedures. Organizational practices shall ensure that an appropriate mechanism is in place to monitor compliance with these requirements and provide a reporting process for review and measurement.

- ***Purpose***

This policy provides the requirements to implement controls to monitor, measure, and report on overall compliance of processes with information security policies. Audit information will be an integral part of all key information technology activities, functions and processes for the purposes of:

- Reconstruction of data in the event of damage or loss;
- Meeting regulatory requirements;
- Meeting business operation commitments;
- Detecting potential security abnormalities;
- Security incident investigation;
- Verification and measurement of the effectiveness of security mechanisms; and
- Auditing processing activity.

Security policies, facilities, processes and procedures are implemented by the enterprise to manage risk. Monitoring of the compliance to the policies will establish accountability for the actions of users. Non-compliance with the policies will increase risk and may result in security exposure that could negatively impact the business. Monitoring of compliance to the security policies is accomplished by:

- Internal program and system reviews;
- Periodic audits of systems;
- Review of security incident reports;
- Periodic or scheduled review of the security controls;
- Detection of unauthorized changes to the security controls;
- Review of failed access attempts (violation reporting); and
- Periodic or scheduled risk assessments.

- ***Policy***

"Contractor" will maintain mechanisms and procedures to monitor compliance to the security policies and require that all deviations and non-compliance with the policies be recorded, and actions taken in accordance with their nature and circumstances. Management shall plan for appropriate resources for policy implementation and enforcement to ensure compliance controls are an integral part of operational processes.

The policy requires an auditable history or trail indicating access, modification and execution activity of users against data and systems and compliance with organizational policies by means of monitoring.

- ***Compliance Mechanism***

Compliance collection and reporting mechanisms shall be integrated into processes and as controls that address and verify compliance with rules, governance and regulatory requirements. Management shall be responsible for establishing reporting mechanisms to monitor and assure compliance with these requirements.

- ***Monitoring Compliance***

To maintain effective internal control and compliance, the "Contractor" Unit ISSO, iSAC, or delegate(s) shall be responsible for the ongoing monitoring and reassessment of the effectiveness of internal controls. The "Contractor" Units shall be accountable for conducting periodic audits to examine the completeness and effectiveness of all internal controls relevant to information security, including adherence to information security policies and standards, applicable legal, regulatory and corporate requirements.

- ***Regulatory and Legislative Compliance (Local and International)***

A defined group is accountable for inventorying and maintaining all applicable regulation and legislation requirements that apply to their business, or customer base. This group will be responsible for working with the business units to ensure that controls are in place to meet these requirements effectively. This group will also be responsible for coordinating mechanism(s) to ensure compliance to these requirements.

- ***Third Parties***

Third parties, and applicable sub-contractors involved in provision of services shall be subject to all requirements under this *Compliance Policy* and the *Third Party Policy*. "Contractor" shall reserve the right to request additional control measures are taken in the protection of its assets. Additional control measures shall be commensurate with the risk assessed in using third parties. "Contractor" management shall reserve the right to undertake compliance or audit reviews of third parties, and applicable sub-contractors involved in provision of services at any time deemed necessary to provide assurance regarding compliance to any and all applicable legal, regulatory and corporate requirements. Third parties, and applicable sub-contractors involved in provision of services shall have in place a mechanism to demonstrate compliance with applicable regulation and/or legislation as part of their established controls reporting as indicated in the service level agreement.

- ***Software Licensing***

Appropriate procedures and monitoring mechanisms shall be in place to ensure compliance with licensed use of software products and other items or services where intellectual property rights apply.

- ***Policy Escalation***

Deviations or non-compliance with the policies must be identified and reported to the immediate manager or CIO. Policy deviation is defined as misapplication or fundamental change in the application of a policy in contradiction to the intent of the policy. Non-compliance is defined as the absence of the application of the statement or intent of a policy.

- ***Roles & Responsibilities***

Business Units are responsible for formulating, developing, documenting, promoting and implementing controls. iSAC is responsible for overseeing the compliance program that provides assurance over effectiveness of controls.

