Internal Revenue Service

Modernization Blueprint

Volume VII - Concept of Operations

November 3, 1997

Internal Revenue Service

Modernization Blueprint

Volume VII - Concept of Operations

November 1, 1997

Table of Contents

List of Charts

VOLUME VII – CONCEPT OF OPERATIONS

INTRODUCTION

I. Introduction

I.A Scope

The *Modernization Blueprint* Volumes I - VI define the Level I and Level II architecture in a manner that provides maximum flexibility for implementation options. The Concept of Operations (CONOPS) intends to bring the *Modernization Blueprint* to life by presenting the workflow and technical implementation characteristics of the architecture. It describes the overall flow of work and data, including a model of the geographic location of functions and applications, the workflow drivers and work processes, security based on workflow and inter- and intra-site connectivity, data locations and general characteristics, and infrastructure components by location. This approach reinforces the architectural concept of complete functional flexibility such that each function can be performed in any location.

I.B Structure

This document is organized at two levels:

- ✦ Operational information is presented for the following:
  - ▲ Work processes and data flows define the various ways the majority of work is performed in the target environment as well as the way data flows between applications and infrastructure components;
  - ▲ Work drivers (mapped to the *Modernization Blueprint* Business Requirements, including performance requirements) define the business events that drive the work processes and data flows;
  - ▲ Data location and characteristics support the work processes;
  - ▲ Security capabilities support the target environment;
  - ▲ Applications (software) support the work processes and data flows; and
  - ▲ Infrastructure components support the applications, computing management and capacity, and data and telecommunications.
- ✦ Modeled site information is presented to provide the geographic distribution support capabilities of the Modernization architecture.

I.C Contents

The *Modernization Blueprint,* Volume VII – Concept of Operations, presents the Modernization architecture at the following two levels:

- ✦ Level I: a high level overview of the work flow, data flow, work drivers, data, security, infrastructure, and applications depicted in the Level I sections of the *Modernization Blueprint*, Volumes III and IV - Functional and Technical

Architecture, including how data and work flow across the geographic topology of the Internal Revenue Service (IRS); and

- Level II: a more detailed description of the work flow, data flow, work drivers, data, security, infrastructure, and applications depicted in the Level II sections of the *Modernization Blueprint*, Volumes III and IV - Functional and Technical Architecture, with the added dimension of the "geographic location" of functions, work, data, security, applications, and infrastructure components.

I.D Site Overview

The *Modernization Blueprint* defines the architecture to be implemented in a diverse geographic topology. In the current environment, stovepipe systems that require a multitude of incompatible hardware and software platforms that do not adequately support the business needs provide a wide variety of tax administrative services.

The Modernization architecture enables the enhancement and expansion of tax administrative services for taxpayers and IRS employees through the centralization of data management and services, business capabilities that can be flexibly deployed in various combinations, and application services delivered to the taxpayer and end user, regardless of their locations.

To bring the *Modernization Blueprint* to life, a model of the baseline target geographic topology is presented in the CONOPS to depict the workflows and processes within the target environment. This model is based on a fixed set of combinations of all the possible capabilities of a site, but it does not represent the entire set of site configurations.

I.D.1 Site Capabilities

Modernization target site capabilities are a mixture of application services, infrastructure services, and functional capabilities combined to provide services to taxpayers and end users. These capabilities, listed below by business function, can be combined to support any IRS location depending on business needs and local conditions.

For example:

- A Submissions Processing Site (SPS) typically supports the Submissions Processing function. Some locations, however, support additional functions such as Customer Service and Compliance.

- Customer Service Sites (CSSs) vary in size and scope and might be co-located with other sites (e.g., an SPS). A Large CSS would support all Customer Service capabilities whereas a Small CSS might support only incoming call, case management, and Management Information Systems (MIS)/Decision Support System (DSS) capabilities.

Possible combinations are limited only by the infrastructure components required to support the capabilities. For example, incoming call capabilities in a CSS can only be provided if the appropriate Regional Call Services (RCS), security management, and regional processors and peripherals connect to Customer Service Call Routing (CSCR) services.

The following sections, organized by the six functions defined in the Functional and Technical Architecture, include the subfunctions (as defined in the Functional and Technical Architecture) traced to manual and automated work activities. The mapped subfunction numbers are listed in parentheses after each item in the following lists.

