



CORRESPONDENCE PROCESSING SERVICES

**FINANCIAL SERVICES CENTER (FSC)
DEBT MANAGEMENT CENTER (DMC)**

Date: June 19, 2017

SAC

Task Order PWS Version Number: 1

DRAFT

Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS.....	3
3.0	SCOPE OF WORK.....	3
3.1	ORDER TYPE.....	3
4.0	PERFORMANCE DETAILS.....	4
4.1	PERFORMANCE PERIOD.....	4
4.2	PLACE OF PERFORMANCE.....	4
4.3	TECHNICAL KICKOFF MEETING.....	4
4.4	GOVERNMENT FURNISHED PROPERTY.....	4
4.5	SECURITY AND PRIVACY.....	4
4.5.1	GENERAL.....	4
4.5.2	ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS.....	4
4.5.3	VA INFORMATION CUSTODIAL LANGUAGE.....	5
4.5.4	INFORMATION SYSTEM DESIGN AND DEVELOPMENT.....	7
4.5.5	INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE.....	7
4.5.6	SECURITY INCIDENT INVESTIGATION.....	7
4.5.7	LIQUIDATED DAMAGES FOR DATA BREACH.....	8
4.5.8	SECURITY CONTROLS COMPLIANCE TESTING.....	9
4.5.9	PRIVACY TRAINING.....	10
4.5.10	POSITION/TASK RISK DESIGNATION LEVEL(S).....	11
5.0	SPECIFIC TASKS AND DELIVERABLES.....	13
5.1	PROGRAM REQUIREMENTS.....	13
5.2	PROGRAM Management.....	13
5.2.1	Correspondence Management.....	13
5.2.1.1	Mail Collection and Extraction.....	13
5.2.1.2	Data Capture.....	13
5.2.1.3	File Creation and Transmission.....	13
5.2.1.4	Records Safekeeping and Destruction.....	14
5.3	REPORTING ACTIVITIES.....	14
6.0	GENERAL REQUIREMENTS.....	14
6.1	PERFORMANCE METRICS.....	14

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Management (OM), and Financial Services Center (FSC) is to support the provision of benefits and services to Veterans of the United States. In meeting these goals, FSC strives to provide high quality, effective, and efficient financial services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. FSC is a franchise fund site operated under the Government Management Reform Act, Public Law (PL) 103-356. Consequently, the FSC does not receive Federally appropriated funding and thus is required to market FSC services to customers. As such, the FSC provides financial services to VA, as well as Other Government Agencies (OGAs).

The VA FSC Debt Management Center (DMC) requires correspondence processing services in conjunction with the Federal government lockbox services offered through the U.S. Treasury (Treasury) under the General Lockbox Network (GLN) program. The services are required to process correspondence submitted by Veterans as a result of indebtedness incurred from various Veterans benefit programs. The volume of Veteran mail includes approximately 750,000 pieces of annual debt management correspondence in addition to 200,000 checks, often in the same mail envelope. Due to workload challenges, DMC has encountered difficulty meeting Federal government timelines for processing checks and correspondence. To mitigate this issue, DMC is in the process of establishing a Service Level Agreement (SLA) with Treasury to use the GLN services provided by U.S. Bank for check processing. Correspondence processing services are not within scope of the GLN contract; therefore, a DMC requires a Contractor with expertise with the GLN business operations to provide this specific service.

2.0 APPLICABLE DOCUMENTS

Treasury Financial Manual Chapter 4600 -

<https://tfm.fiscal.treasury.gov/v1/p5/c460.html>

3.0 SCOPE OF WORK

The Contractor shall provide DMC correspondence processing services including mail collection and extraction, data capture, file creation and transmission, records safekeeping and destruction and various daily and monthly reporting. The Contractor shall provide staff with expertise in all areas of GLN business operations including, but not limited to, standardization and operation efficiencies, program management, IT, and customer service.

3.1 ORDER TYPE

The effort shall be proposed on a Firm Fixed Price (FFP) contract.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a 12-month base period with four 12-month option periods.

4.2 PLACE OF PERFORMANCE

4.3 EFFORTS UNDER THIS TASK ORDER (TO) SHALL BE PERFORMED AT THE CONTRACTOR'S FACILITY. TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM.