ADDENDUM (as applicable)

Cybersecurity and Protecting Sensitive Information

The full text of the tasks are described, as follows:

Task A - Personally Identifiable Information Contract Closeout

(a) *Definition.* Personally Identifiable Information (PII) - as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, PII refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

(b) *Certification of Sanitization of RRB-provided and RRB-Activity-Related Files and Information (including but not limited to all records, files, and metadata in electronic or hardcopy format).* As part of contract closeout, the Contractor shall submit a *Certification of Sanitization of RRB-provided and RRB-Activity-Related Files and Information* to the Contracting Officer and the Contracting Officer's Representative (COR) following the template provided in Appendix G of National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization Revision 1,* which assesses risk associated with Personally Identifiable Information (PII) that was generated, maintained, transmitted, stored or processed by the Contractor. The Chief Privacy Officer (CPO) shall review the Certification and coordinate with the Contracting Officer and the COR.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task B - Contractor Return of all RRB-Provided and RRB-Activity-Related Information

(a) Within thirty (30) days (or a different time period approved by RRB) of an RRB request, or after the end of the contract performance period, the Contractor must return all originals of all RRB-provided and RRB-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must return originals obtained while conducting activities in accordance with the contract with RRB; or distributed for any purpose by the Contractor to any other related organization and/or any other component; or received from the Contractor by any other related organization and/or any other component. Contractors must return all originals so that they cannot be used for further business by Contractor.

(b) Concurrent with the return of all originals as set forth in paragraph (a), the Contractor must document to the RRB the return of all originals of all RRB-provided and RRB-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must document originals obtained while conducting activities in accordance with the contract with RRB; or distributed for any purpose by the Contractor to any other related organization and/or any other component; or received from the Contractor by any other related organization and/or any other component.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task C - Verified Secure Destruction of All RRB-Provided and RRB-Activity-Related Information

(a) Within 60 days after the end of the contract performance period or a time period approved by RRB, or after the contract is suspended or terminated by RRB for any reason, and after RRB has accepted and approved the Contractor's return of information, the Contractor must execute secure destruction (either by the Contractor or third-party firm approved in advance by RRB) of all existing active and archived originals and/or copies of all RRB-provided and RRB-activity-related files and information (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with RRB; or distributed for any purpose by the Contractor to any other related organization and/or any other component; or received from the Contractor by any other related organization and/or any other component. Destruction Methods shall be by procedures approved by RRB in advance in writing.

(b) Within 75 days after the end of the contract performance period or a time period approved by RRB, or after the contract is suspended or terminated by RRB for any reason, and after RRB has accepted and approved the Contractor's return of information, the Contractor must document to the RRB the secure destruction of all existing active and archived originals and/or copies of all RRB-provided and RRB-activity-related files and information, (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with RRB; or distributed for any purpose by the Contractor to any other related organization and/or any other component; or received from the Contractor by any other related organization and/or any other component. Destruction Methods shall be by procedures approved by RRB in advance in writing.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task D - Contractor Return of all RRB-Owned and Leased Computing and Information Storage Equipment

(a) Within 60 days (or a different time period approved by RRB) after the end of the contract performance period, the Contractor must return all RRB-owned and leased computing and information storage equipment to RRB.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task E - Authority to Operate (ATO) Suspension or Revocation

(a) *Definitions*.

(i) Authority to Operate (ATO) - Signed by the RRB chief information officer (CIO), ATOs are issued for all information systems that input, store, process, and/or output Government information. In order to be granted an ATO, all federal information systems must be compliant with National Institute of Standard and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, instead of NIST SP 800-53.