I.D.1.a Submissions Processing

a) Receipt and processing of paper tax and information returns, remittances, and correspondence (SP.01, SP.04);

b) Receipt and processing of electronic tax and information returns (SP.02, SP.04);

c) Receipt and processing of electronic remittances (SP.02, SP.03);

d) Receipt and processing of electronic correspondence (e.g., electronic mail and voice mail) (SP.02);

e) Issue detection during the processing of the return at the SPS (CO.01, SP.03, SP.04); and

f) Submissions tracking and performance management (SP.05)

I.D.1.b Corporate Processing

a) Validate and post corporate data (CP.01, CP.09);

b) Account settlement (CP.02);

c) Issue detection prior to the issuance of refunds (CP.03);

d) Notice and correspondence generation (CP.04);

e) Refund generation and disbursements to the Department of Treasury (CP.02);

f) Corporate case management (CP.06);

g) Corporate data access (CP.07);

h) Corporate data management (CP.05);

i) Extracts for MIS and DSS (CP.08);

j) MIS and ad hoc reporting (CP.08);

k) Data and application synchronization (CP.05); and

l) Disaster recovery (CP.05)

I.D.1.c Customer Service

a) Issue resolution based on incoming telephone calls (CS.01, CS.06, CS.08, CO.08);

b) Issue resolution based on outgoing telephone calls (CS.03, CS.04, CS.06, CS.08);

c) Issue resolution based on image and/or paper correspondence (CS.02, CS.04, CS.06, CO.08);

d) Issue resolution based on electronic correspondence (e.g., electronic mail and voice mail) (CS.02, CS.04, CS.06, CO.08);

e) Issue resolution based on internally generated cases (CS.03, CS.04, CS.06, CS.08, CS.09);

f) Local case management (CS.07);

g) MIS reporting (CS.09);

h) Decision support (CS.09); and

i) Non-face-to-face Compliance (Compliance and outgoing correspondence for Compliance field activities) (CS.01, CS.06, CS.08, CO.08)

I.D.1.d Compliance

a) Desk examination (CO.02, CO.05, CO.07, CO.09);

b) Field examination (CO.02, CO.05, CO.07, CO.09);

c) Desk collection (CO.05, CO.07, CO.09);

d) Field collection (CO.04, CO.05, CO.07, CO.09);

e) Local case management (CO.06);

f) Research and decision support (CO.03);

g) MIS reporting (CO.10); and

h) Walk-in taxpayer assistance (CS.01, CS.06, CS.08, CO.08)

I.D.1.e Financial Reporting

a) Source data identification and posting (FR.01);

b) Data posting (FR.02);

c) Summary transaction processing and maintenance (FR.03, FR.04, FR.05);

d) General ledger account processing and maintenance (FR.06);

e) Standard financial reporting (FR.07); and

f) Ad hoc financial reporting (FR.08)

I.D.1.f Infrastructure Services

a) Security Management (IS.04);

b) Secure Dial-in (IS.04);

c) RCS including Voice Response, Automated Call Distributor (ACD), and Predictive Dialer Management (IS.05);

d) National Contact Manager (i.e., CSCR) (IS.05);

e) Operations Management (IS.03);

f) Network Management (IS.03);

g) Capacity Management (IS.03);

h) Problem Management (IS.03);

i) Configuration Management (IS.03);

j) Print Farm (IS.05)[1];

k) Transaction Processing Services (IS.05);

l) Message processing (e.g., brokering) (IS.05);

m) Development environment and support (IS.01);

n) Integration test environment and support (IS.02);

o) Systems Acceptance Testing (SAT) environment and support (IS.02);

[1] The site of the Print Farm has not been determined.

p) Workflow Management Services (IS.03);

q) Mainframe processors and peripherals (IS.05);

r) Regional processors and peripherals (IS.05);

s) Desktop processors and peripherals (IS.05);

t) Mobile processors and peripherals (IS.05); and

u) Common Communications Gateway (CCG) (IS.05)

I.D.2 Concept of Operations Sites

The Level I and Level II CONOPS describes the following model site types and associated site capabilities.

