Department of Veterans Affairs

**Beneficiary Travel Self-Service System (BTSSS) Claim Ingest API**

Interface Control Document

v1.1

August 2022



Document Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Author | Date | Version Description |
| 1.1 | BTSSS Claims API Team | 08/08/2022 | Refinements to Interface Request/Responses |
| 1.0 | BTSSS Claims API Team | 09/20/2021 | Initial Document |

Table of Contents

[Document Version History 2](#_Toc110857006)

[1 Introduction 6](#_Toc110857007)

[1.1 Purpose 6](#_Toc110857008)

[1.2 Scope 6](#_Toc110857009)

[1.3 Business Use Cases 6](#_Toc110857010)

[1.3.1 Submit Claim 6](#_Toc110857011)

[1.4 Department of Defense Architecture Framework (DoDAF) Viewpoints 7](#_Toc110857012)

[2 Systems Definition 7](#_Toc110857013)

[2.1 Systems 7](#_Toc110857014)

[2.1.1 Beneficiary Travel Self-Service System (BTSSS) 7](#_Toc110857015)

[2.2 Systems Diagram 8](#_Toc110857016)

[2.3 Design Assumptions 9](#_Toc110857017)

[2.3.1 System Environment 9](#_Toc110857018)

[2.4 Integration Patterns 9](#_Toc110857019)

[3 System Interface Definition 9](#_Toc110857020)

[3.1 Interface Overview 9](#_Toc110857021)

[3.2 Interface Operations 11](#_Toc110857022)

[3.3 Communication 12](#_Toc110857023)

[3.3.1 Flow Control 12](#_Toc110857024)

[3.3.1.1 Errors 12](#_Toc110857025)

[3.4 Operational Environment 13](#_Toc110857026)

[3.4.1 System Uptime 13](#_Toc110857027)

[3.4.2 Use of Date/Time in Transactions 13](#_Toc110857028)

[3.5 Change Control 13](#_Toc110857029)

[4 Interface Specifications 13](#_Toc110857030)

[4.1 Azure App Services Definition 13](#_Toc110857031)

[4.1.1 RESTful Web Services 13](#_Toc110857032)

[4.1.2 JavaScript Object Notation (JSON) 13](#_Toc110857033)

[4.1.2.1 Claim API JSON Request Body Sample 14](#_Toc110857034)

[4.1.2.2 Claim API JSON Nominal Response Body Sample 15](#_Toc110857035)

[4.1.2.3 Claim API JSON Off-Nominal Multiple Appointments Response Body Sample 15](#_Toc110857036)

[4.1.2.4 Claim API JSON Off-Nominal Claim Exists Response Body Sample 15](#_Toc110857037)

[4.2 Hypertext Transfer Protocol Secure (HTTPS) 15](#_Toc110857038)

[4.3 Cybersecurity Compliance 16](#_Toc110857039)

[4.3.1 Authentication 16](#_Toc110857040)

[4.3.1.1 OAuth 2.0 Authentication 16](#_Toc110857041)

[4.3.1.2 TLS 1.2 16](#_Toc110857042)

[4.3.2 Authorization 16](#_Toc110857043)

[4.3.2.1 OAuth 2.0 Authorization 17](#_Toc110857044)

[4.3.3 Security and Integrity 17](#_Toc110857045)

[4.3.4 Confidentiality 17](#_Toc110857046)

[4.3.5 Interconnection Security Agreement (ISA) 18](#_Toc110857047)

[5 Approvals 19](#_Toc110857048)

[Appendix A: Acronyms and Definitions 20](#_Toc110857049)

[Appendix B: Points of Contact 22](#_Toc110857050)

Table of FIGUres

[Figure 1 – Systems Interface Description – High-Level Architecture View 8](#_Toc110857051)

Table of Tables

Table 1 – Requirement–Use Case–Workflow Mapping 6

Table 2 – Beneficiary Travel Self-Service System (BTSSS) Description 7

Table 3 – High-Level Architecture Component Description 9

Table 4 – Environment 9

Table 5 – Systems-Systems End to End 10

Table 6 – Systems Resource Flow Matrix 11

Table 7 – Common Client Errors 12

Table 8 – Acronym List 21

Table 9 – Points of Contact 22

# Introduction

This Interface Control Document (ICD) describes the Claim Ingest Service Application Programming Interface (API) for the Beneficiary Travel Self-Service System (BTSSS). It identifies the entry points, protocols observed, messages exchanged and data items in the messages. This document also reviews the security considerations that must be upheld for secure data exchange.