(ii) Information Security Incident - an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(iii) Sensitive Information - As defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where 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 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

(b) In the event of an Information Security Incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this requirement, the Contracting Officer may direct the Contractor to take additional security measures to secure Sensitive Information. These measures may include restricting access to Sensitive Information on the Contractor information technology (IT) system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the Sensitive Information from the Internet or other networks or applying additional security controls.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task F - Security Monitoring and Alerting Requirements

(a) All Contractor-operated systems that use or store RRB information must meet or exceed RRB policy requirements pertaining to security monitoring and alerting. All systems are subject to the requirements of existing federal law, policy, regulation and guidance (e.g., Federal Information Security Modernization Act of 2014). The Contractor must comply with the RRB-used Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) policy for security monitoring and alerting, which includes requirements not limited to:

(1) System and Network Visibility and Policy Enforcement at the following levels:

(i) Edge
(ii) Server / Host
(iii) Workstation / Laptop / Client
(iv) Network
(v) Application
(vi) Database
(vii) Storage
(viii) User

(2) Alerting and Monitoring

(3) System, User, and Data Segmentation

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task G - IT Security and Privacy Awareness Training

(a) The Contractor must ensure that all Contractor personnel complete RRB-provided mandatory security and privacy training prior to gaining access to RRB information systems. Non-compliance may result in denial of system access.

(b) The Contractor must ensure that all Contractor personnel complete security and privacy refresher training on an annual basis. RRB will provide notification and instructions to the Contractor on completing this training.

(c) The Contractor must ensure that each Contractor employee review and acknowledge the *RRB Rules of Behavior* pertaining to appropriate use of RRB information systems prior to gaining access to RRB information systems. The Contractor must also ensure that each Contractor employee reviews these *RRB Rules of Behavior* at least annually. RRB will provide notification to the Contractor when these reviews are required.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task H - Specialized Information Security Training for Staff with Significant Security Responsibilities

(a) The Contractor must ensure that Contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the RRB role-based training program *(program provided after Contract award)*. The objective of the information security role-based training is to develop an RRB information security workforce with a common understanding of the concepts, principles, and applications of information security to ensure the confidentiality, integrity and availability of RRB's information and information systems. The Contractor is required to report training completed to ensure competencies are addressed. The Contractor must ensure employee training hours are satisfied in accordance with RRB Security and Privacy Training Standards *(provided after Contract award)*. The Contracting Officer's Representative (COR) will provide additional information for specialized information security training based on the requirements in paragraph (b).

(b) The following role-based requirements are provided:

[Program office adds role-based requirements; otherwise write "none" or "not applicable"]

(c) The Contractor must ensure that all IT and Information Security personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task I - Federal Reporting Requirements

(a) Contractors operating information systems on behalf of RRB must comply with Federal Information Security Modernization Act (FISMA) 44 USC Section 3541 reporting requirements. Annual and quarterly data collection will be coordinated by RRB. Contractors must provide RRB with the requested information based on the timeframes provided with each request. Contractor systems must comply with monthly data feed requirements as coordinated by RRB. Reporting requirements are determined by the Office of Management and Budget (OMB), and may change for each reporting period. The Contractor will provide the RRB Contracting Officer's Representative (COR) with all information to fully satisfy FISMA reporting requirements for Contractor systems.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task J - Protecting Sensitive Information

(a) Definitions.

(1) Sensitive Information.

As defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where 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 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

(2) Personally Identifiable Information (PII).

PII, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the RRB Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) Sensitive PII.

Sensitive PII refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) Authorization to Use, Store, or Share Sensitive Information.

(1) Through the Contracting Officer, the Contractor must obtain written approval by the Chief Information Officer (CIO) or designee prior to the use or storage of RRB Sensitive Information, or sharing of RRB Sensitive Information by the Contractor with any subcontractor, person, or entity other than the RRB.

(2) The Contractor shall not remove Sensitive Information from approved location(s), electronic device(s), or other storage systems, without prior approval of the CIO or designee obtained through the Contracting Officer.

(c) Information Types. Sensitive Information includes PII, which in turn includes Sensitive PII. Therefore all requirements for Sensitive Information apply to PII and Sensitive PII, and all requirements for PII apply to Sensitive PII.