Site Type	Submissions Processing	Corporate Processing	Customer Service	Compliance	Financial Reporting	Infrastructure
SPS	a, d, e, f				a	a, b, c, k, l, p, r, s
Primary Computing Center (PCC)	b, c	a, b, c, d, e, f, g, h, j			b	a, d, e, f, g, i, k, l, p, q, r, s, u
Large Customer Service Site			a, b, c, d, e, f, g, h, I		a	a, b, c, k, l, r, s
Small Customer Service Site			a, b, c, d, e, f, g, h, I		a	a, c, r, s
District Office (DO)				a, b, c, d, e, f, g, h	a	a, c, r, s, t
Large Post of Duty (POD)				a, b, c, d, e, h	a	a, c, r, s, t
Small POD				a, b, c, d, e, h	a	a, c, r, s, t
National Office/New Carrollton					c	a, e, f, g, r, s
Other Computing Centers (OCCs)		i, j, k, l	g, h	g, h	c, d, e, f	a, e, f, g, h, k, l, m, n, o, q, r

VOLUME VII – CONCEPT OF OPERATIONS

WORK PROCESSES AND DATA FLOWS

II. Work Processes and Data Flows

Chart II-1, Modernized Target - Geographic Topology Model, depicts a model of the Level II modernized environment across the entire enterprise. Each block represents a typical site type and includes the primary technical and functional capabilities of the site as well as the interconnectivity between other sites. The technical and functional capabilities, such as the Enhanced Regional Infrastructure System (ERIS), the RCS, and the Customer Service capabilities are the building blocks used to construct a site based on local needs, employee density, and conditions. This section describes the work processes and data flows within and between modeled sites.