BTSSS is a cloud-based Dynamics 365 solution. It provides a more Veteran-focused experience for beneficiary travel reimbursements, allowing claimants to submit and track travel claims at their convenience. BTSSS also provides capabilities for beneficiaries to receive payments by Electronic Funds Transfer (EFT) and to electronically file for mileage reimbursement. BTSSS can be launched using a desktop, mobile device, or smart phone.

## Purpose

The purpose of this ICD is to describe the architecture and interfaces for the submission of Health Information between BTSSS and potential client systems.

This document specifies the interface requirements to be met by the participating systems. It describes the concept of operations for the interface, defines the message structure and protocols that govern the exchange(s) of data and identifies the communication paths along which the data is expected to flow.

## Scope

This document specifies the interface between BTSSS Claims Ingest API and the potential service clients. Upon formal approval of each participating system, this ICD will be incorporated into the requirements baseline for each system. This document details the functional, performance, operational and design requirements for the interface and describes the record layouts for the data that BTSSS expects from the client system. This data is used to create BTSSS claims with mileage expenses. It is intended for all parties requiring such information, including software developers, system designers and testers responsible for implementing the interface.

## Business Use Cases

The systems and interfaces addressed in this document support the following Requirements and Business Use Cases.

| Requirement | Requirement Description | Business Use Cases | Workflows |
| --- | --- | --- | --- |
| Submit Claim for Mileage Expense | Supports the submission of claims processing for mileage expenses without a graphical users interface. | * Submit Mileage Claim |  |

Table 1 – Requirement–Use Case–Workflow Mapping

### Submit Claim

This Use Case describes the workflow that submits a claim for mileage expense. A client system sends a POST request. The POST Claim Ingest Service API responds with the claim ID.

## Department of Defense Architecture Framework (DoDAF) Viewpoints

N/A

# Systems Definition

This section describes the systems that will be accessed by the interfaces defined in this ICD and provides a diagram of how they are connected to each other.

## Systems

The systems that are relevant to this ICD is BTSSS. Systems can leverage APIs to perform the activities that fulfill the business functions outlined in *Section 1.3 Business Use Cases*.

### Beneficiary Travel Self-Service System (BTSSS)

The Beneficiary Travel Self-Service System (BTSSS) is used by beneficiaries to submit travel reimbursements to VA. The Claims Ingest API interface allows for an external system to submit claims for mileage expenses without needing a GUI.

| Field | Value |
| --- | --- |
| System Name | Beneficiary Travel Self-Service System |
| Vendor | Department of Veterans Affairs |
| Description | BTSSS provides a more Veteran-focused experience for beneficiary travel reimbursements, allowing Claimants to submit and track travel claims at their convenience.  BTSSS also provides capabilities for Beneficiaries to receive payments by EFT. |
| Release and Version | v2.3.1 |

Table 2 – Beneficiary Travel Self-Service System (BTSSS) Description

## Systems Diagram

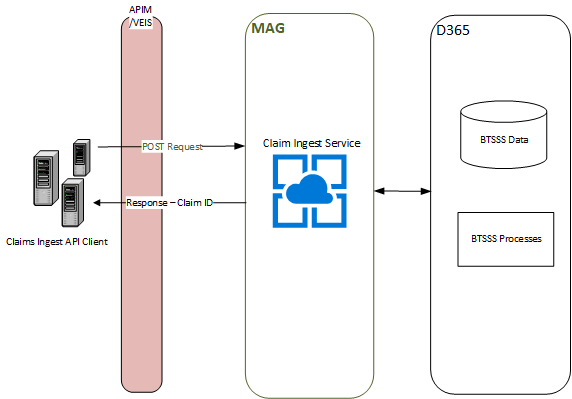


Figure 1 – Systems Interface Description – High-Level Architecture View

Table 3 describes each of the components in this view.

| Component Name | Description |
| --- | --- |
| BTSSS | Provides an intuitive interface for Claimants, such as Veterans and Caregivers, to submit and track their beneficiary travel claims. BTSSS provides a more Veteran-focused experience for beneficiary travel reimbursements, allowing Claimants to submit and track travel claims at their convenience. BTSSS also provides capabilities for Beneficiaries to receive payments by EFT and helps to eliminate fraud, waste, and abuse. |
| BTSSS D365 | The foundation of the BTSSS is Microsoft Dynamics 365, customized for processing Veteran and Beneficiary reimbursement claims for mileage, transportation, meals, and lodging expenses. The BTSSS Claims Management D365 application is internal within the VA firewall used by Travel Clerks and other Veteran Travel Program (VTP) personnel. |
| MAG | BTSSS exposes and App Service serving as an API to interface with BTSSS. Components are implemented as WEB API projects on the Microsoft Azure Gov (MAG) Cloud. |