(d) Information Security Incidents. An *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(1) Information Security Reporting Requirements.

(i) The Contractor must report all Information Security Incidents and Privacy Breaches in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. An information security report shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for Sensitive Information, or has otherwise failed to meet contract requirements.

(ii) The Contractor must report via email all Information Security Incidents and Privacy Breaches to the RRB Service Helpdesk immediately, but not later than 30 minutes, after becoming aware of the Incident. The Contractor shall email the RRB Computer Security Incident Response Team (CSIRT) at CSIRT@RRB.gov, and shall also email the Contracting Officer and Contracting Officer Representative (COR). If the Contractor fails to report in 30 minutes, specific Government remedies may include termination in accordance with RRB Requirement *Termination for Default – Failure to Report Information Security Incident*.

(iii) The types of information required in an Information Security Incident and Privacy Breach reports include: Contractor name and point-of-contact (POC) information, Contract number; the type, amount and description of information compromised; and incident details such as location, date, method of compromise, and impact, if known.

(iv) The Contractor shall not include any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, the Contractor shall use Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information in attachments to email.

(v) If applicable, the Contractor must also provide supplemental information or reports related to a previously reported incident directly to the Contracting Officer, COR and RRB Service Helpdesk at CSIRC@RRB.gov. The Contractor shall include any related ticket numbers in the subject line of the email.

(2) Information Security Incident Response Requirements.

(i) All determinations related to Information Security Incidents and Privacy Breaches, including response activities, notifications to affected individuals and related services (e.g., credit monitoring and identity protection) will be made in writing by authorized RRB officials at RRB's discretion and communicated by the Contracting Officer.

(ii) The Contractor must provide full access and cooperation for all activities determined by RRB to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents. The Contractor shall maintain the capabilities to: determine what sensitive information was or could have been accessed and by whom, construct a timeline of user activity, determine methods or techniques used to access the information, identify the initial attack vector, and remediate and restore the protection of information. The Contractor is required to preserve all data, records, logs and other evidence that are reasonably necessary to conduct a thorough investigation of the Information Security Incident.

(iii) The Contractor is responsible for performing Incident and Privacy Breach Response activities required by RRB, including but not limited to inspections, investigations, forensic reviews, data analyses and processing by RRB and others on behalf of RRB. As requested by the Contracting Officer, the Contractor may provide technical support for the Government's final determinations of responsibility activities for the Incident and/or liability activities for any additional Incident Response activities (e.g., possible restitution calculation to affected individuals).

(iv) RRB, at its sole discretion, may obtain the assistance of Federal agencies and/or third-party firms to aid in Incident Response activities.
(v) The Contractor is responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by RRB.

(e) *Contractor Plan for Protection of Sensitive Information.* The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Upon contract award, the Contractor shall develop and maintain a documentation plan addressing the following minimum requirements regarding the protection and handling of Sensitive Information:

(1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.

(2) Proper control and storage of mobile technology, portable data storage devices, and communication devices.

(3) Proper use of Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information while at rest and in transit throughout RRB, Contractor, and/or subcontractor networks, and on host and client platforms.

(4) Proper use of FIPS 140-2 compliant encryption modules to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

(5) Information Security Incidents. The Contractor shall report to the Government any security incident involving Personally Identifiable Information (PII) of which it becomes aware.

(6) Contractor Access to RRB IT Systems. The Contractor shall configure their network to support access to government systems (e.g., configure ports and protocols for access).

(a) Requirement for Business to Government (B2G) network connectivity. The Contractor will connect to the B2G gateway via a Contractor-procured Internet Service Provider (ISP) connection, and assume all responsibilities for establishing and maintaining their connectivity to the B2G gateway. This will include acquiring and maintaining the circuit to the B2G gateway, and acquiring a FIPS-140-2 Virtual Private Network (VPN)/Firewall device compatible with the Agency's VPN device. Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the Contractor.

(b) Dial-Up ISP Connections are not acceptable.