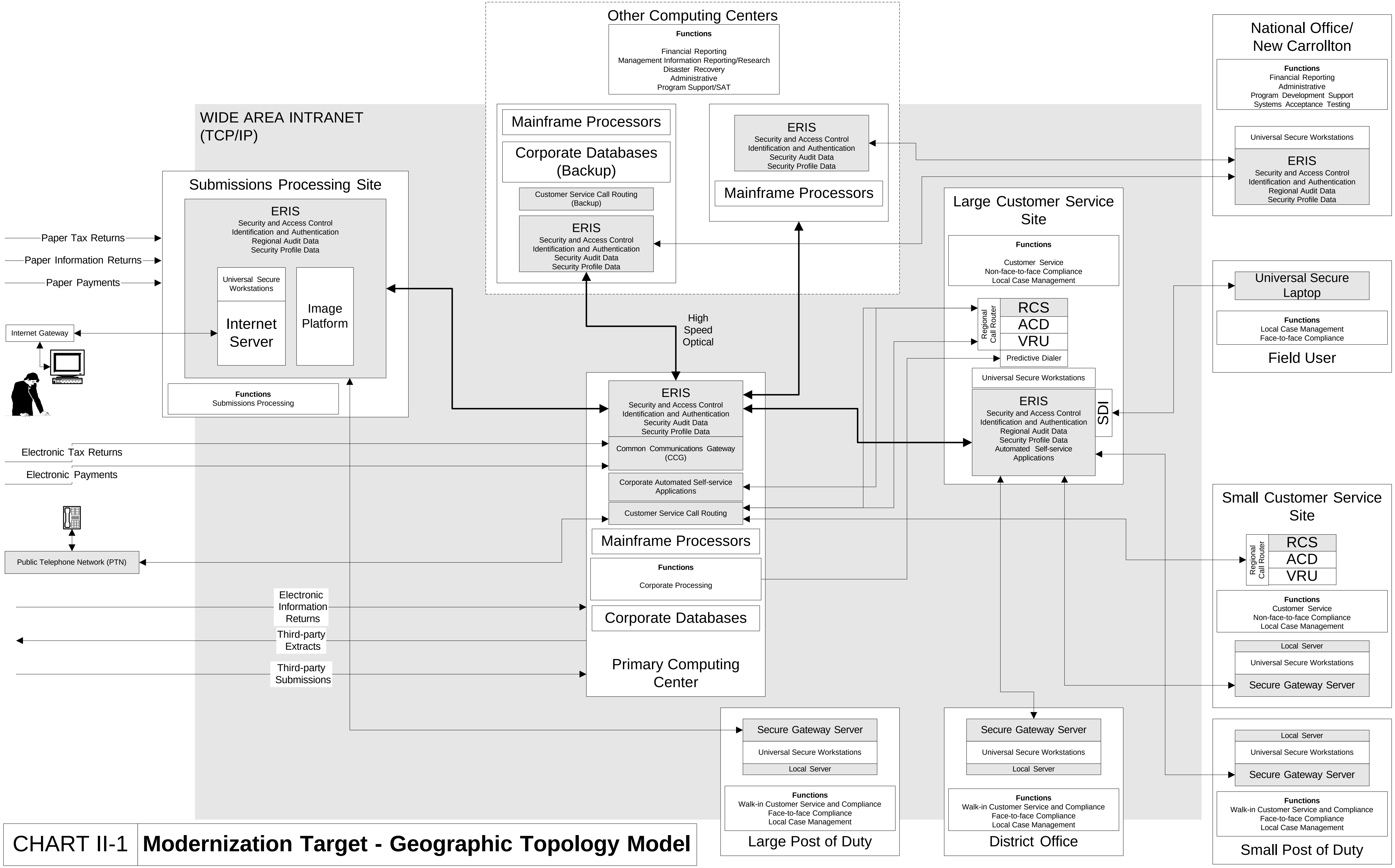

CHART II-1 **Modernization Target - Geographic Topology Model**

II.A Level I

The work processes and data flows for the Modernization environment begin with the receipt of paper and electronic (including Internet) tax returns, paper information returns, payments, and correspondence at the **SPS**. Electronic information returns and electronically submitted tax returns from preparers are received at the PCC and then forwarded to the SPS for processing. Each tax-related item received is identified, assigned a unique identifier (ID), and tracked through the submissions process. Paper material is processed using image-based data capture techniques, automated-verification and fraud-detection business rules, and image-based data correction. Electronic receipts are authenticated (at the PCC ERIS), validated, and processed through the same automated verification and fraud detection processes. Completed items, including verified items with outstanding issues, are transmitted to the PCC for corporate processing.

The transmitted data from the SPSs is received at the **PCC** and routed to the applications that post data to the Corporate Case Database (CCDB), the Information Returns Database (IRDB), the Payment Information Database (PIDB), the Tax Return Database (TRDB), and other appropriate databases. Scheduled mainframe background applications settle accounts using the Tax Accounts Database (TADB) in addition to the data posted to the other corporate databases. Errors detected during the posting and settlement processes are assigned to an inventory and processed in the same manner as cases in the corporate inventory. Additional issue and fraud detection business rules are applied, generating identified issues prior to the issuance of notices or refunds. Completed notices are forwarded to the Print Farm[1], completed refunds are forwarded to the Treasury Regional Finance Center (RFC) for printing or electronic funds transfer to the taxpayer's bank account, and detected issues are forwarded to corporate case processing for case creation and assignment.

Taxpayers contact the IRS for three primary reasons: to obtain filing and Tax Law information, to respond to a notice or refund mailed to them by the IRS, and to determine the status of a requested refund. Telephone calls from taxpayers are initially routed based on taxpayer-provided data through a telephone (e.g., Taxpayer Identification Number (TIN), Personal Identification Number (PIN), and other unique identification data). The calls are then forwarded to the PCC's CSCR system.

Telephone calls from taxpayers are distributed to **CSSs** based on CSCR and management inventories. Priorities are handled initially by the voice response unit (VRU) and ACD features, which analyze the data collected; attach the appropriate entity, case, and account data; and forward the call and collected data to the appropriate application and site. Taxpayers are given automated self-service application (ASSA) options, including account inquiries and updates. ASSAs guide the taxpayer through predetermined scripts that provide access to local static data (e.g., filing information and Tax Law material) or to authenticated access and update of corporate account data through applications at the PCC. Taxpayers with disabilities are provided with special telephone numbers specific to the

[1] The site of the Print Farm is to be determined.

contact media such as a Telecommunications Device for the Deaf (TDD) and a voice recognition device. During a VRU session, the taxpayer can choose to leave a voice mail message or to speak directly to a Customer Service Representative (CSR), which routes the telephone call to the next available CSR. Calls from taxpayers who choose to speak to a CSR are queued to be delivered to the next available representative, based on issue and account data at the site that receives the call, or to any national site capable of handling telephone taxpayer assistance. CSRs use transactions available to their universal secure workstations to access, update, and settle accounts located at the PCC as required.

Taxpayers who choose to contact the IRS through the Internet can use electronic mail in addition to the same ASSAs available through the telephone. Internet servers within the ERIS platform, which is located at the SPS (or other designated locations), use the same local static data and corporate applications to provide services to the taxpayers if the appropriate identification and authentication algorithms allow access to account and entity information.