4.4 GOVERNMENT FURNISHED PROPERTY

N/A

4.5 SECURITY AND PRIVACY

4.5.1 GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

4.5.2 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

Correspondence Processing Services - DMC

TAC Number: TAC-

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

4.5.3 VA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data

Correspondence Processing Services - DMC

TAC Number: TAC-

destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

Correspondence Processing Services - DMC

TAC Number: TAC-

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

4.5.4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

N/A

4.5.5 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

N/A

4.5.6 SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved, the

circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

4.5.7 LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. The Contractor/Subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

Correspondence Processing Services - DMC

TAC Number: TAC-

- 1) Nature of the event (loss, theft, unauthorized access);
 - 2) Description of the event, including:
 - (a) Date of occurrence;
 - (b) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - 3) Number of individuals affected or potentially affected;
 - 4) Names of individuals or groups affected or potentially affected;
 - 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
 - 6) Amount of time the data has been out of VA control;
 - 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - 8) Known misuses of data containing sensitive personal information, if any;
 - 9) Assessment of the potential harm to the affected individuals;
 - 10) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate; and
 - 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
- d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
- 1) Notification;
 - 2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - 3) Data breach analysis;
 - 4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - 5) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
 - 6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

4.5.8 SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

4.5.9 PRIVACY TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - 1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and annually complete this required privacy and security training; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.
 - 2) Successfully complete the appropriate VA Privacy training and annually complete required privacy training;
 - 3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*
- b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals to perform work on this contract. The status reporting shall identify the following: a single Contractor Security Point of Contact (POC), the names of

Correspondence Processing Services - DMC

TAC Number: TAC-

all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date.

The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security".

4.5.10 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task			
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Correspondence Processing Services - DMC

TAC Number: TAC-

Position Sensitivity and Background Investigation Requirements by Task			
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

4.5.11 BACKGROUND INVESTIGATION

The position sensitivity impact for this effort has been designated as **Low** and the level of background investigation is **NACI**. The current cost for this is **\$381.00**.

4.5.11.1 CONTRACTOR'S RESPONSIBILITIES

The Contractor shall bear the expense of background investigations for all contractor personnel.

The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

The following procedure shall be followed for personnel who have received a favorable/unfavorable background investigation:

- 1) FSC accounting staff will issue a Bill of Collection (BOC) letter to the vendor.
- 2) The vendor has 30 days from the BOC issue date to submit payment via cash, check, US postal money order, express money order, or bank draft.
- 3) If payment is not received, interest and penalties provided in the BOC will be added to the BOC amount owed. Follow-up letters will be sent to the vendor if payments are not received in 30 days and will include additional interest and penalties added in.
- 4) Vendor's rights to dispute the BOC are included in the BOC itself.

Please Note: Payments received for BOCs are not applied against the contract obligation and do not require an amendment or modification to the contract.

Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

Further, the Contractor shall be responsible for the actions of all individuals provided to work for the VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident."

4.5.11.2 GOVERNMENT'S RESPONSIBILITIES

The VA facility will pay for investigations conducted by the Office of Personnel Management (OPM) in advance.

The SIC will notify the Contracting Officer and Contractor after adjudicating the results of the background investigations received from OPM.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROGRAM REQUIREMENTS

The Contractor shall provide correspondence management service. Contractor shall provide staff with expertise in all areas of the GLN business operations including, but not limited to, standardization and operational efficiencies, program management, customer service, and technical innovation. Contractor shall have experience in retail and wholesale lockbox processing, staffing methodology, and the ability to meet the technical and processing requirements specified in Section 5.2. Service location must be geographically dispersed to address risk, and have scalability to increase or decrease volume as need during the term of the contract. Contractor shall provide standardized procedures and operations in order to optimize efficiency and output.

5.2 PROGRAM MANAGEMENT

The Contractor shall provide a dedicated support team to success of the DMC. The team shall include a diverse mix of skill sets that corresponds to major aspects of lockbox processing. The Contractor shall perform the following activities:

5.2.1 Correspondence Management

- 5.2.1.1 Mail Collection and Extraction – Mail shall be picked up from the post office in accordance with bank's mail pickup schedule on a daily basis. Mail should be processed within 24 hours of receipt.
- 5.2.1.2 Image Processing/Data Capture – All correspondence and envelopes shall be scanned and all standard metadata shall be captured.
- 5.2.1.3 File Creation and Transmission – A daily image file in the multi-page, searchable PDF format shall be created and transmitted to the Financial Services Center via Secure File Transfer Protocol.

Correspondence Processing Services - DMC

TAC Number: TAC-

- 5.2.1.4 Records Safekeeping and Destruction – All image files shall be stored for a period of 30 days. All documents shall be destroyed 10 days after processing.

5.3 REPORTING ACTIVITIES

A monthly report detailing correspondence receipt volumes shall be provided.

6.0 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none">Shows understanding of requirementsEfficient and effective in meeting requirementsMeets technical needs and mission requirementsProvides quality services/products	Satisfactory or higher
B. Milestones and Schedules	<ol style="list-style-type: none">Quick response capabilityProducts completed, reviewed, delivered in accordance with the established scheduleNotifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none">Currency of expertise and staffing levels appropriatePersonnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	<ol style="list-style-type: none">Integration and coordination of all activities to execute effort	Satisfactory or higher

Correspondence Processing Services - DMC

TAC Number: TAC-

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the TO to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

DRAFT