(c) The Contractor must comply with the Agency's Guidance regarding allowable ports, protocols and risk mitigation strategies (e.g. File Transfer Protocol or Telnet).

(7) IT Security and Privacy Awareness Training. The Contractor must ensure annual security education, training, and awareness programs are conducted for their employees performing under the subject contract that addresses, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering and insider threat for their employees. The Contractor must also ensure employees performing under the subject contract receive the Agency's initial and annual information security awareness training.

(8) The Contractor must not conduct default installations of "out of the box" configurations of Commercially Off the Shelf (COTS) purchased products. The contractor shall configure COTS products in accordance with RRB, NIST, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or Center for Internet Security (CIS) standards. Standards are listed in order of precedence for use. If standards do not exist from one of these sources, the contractor shall coordinate with RRB to develop a configuration.

(f) *Subcontract flowdown*. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task K - Security Assessment and Authorization (SA&A)

(a) The Contractor is required to undergo Security Assessment and Authorization (SA&A); i.e., the process by which a federal agency examines its information technology infrastructure and develops supporting evidence necessary for security assurance accreditation, prior to using information systems to access and/or store Government information, potentially including Sensitive Information. The Contractor's facilities must also meet the security requirements for "moderate confidentiality impact" as defined by the Federal Information Processing Standards (FIPS) 199 publication *Standards for Security Categorization of Federal Information and Information Systems*.

(b) For all information systems that will input, store, process, and/or output Government information, the contractor shall obtain an Authorization to Operate (ATO) signed by the Chief Information Officer (CIO) from the Contracting Officer (working with the Contracting Officer's Representative (COR)) before using RRB information in the system. The contractor may be able to obtain an Authorization to Test from the CIO for the office obtaining services that will allow use of RRB information in certain circumstances to facilitate system development or implementation. Before a federal information system can be granted an ATO, it must be compliant with National Institute of Standard and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (instead of NIST SP 800-53) in order to be granted an ATO.

(c) FIPS 199 moderate confidentiality impact must be utilized for Contractor information technology (IT) systems and security control baseline requirements.

(d) Prior to Agency SA&A activities, the COR must complete a Privacy Threshold Analysis (PTA) for all IT systems. Then the COR must provide the completed PTA to the RRB Privacy Officer for a determination of whether a Privacy Impact Assessment (PIA) is required. If a determination is made that a PIA is required, it will be completed by RRB in accordance with RRB PIA Template instructions.

(e) The Contractor is responsible for preparing SA&A documentation with the use of RRB tools and security documentation templates including System Security Plan, Security Assessment Report, Contingency Plan, and Incident Response Plan. The Contractor must follow federally mandated SA&A and Risk Management Framework (RMF) processes throughout the IT system lifecycle process to ensure proper oversight by RRB. RMF modifies the traditional Certification and Accreditation process and integrates information security and risk management activities into the system development life cycle.

(f) The Contractor must submit SA&A documentation as defined in paragraph (e) to the COR at least 60 days before the ATO expiration date.

(g) The Contractor shall fix or mitigate system or security vulnerabilities within a time frame commensurate with the level of risk (as identified by the RRB and Contractor) they present:

- Critical Risk = 15 business days from vulnerability notification from contractor
- High Risk = 30 business days from vulnerability notification from contractor
- Moderate Risk = 30 business days from vulnerability notification from contractor
- Low Risk = 30 business days from vulnerability notification from contractor

(h) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task L - Contractor System Oversight/Compliance

(a) Pursuant to National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 4, the RRB and GAO have the authority to conduct site reviews for compliance validation and will conduct security reviews on a periodic and event-driven basis for the life of the contract. Full cooperation by the Contractor is required for audits and forensics.

(b) The Contractor shall provide RRB access to the Contractor's facilities, installations, operations, documentation, databases, information technology (IT) systems and devices, and personnel used in performance of the contract, regardless of the location. The Contractor shall provide access to the extent required, in RRB's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of agency data or to the function of information technology systems operated on behalf of agency, and to preserve evidence of information security incidents. This information shall be available to the RRB upon request.