Table 3 – High-Level Architecture Component Description

## Design Assumptions

* The patient identifier is the Internal Control Number (ICN) received from the Master Person Index (MPI). The BTSSS Claims Ingest API application will use the ICN as the main patient identifier. Future versions of the API might enable the support of Electronic Data Interchange Personal Identifier (EDIPI).

### System Environment

The following table describes the BTSSS Test / Prod Environments.

| **Environment** | **MAG Resource Group** | **Interface Name** | **Interface URL** | **BTSSS D365** |
| --- | --- | --- | --- | --- |
| DEV/TEST | VEIS-DEVTEST-GOV-INTERNAL-INT-EAST-API-RG | claimingestsvc-devtest-btsss-east | https://dev.integration.d365.va.gov/veis/ EC/ClaimIngestSvc/api/ClaimIngest/submitclaim | https://dvagov-btsss-dev2.crm9.dynamics.com/ |
| QA | VEIS-PREPROD-GOV-INTERNAL-INT-EAST-API-RG | claimingestsvc-ppd-btsss-east | https://nonprod.integration.d365.va.gov/veis/ EC/ClaimIngestSvc/api/ClaimIngest/submitclaim | https://dvagov-btsss-qa.crm9.dynamics.com/ |
| PROD | TBD | TBD | TBD | https://dvagov-btsss.crm9.dynamics.com/ |

Table 4 – Environment

## Integration Patterns

N/A

# System Interface Definition

This section identifies and describes the interface operations used to communicate between the systems defined in *Section 2.1*: *Systems*. Detailed interface specifications are provided in *Section 4:* *Interface Specifications*.

## Interface Overview

The Claims Ingest API associated with claim ingest is listed in Table 5.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operation Name | Source System | Target System | Interface Type | Data Domain | Message Type | Batch/  Real Time | Service and Protocol | Security Protocol |
| Submit Claim | TBD | BTSSS | API | Claims | JSON | Real Time | HTTPS | TLS1.2 |

Table 5 – Systems-Systems End to End

## Interface Operations

The following table lists the operations exposed by the API, including details that are provided in the Interface Exchange Matrix. Details for each transaction are provided in *Section 4:* *Interface Specifications*.

| Operation Name | Operation Description | Source System | Target System | Message Type | Message Response Type | Connection Initiator | Port Number |
| --- | --- | --- | --- | --- | --- | --- | --- |
| submitclaim | Client sends a POST request and Claims Ingest Service responds with Claim ID. | TBD | BTSSS | POST | HTTP Response | Client | 443 |

Table 6 – Systems Resource Flow Matrix

## Communication

MAG services provides standard messaging services that support transmission and receipt of data through external interfaces, consisting of the following core component:

* OAuth 2.0-compliant authorization server (OAuth 2.0 Server) checks a user authorization request to access MAG resources and passes an authorization token back to the application if the user is authorized.

### Flow Control

Network Flow Control will follow standard link/transport protocol layer mechanisms used by the Representational State Transfer (REST)ful API interface

The communication relies on acknowledgement messages returned as data to validate receipt and processing of transactions. Communications acknowledgements are the HTTP responses received when data is posted to the destination web server. The response indicates that the payload was delivered to the web server without error. A successful response is represented by an HTTP 200 code and message containing the ID of the newly created claim. If it fails or is rejected, it will return a 204 No Content or a 404 Not Found error code, with error information.

#### Errors

Errors in the context of BTSSS Claims Ingest API are HTTP errors. An error response will be sent to the client with an appropriate message based on the HTTP status code. The common application errors that can be encountered on API calls that receive request bodies is shown below. Additional API specific responses will be added as they are defined.

| Error | Example |
| --- | --- |
| Failing to send a required query parameter will result in a 400 Bad Request response. | HTTP/1.1 400 Bad Request  no supported search parameters provided |
| Requesting the secure endpoint (non-open) without valid credentials will result in a 401 Unauthorized response. | HTTP/1.1 401 Unauthorized |
| Requesting a resource that does not exist will result in a 404 Not Found response. | HTTP/1.1 404 Not Found |

Table 7 – Common Client Errors

## Operational Environment

The Claims Ingest API will be deployed to the MAG as an Azure Service resource and rely on the services levels and infrastructure it provides.