Cases in the corporate inventory, including automated underreporter, delinquent tax and information returns, delinquent payments, detected cases of non-filing, and correspondence, may be selected based on business rules by corporate or local case management for telephone follow-up activities by CSRs. These cases are queued to the predictive dialing platform within RCS and delivered to the next available CSR in a CSS for taxpayer contact. Based on business rules, these cases might be selected for taxpayer contact using correspondence.

Cases in the corporate inventory in process are managed at the corporate level and are assigned to specific organizations within the **DO and Post of Duty (POD)**. The corporate case management applications apply enterprise-level rules, such as case distribution and the prioritization of cases based on value and age, and provide management with timely case summary information to support national-level priority and resource allocation decisions. Local case management applications hosted at the PCC are accessed through the universal secure workstation for individual Revenue Agent and Revenue Officer assignments. Cases are worked in these locations by accessing transaction-based applications at the PCC through the universal secure workstation.

Revenue Agents and Revenue Officers who work in the field or at the taxpayer's location (**field users**) use universal secure laptops to download encrypted case data and process the case using applications identical to the capabilities available to workstation users. Periodically, the data on the laptop is securely uploaded to the PCC, through ERIS at a Large CSS or an SPS, for processing.

Financial Reporting, corporate-wide case management, planning, and staff-allocation activities are based in the **National Office/New Carrollton (NO/NC)** sites using corporate applications at the PCC and the **OCC**[2]**.** Financial data is collected from every application

[2] The location of the Financial Accounting Database and financial reporting applications is currently under review and might change.

that affects tax accounts and payments and stores it in the PIDB and the TADB. Summarized data is stored in the Financial Accounting Database (FADB) and made accessible to the NO/NC sites for reports, adjustments and error corrections, and transmissions to the Department of Treasury.

Other functions that support the tax administration programs located at the OCC are program support, infrastructure support, program development, systems acceptance testing, and disaster recovery.

II.B Submissions Processing Site

Chart II-2, Submissions Processing Site, depicts the flow of work within the SPS and to and from connected sites. The work processes and data flows for the Modernization environment begin with the receipt of paper and electronic (including Internet) tax returns, paper information returns, payments, and correspondence. The paper material is processed using image-based data capture techniques, automated verification and fraud detection business rules, and image-based data correction. Electronic receipts are authenticated at the PCC ERIS, validated, and processed through the same automated verification and fraud detection processes. Completed items, including verified items with outstanding issues, are transmitted to the PCC for corporate processing.

Taxpayers who choose to contact the IRS through the Internet are provided with the same ASSAs available through the telephone. Internet servers within the ERIS platform, which is located at the SPS (or other designated locations), use the same local static data and corporate applications to provide services to the taxpayers if the appropriate identification and authentication algorithms allow access to account and entity information.

The SPS hosts full ERIS and RCS capabilities that support Submissions Processing and other sites (e.g., Small CSS and DO) via high-speed telecommunications links to the corporate environment through its ERIS.