(c) All Contractor systems used in the performance of the contract must comply with Information Security Continuous Monitoring (ISCM) and Reporting as identified in OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*. In addition, RRB reserves the right to perform ISCM and IT security scanning of Contractor systems with tools and infrastructure of RRB's choosing.

(d) All Contractor systems used in the performance of the contract must perform monthly vulnerability scanning as defined by RRB IT and Security Policy, and the Contractor must provide scanning reports to the Contracting Officer, who will forward them to the RRB Chief Information Security Officer (CISO) or designee on a monthly basis.

(e) All Contractor systems used in the performance of the contract must participate in the implementation of automated security controls testing mechanisms and provide automated test results in Security Compliant Automation Protocol (SCAP) compliant data to the Contracting Officer, who will forward to the RRB CISO or designee on a monthly basis.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task M - Contractor Access to RRB IT Systems

(a) Immediately following contract award, the Contractor shall provide to the Contracting Officer's Representative (COR) a complete list of Contractor employee names that require access to RRB information systems.

(b) The Contractor shall provide a Contractor employee change report by the fifth day of each month after contract award to the COR. The report shall contain the listing of all Contractor employees who separated or were hired under the contract in the past 60 days. This report shall be submitted even if no separations or hires have occurred during this period. Failure to submit a Contractor employee change report may, at the Government's discretion, result in the suspension of all network accounts associated with this contract. The format for this report will be provided by the COR.

(c) (1) The Contractor shall require each of its employees who will need system access for six months or less to utilize a Personal Identity Verification-Interoperable (PIV-I) card or equivalent, as determined by RRB, in order to access RRB information technology (IT) systems and Sensitive Information. The Contractor shall ensure that its employees will not share accounts to access RRB IT systems and Sensitive Information.

(2) The Contractor shall require each of its employees who will need system access for more than six months to utilize an HSPD-12 compliant Personal Identity Verification (PIV) card, such as the RRB PIV card, in order to access RRB IT systems and Sensitive Information. The Contractor shall ensure that its employees complete a federal government-initiated background investigation as part of the PIV issuance process. The Contractor shall ensure that its employees will not share accounts to access RRB IT systems and Sensitive Information.

(d) RRB, at its discretion, may suspend or terminate Contractor access to any systems, information/data, and/or facilities when an Information Security Incident or other electronic access violation, use or misuse issue warrants such action. The suspension or termination shall last until RRB determines that the situation has been corrected or no longer exists. Upon request by RRB, the Contractor shall immediately return all RRB information/data, as well as any media type that houses or stores Government information.

(e) The Contractor shall notify the COR at least five days prior to a Contractor employee being removed from a contract (notification shall be at least 15 days for key personnel in accordance with requirement 1552.237-72, *Key Personnel*). For unplanned terminations or removals of Contractor employees from the Contractor organization that occur with less than five days notice, the Contractor shall notify the COR immediately. The Contractor shall ensure that HSPD-12/PIV cards issued to a Contractor's employee shall be returned to the COR prior to the employee's departure.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task N - Individual Notification for Personally Identifiable Information

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the RRB Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) The Contractor shall have in place procedures and the capability to notify any individual whose Personally Identifiable Information (PII) resided in the Contractor information technology (IT) system at the time of an Information Security Incident not later than five business days after being directed by the Contracting Officer to notify individuals, unless otherwise approved by the Contracting Officer. The procedures must be approved by the RRB prior to use. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval, by the Contracting Officer in consultation with authorized RRB officials at RRB's discretion. The Contractor shall not proceed with notification unless the Contracting Officer has determined in writing that notification is appropriate.