### System Uptime

The system is expected to support the same availability requirements as BTSSS. Availability requirements beyond the control of the interfacing systems (e.g., network availability) are beyond the scope of this ICD.

### Use of Date/Time in Transactions

BTSSS will use Coordinated Universal Time (UTC) for all dates and times exchanged in the interface (e.g., 20190320115200+0000).

## Change Control

Any modifications to this ICD will be coordinated with the appropriate point of contact, as defined in *Appendix C:* *Points of Contact* and will go through a formal change control process. Changes will be subject to agreement between VA and the BTSSS project team. Reference all applicable procedures and tracking mechanisms for agency-specific Change Control Boards (CCBs)—Program Executive Office (PEO), VA Enterprise System Engineering Configuration Control (ESECC), etc.

# Interface Specifications

Additional system interface specifications are provided in the subsections that follow.

## Azure App Services Definition

MAG platform will host the Claims Ingest API as an App Service resource.

### RESTful Web Services

For BTSSS Claims Ingest, content is accessible in JavaScript Object Notation (JSON) format and provides a POST endpoint.

### JavaScript Object Notation (JSON)

JSON is a format that uses JavaScript objects as data. It typically allows the user to use arrays or objects as the request body or response body in web services. JSON objects are denoted between curly brackets (‘{‘ and ‘}’). Fields in a JSON object are denoted by a string identifier, a colon and then a value. The value can be of any of the JavaScript data types. JSON arrays are denoted between square brackets (‘[‘ and ‘]’) and are typically a list of JSON objects but can also be any JavaScript data type.

Azure App Services utilize standard defined media types for JSON content, which are requested via the Accept header.

application/json

#### Claim API JSON Request Body Sample

{

"clientNumber": "1234GVATU",

"claimantID": "1234567890V123456",

"ClaimantIdType": "icn",

"Appointment": {

"appointmentDateTime": "2021-05-01"

},

"mileageexpense": {

"tripType": "RoundTrip"

}

}

Please note the following as far as the payload elements:

* Each client that is integrated with BTSSS will have its own unique value. This ClientNumber will be a value that once onboarded as a recognized client with BTSSS, will be provided by BTSSS.
* ClaimantIDType.  
  "icn" is only option currently supported  
  "edipi" is a future enhancement and not currently supported
* Claimaint ID would be the ID in the format of the ClaimantIDType.  
  Since ICN is currently the only supported option then this is an ICN value.  
  The example above shows a fake example ICN.  
  The ICN format is a 17 alpha-numeric identifier and the format is: 10 digits + “V” + 6 digits.  It’s the VA internal person identifier, and it’s created and assigned by the MPI system when the Veteran is first created in MPI
* Appointment.AppointmentDateTime  
  The current format supported is: "YYYY-MM-DD"  
  Currently, specifying a time for the appointment is not supported.  
  The date is the date the appointment occurred at the site.
* MileageExpense.TripType  
  Two values are supported:  
  "OneWay"  
  "RoundTrip"

#### Claim API JSON Nominal Response Body Sample

{

"value": {

"claimNumber": "TC202207000011666"

},

"formatters": [],

"contentTypes": [],

"declaredType": null,

"statusCode": 200

}

Please note that the value.claimNumber is a string representing the claim number that was created in BTSSS.

#### Claim API JSON Off-Nominal Multiple Appointments Response Body Sample

If a contact in BTSSS has multiple appointments in the same day the behavior is as follows:

Claim request is by day.  If there are multiple appointments found in BTSSS the condition is not currently supported and will result in a 400 Bad Request response and no claim would be created.

{

"currentDate": "[07/29/2022 01:05:41 PM]",

"message": "10/16/2020 : There were multiple appointments for that date"

}

#### Claim API JSON Off-Nominal Claim Exists Response Body Sample

Claims are a one to one – one claim per one appointment.  If a claim already exists a 400 Bad Request response is returned and no duplicate claim would be created.

{

"currentDate": "[07/29/2022 03:28:48 PM]",

"message": "10/16/2020 : This appointment already has a claim associated with it."

}

## Hypertext Transfer Protocol Secure (HTTPS)

BTSSS Claims Ingest API will use HTTPS to exchange data.