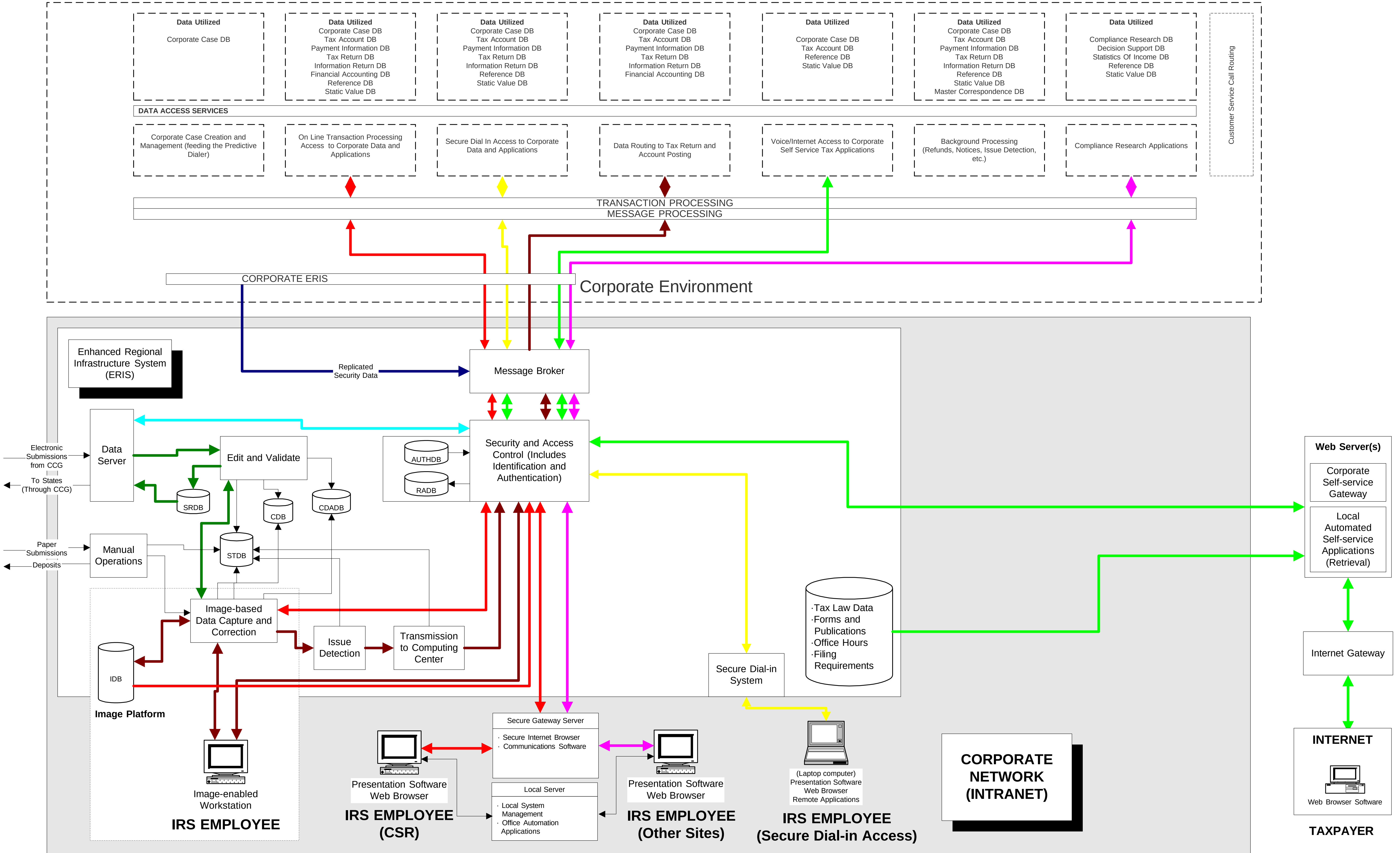

CHART II-2 **Submissions Processing Site**

II.B.1 General Work Process Information

The work processes in the SPS for Submissions Processing are categorized as follows:

- Paper (tax and information returns, remittances, credit- and debit-card payments and correspondence);
- Electronic (tax and information returns and remittances); and
- Internet (tax and information returns and correspondence).

General work processes throughout the SPS are as follows:

- Errors detected during posting and settlement to the corporate databases are inventoried and processed in the same manner as Customer Service cases;
- Scanned material is stored in the Image Database (IDB) to support downstream access to images using indices built at the PCC;
- Paper-based submissions are retained at the SPS until processing is completed for each item. Following completion of the processing for an item, all associated paper is appropriately archived;
- Captured data is stored in the Character Database (CDB); and
- MIS data is collected from every application including, but not limited to, audit tracking data (who, what, when, where, and how), performance data, and inventory levels.

II.B.2 Paper Processing

Paper items (mail and facsimile) are received in the SPS, presorted to the extent possible, and forwarded to scan preparation. The mail is opened, sorted, and forwarded for tax- and information-return processing, remittance processing (which might include credit- and debit-card payments), and correspondence processing. At this point, each document deemed necessary for tax administration purposes receives a unique ID, which establishes traceability to the source.

Remittances attached to tax returns are separated from the returns (and a voucher is created if one did not accompany the return). Remittances received without a tax return (e.g., payments based on notices returned to a lock box) and the associated vouchers are batched and prepared for deposit processing. The vouchers and remittances are scanned and stored in the IDB, the data is captured through an automated process (e.g., intelligent character recognition (ICR)), and the remittances are balanced to validate the collected information. To the extent possible, the entity data is validated and corrected as described below, and remittance errors are identified as issues (e.g., cannot associate a remittance with an entity). All remittances are then forwarded for deposit to a Federal Reserve Board (FRB) member bank, and the remittance data is transmitted to the PCC for posting to the PIDB, account posting, and settlement processing.