(c) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(1) A brief description of the incident;
(2) A description of the types of PII and Sensitive PII involved;
(3) A statement as to whether the PII or Sensitive PII was encrypted or protected by other means;
(4) Steps individuals may take to protect themselves;
(5) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(6) Information identifying who individuals may contact for additional information, including Contractor name and point of contact (POC) and contract number.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task O - Credit Monitoring and Identity Protection

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the RRB Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) *Credit Monitoring Requirements*. In the event that an Information Security Incident involves PII or Sensitive PII, the Contractor may be required to do the following tasks as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described in the "Individual Notification for Personally Identifiable Information" requirement;

(2) Provide credit monitoring and identity protection services to individuals whose data was under the control of the Contractor or resided in the Contractor information technology (IT) system at the time of the Information Security Incident for a period beginning the date of the Incident and extending not less than 18 months from the date the individual is notified; and/or

(3) Use a dedicated call center; or establish one if necessary and as authorized in writing by the Contracting Officer. Call center services provided by the Contractor shall include:

(i) A dedicated telephone number for affected individuals to contact customer service within a fixed time period as determined by the Contracting Officer;

(ii) Information necessary for affected individuals to access credit reports and credit scores;

(iii) Weekly reports submitted to the Contracting Officer's Representative (COR) on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or RRB, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or RRB for resolution, as appropriate;

(v) Preparation of customized frequently-asked-questions-and-answers (FAQs), in consultation as applicable with other parties like subject matter experts and CORs, and that must be approved in advance in writing by the Contracting Officer; and

(vi) Information for affected individuals to contact customer service representatives and fraud resolution representatives for credit monitoring and identity protection assistance.

(c) *Credit monitoring and identity protection services.* At a minimum, the Contractor shall provide the following credit monitoring and identity protection services:

(1) Triple credit bureau monitoring with Equifax, Experian and Transunion;

(2) Daily customer service;

(3) Alerts provided to the individual for changes in credit posture and fraud; and/or

(4) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task P - Compliance with IT Security Policies

(a) Information systems and system services provided to RRB by the Contractor must comply with current RRB information technology (IT), IT security, physical and personnel security and privacy policies and guidance, and RRB Acquisition Regulation 1552.211-79, *Compliance with RRB Policies for Information Resources Management*.

(b) Contractors are also required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA) of 2014, Privacy Act of 1974, E-Government Act of 2002, Federal Information Processing Standards (FIPS), the 500- and SP500- and 800-Series Special Publications (SP), Office of Management and Budget (OMB) memoranda and other relevant Federal laws and regulations that are applicable to RRB.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task Q - Secure Technical Implementation

(a) The Contractor shall use applications that are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB).

(b) The Contractor's standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration.

(c) Contractor applications designed for normal/regular, i.e., non-privileged end users must run in the standard user context without elevated system administration privileges.

(d) The Contractor shall apply due diligence at all times to ensure that Federal Information Processing Standard (FIPS) 199 "moderate confidentiality impact" security is always in place to protect RRB systems and information.

(e) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task R - Internet Protocol Version 6 (IPv6)

(a) In accordance with RRB technical standards, all system hardware, software, firmware, and/or networked component or service (voice, video, or data) utilized, developed, procured, acquired or delivered in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and/or storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, devices and systems shall maintain interoperability with IPv4 products.

(b) Any IP product or system utilized, developed, acquired, produced or delivered must interoperate with both IPv6 and IPv4 systems and products, in an equivalent or better way than current IPv4 capabilities with regard to functionality, performance, management and security; and have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(c) As IPv6 evolves, the Contractor shall upgrade or provide an appropriate migration path for each item developed, delivered or utilized, at no additional cost to the Government. The Contractor shall retrofit all non-IPv6 capable equipment, as defined above, which is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.

(d) The Contractor shall provide technical support for both IPv4 and IPv6.

(e) All Contractor-provided system or software must be able to operate on networks supporting IPv4, IPv6, or one supporting both.

(f) Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance, at no additional cost to the Government.

(g) RRB reserves the right to require the Contractor's products to be tested within an RRB or third-party test facility to demonstrate contract compliance.