## Cybersecurity Compliance

### Authentication

Authentication refers to the process of enforcing a credential that proves the entity (system or person) making the connection is who they claim to be. Authentication also provides the basis for non-repudiation, auditing and accounting activities on a system. Authentication may be layered and is especially important for externally facing or user-facing functions and interfaces. Authentication protocols utilized for service-to-service or system-to-system communication should be utilized to both limit unauthorized connections and to distinguish between different external systems within application logs. The persistence and storage of user/consumer secrets, encryption keys, password and rotation policies and token revocation and expiration periods are important factors to understand when documenting the authentication of an interface, whether user facing or system-to-system. There must always be some level of authentication in place for connections crossing the security boundary of the system.

#### OAuth 2.0 Authentication

The BTSSS Claims Ingest API utilizes the Oauth 2.0 protocol. This authentication process is handled by VAEC and would provide the client ID and Secret which properly identifies users and access to services exposed in the MAG.

Any client wishing to leverage Claim API must have VAEC access. Access can be obtained by submitting an ECSO Intake Request with VAEC by navigating to <https://dvagov.sharepoint.com/sites/OITECSO>.

A client request would require the following info:

A Service Principal (aka app registration) for each environment you plan to call.  This can be done in the same ticket.

The resource group for the apps being accessed:

App: claimingestsvc-devtest-btsss-east | RG: veis-devtest-gov-internal-int-east-api-rg

App: claimingestsvc-ppd-btsss-east| RG: VEIS-PREPROD-GOV-INTERNAL-INT-EAST-API-RG

Once complete the VAEC MAG team will provide the new client with a *name, clientid, and clientsecret.*    
**New clients must not lose their client secret as once it is provided it cannot be viewed or retrieved again.  A new one must be generated which may necessitate additional overhead.**

The BTSSS team will also need to configure and provide a clientNumber which identifies the client system for dev, nprod, and prod environments as appropriate.

#### TLS 1.2

BTSSS Claims Ingest API connections leverage TLS 1.2 protocol. BTSSS Claims Ingest API supports REST and use JSON as the payload format when establishing a secure connection using Transport Layer Security (TLS) over HTTPs to the destination server.

### Authorization

Authorization refers to the process of ensuring that the user identified during authentication is approved to access the system as requested. System and user account authorization access should be limited according to the principles of least privilege whenever possible. Several authorization models exist for software design including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Discretionary Access Control, Mandatory Access Control, and others. There is value in a cybersecurity review to understand the high-level authorization constructs available within the target system.

#### OAuth 2.0 Authorization

VAEC OAuth enables clients to authenticate its processes and then obtain authorized access to MAG resources. Once authenticated, a unique client Id (to be provided when first requesting the use of the service) will be included in each POST request that allows the Claims Ingest API to identify the caller and confirm access to the service is authorized.

### Security and Integrity

The data exchanged through this interface includes Personally Identifiable Information (PII) and Protected Health Information (PHI) and will be protected and safeguarded in accordance with the Health Insurance Portability and Accountability Act (HIPAA), Privacy Act, applicable regulatory requirements, and Department policies. The data also contains Controlled Unclassified Information (CUI) identified as VA sensitive information and will be protected in accordance with the protection standards mandated through the Confidentiality, Integrity and Availability (CIA) levels assigned, as identified in VA Directive 6500 and the Department of Defense Instruction (DoDI) 8510. Each Department shall safeguard the exchanged data, which can only be accessed by authorized personnel with the need to know, to ensure that it is used only for intended purposes and retains its content integrity.

These standards ensure compliance with the following statutes:

* Privacy Act, 5 U.S.C. 552a, implemented by VA at 38 CFR 1.575-1.582
* VA Claims Confidentiality Statute (formal title, Confidential Nature of Claims), 38 U.S.C. 5701, implemented by 38 CFR Section 1.500-1.527
* Confidentiality of Medical Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR Section 17.500-17.511
* U.S. Code, Title 10, Section 1030, Fraud and Related Activity in Connection with the Computer Security Act of 1987
* Health Insurance Portability and Accountability Act (HIPAA)

The MAG provides security through implementation of a Transmission Control Protocol (TCP) socket and use of Hypertext Transfer Protocol Secure (HTTPS) to restrict the exchange of data through creation of a two-way communication link using port, Internet Protocol (IP) address and protocols/services to restrict the flow of data between known points. Each interface is designed using a standard approach specific to the data format and method of secure exchange implemented for that interface.

### Confidentiality

VA must ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of individually identifiable information and records, including PHI and to protect against any anticipated threats or hazards to the security or integrity of such records, which would result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

Transmission security is provided using TLS 1.2 to support exchange of formatted messages and data through an encrypted transmission.

### Interconnection Security Agreement (ISA)

System security considerations:

* **Data Sensitivity:** All Electronic Health Record (EHR) data contains protected health information (PHI) and personally identifiable information (PII).
* **Transport Security Methods:** The security of information passed through this bi-directional connection is FIPS 140-2 compliant. Data is encrypted for exchange using TLS 1.2 configured with digital certificates.
* **User Community:** All authorized users shall have current background investigations and level of trust determination as required by the Departments. Each authorized user will have least-privileged access based on defined roles. Each Department shall compile and manage required user profiles for its user community.
* **Trusted Behavior Expectations:** Each Department expects its users to safeguard sensitive data in accordance with HIPAA, Privacy Act, and applicable regulatory requirements.
* **Security Documentation:** Each Department shall document and maintain system security artifacts and manage system security risks, in accordance with the National Institute of Standards and Technology (NIST), Authority-to-Operate (ATO) reciprocity, interagency risk assessment processes and applicable regulatory authorities.
* **Incident Reporting:** Incident reporting is conducted in accordance with Office of Management and Budget (OMB) Memorandum 17-12, Section 13402 of The Health Information Technology for Economic and Clinical Health Act (HITECH) Act, and the Breach Notification Rule at 45 C.F.R. § 164.400-414.

# Approvals

The undersigned acknowledge that they have reviewed this Interface Control Document and agree with the approach it presents. Changes to this document will be coordinated with and approved by the undersigned or their designated representatives.

|  |
| --- |
| **Michelle Ortiz, BTSSS PM**  **Date Approved:** |

1. Acronyms and Definitions

| Acronym | Definition |
| --- | --- |
| ABAC | Attribute-Based Access Control |
| API | Application Programming Interface |
| App | Application |
| ATO | Authority-to-Operate |
| BTSSS | Beneficiary Travel Self-Service System |
| CCB | Change Control Board |
| CIA | Confidentiality, Integrity and Availability |
| CUI | Controlled Unclassified Information |
| DHA | Defense Health Agency |
| DHMSM | DoD Healthcare Management System Modernization |
| DoD | Department of Defense |
| DoDAF | Department of Defense Architecture Framework |
| DoDI | Department of Defense Instruction |
| ECSO | Enterprise Cloud Solutions Office |
| EDIPI | Electronic Data Interchange Personal Identifier |
| EFT | Electronic Funds Transfer |
| EHR | Electronic Health Record |
| ESECC | Enterprise System Engineering Configuration Control |
| FIPS | Federal Information Processing Standard |
| HIPAA | Health Insurance Portability and Accountability Act |
| HITECH | Health Information Technology for Economic and Clinical Health |
| HTTPS | Hypertext Transfer Protocol Secure |
| IA | Integration Architect |
| ICD | Interface Control Document |
| ID | Identification/Identifier |
| IP | Internet Protocol |
| ISA | Interconnection Security Agreement |
| JSON | JavaScript Object Notation |
| MAG | Microsoft Azure Government |
| MPI | Master Person Index |
| NIST | National Institute of Standards and Technology |
| OAuth | Open Authorization |
| OMB | Office of Management and Budget |
| PEO | Program Executive Office |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| PM | Program Manager |
| RBAC | Role-Based Access Control |
| REST | Representational State Transfer |
| TBD | To Be Determined |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| VA | Department of Veterans Affairs |
| VAEC | VA Enterprise Cloud |
| VEIS | Veterans’ Enterprise Integration Service |
| VTP | Veteran Travel Program |

Table 8 – Acronym List

1. Points of Contact

| Role | Name | Title | Phone and E-mail |
| --- | --- | --- | --- |
| Project Manager | Michelle Ortiz | Interface Project Manager | [michelle.ortiz3@va.gov](mailto:michelle.ortiz3@va.gov) |
| ICD Author | Aaron Kauffman | BTSSS ICD Analyst | aaron.kauffman@va.gov |
| Technical Lead | Lesley Brown | BTSSS Tech Lead | [lesley.brown1@va.gov](mailto:lesley.brown1@va.gov) |

Table 9 – Points of Contact