(h) In accordance with FAR 11.002(g), this acquisition must comply with the National Institute of Standards and Technology (NIST) US Government (USG) v6 Profile and IPv6 Test Program. The Contractor shall fund and provide resources necessary to support these testing requirements, and it will not be paid for as a direct cost under the subject contract.

(i) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task S - Cloud Service Computing

(a) The Contractor handling RRB information or operating information systems on behalf of RRB must protect RRB information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction per the Federal Information Security Modernization Act (FISMA) and RRB policy.

(b) RRB information stored in a cloud environment remains the property of RRB, and not the Contractor or cloud service provider (CSP). The Contractor may also be the CSP. RRB retains ownership of the information and any media type that stores Government information.

(c) In the event the Contractor is the CSP or can control the CSP through a subcontracting or other business relationship then the following requirements will apply:

(1) The CSP does not have rights to use the RRB information for any purposes other than those explicitly stated in the contract or applicable "Rights in Data" contract requirements.

(2) The CSP must protect RRB information from all unauthorized access.

(3) The CSP must allow RRB access to RRB information including data schemas, metadata, and other associated data artifacts that are required to ensure RRB can fully and appropriately retrieve RRB information from the cloud environment that can be stored, read, and processed.

(4) The CSP must have been evaluated by a Third Party Assessment Organization (3PAO) certified under the Federal Risk and Authorization Management Program (FedRAMP). The Contractor must provide the most current, and any subsequent, Security Assessment Reports to the Contracting Officer's Representative (COR) for consideration by the Information Security Officer (ISO) as part of the Contractor's overall Systems Security Plan.

(5) The Contractor must require the CSP to follow cloud computing contract best practices identified in "Creating Effective Cloud Computing Contracts for the Federal Government" produced by the Federal Chief Information Officer (CIO) Council and Federal Chief Acquisition Officers Council.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task T - Contract Performance Information and Testimony

(a) Dissemination of Contract Performance Information. The Contractor must not publish, permit to be published, or distribute to the public, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. A copy of any material proposed to be published or distributed must be submitted to the Contracting Officer for written approval prior to publication.

(b) Contractor Testimony. All requests for the testimony of the Contractor or its employees, and any intention to testify as an expert witness relating to: (a) any work required by, and or performed under, this contract; or (b) any information provided by any party to assist the Contractor in the performance of this contract, must be immediately reported to the Contracting Officer.

(c) *Subcontract flowdown*. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task U - Rehabilitation Act Section 508 Standards

(a) All electronic and information technology (EIT) procured through this contract must meet the applicable accessibility standards at 36 CFR 1194, unless a FAR 39.204 exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.access-board.gov/sec508/508standards.htm.

(b) The following standards are determined to be applicable to this contract:

(1) 1194.21. Software applications and operating systems
(2) 1194.22. Web-based intranet and Internet information and applications
(3) 1194.23 Telecommunications products
(4) 1194.24 Video and multimedia products
(5) 1194.25 Self-contained, closed products
(6) 1194.26 Desktop and portable computers
(7) 1194.31 Functional performance criteria
(8) 1194.41 Information, documentation, and support

(c) RRB is required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to electronic and information technology for disabled individuals within its employment, and for disabled members of the public seeking information and services. This access must be comparable to that which is offered to similar individuals who do not have disabilities. Standards for complying with this law and any future updates are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board").

(d) Contractor deliverable(s) must comply with these standards.
(e) The final work product must include documentation that demonstrates or provides assurance that the deliverable conforms to the Section 508 Standards promulgated by the Access Board.

(f) In the event of a dispute between the Contractor and RRB, RRB's assessment of the Section 508 compliance will control and the Contractor will make any additional changes needed to conform with RRB's assessment, at no additional charge to RRB.

(g) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task V - Termination for Default - Failure to Report Information Security Incident

(a) Definition. *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(b) If the Contractor was aware of an Information Security Incident and did not disclose it in accordance with the requirements specified in this contract or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.