Credit- and debit-card payments are embedded with the tax return (on the tax return form).[3] Returns that include credit- and debit-card payments are processed through an additional application that interfaces with a credit- and debit-card clearinghouse to authenticate the payment, collect the authorization number from the clearinghouse, and associate the payment information with the return.

Tax and information returns are prepared for scanning. The material is scanned, stored in the IDB, and processed through an automated data capture engine (e.g., ICR). Based on business rules, additional data may be captured from selected returns. The collected data is validated, which includes entity verification[4], automated business rules for tax return data, tax and refund computations, and fraud and other issue detection. If errors are detected that can be corrected, they are queued for end-user modifications based on automated priority rules (e.g., receipt date and refund versus balance due). Returns that cannot be completely processed by the IRS due to uncorrectable errors either are prepared and returned to the taxpayer for further action or are processed for appropriate penalty assessment.

Using a secure image workstation, end users log into the verification and correction process. Based on the end-user security profile, which limits the type of activities that an end user can access, work is delivered to the workstation from the queues loaded during the automated verification process. The end user reviews the material presented to him or her using the universal secure workstation, which displays an image of the return, the captured data, and the errors. The end user applies the appropriate modifications and forwards the return back to queue management. Queue management functions provide the flexibility to adjust workloads based on changing priorities, staff mix, numbers and types of errors, and inventories.

After verification, remaining errors are identified as issues and, with verified returns, are transmitted to the PCC for posting to the IRDB and the TRDB, account posting and settlement processing, and issues posting to the CCDB.

Paper correspondence, including applications and registrations, is prepared for scanning; It is scanned, and the images are queued for review by the CSRs. The CSRs, following a process similar to the tax return verification process, review each correspondence image, associate it to an entity and/or case when applicable, categorize the correspondence (e.g., relate it to an existing issue or create a new issue), and transmit the data to the PCC for case management processing. (Correspondence received in other sites is managed and captured in the same manner.)

- ✦ Paper information returns are processed in the same manner as tax returns with the following exceptions: Remittance or credit- and debit-card payment information is not usually associated with an information return; and

[3] This approach is one option. A voucher approach may also be used for credit- and debit-card payments.

[4] There are two possible approaches for entity verification: access entity data at the PCC or download entity data periodically to the SPS for local use.

✦ Issues are identified for compliance action if there are discrepancies between data on the information return and the tax return.

II.B.3 Electronically Submitted Returns

Returns and remittances received electronically from business and individual taxpayers are delivered from tested and approved transmitters to the PCC through the CCG and forwarded to the SPS[5] for processing. In addition, preselected individual taxpayers and businesses may file electronically using touch-tone telephones or the Internet.

Transmitters apply IRS-defined formats and transmission requirements and transmit the tax return and/or remittance information to the IRS through the ERIS front-end CCG at the PCC. ERIS applications identify and authenticate transmissions and forward valid transmissions to SPS Submissions Processing applications for processing.

Returns transmitted electronically are assigned unique IDs and validated for format and structure. If errors are detected, the transmission is rejected, and an electronic message is returned to the originator through the PCC ERIS. (Originator, or transmitter, addresses are established when they are approved for electronic filing.) Returns that do not contain format or structure errors are forwarded to the automated-work-flow paper environment and are processed in the same manner as paper returns. (Image display, however, is slightly different: A structured presentation of the electronically filed data is displayed if errors are detected.) For returns filed using the joint Federal/State Electronic Filing program, either the state's data is stripped from the federal data and stored in the State Return Database (SRDB), where participating states have secure access to their data for downloading and processing, or the data is processed by the IRS in accordance with the appropriate Federal/State agreement.

Taxpayers who are eligible for the TeleFile program are notified by mail prior to the tax-filing season. The notification package includes a secure, unique authorization code the taxpayer uses during the telephone filing session. That code, in conjunction with the TIN, identifies the taxpayer to the ERIS-based TeleFile application when he or she begins a telephone filing session. Following the VRU session—which collects basic tax-filing information, assigns a unique ID to the return, and links the return data to the appropriate TIN—the data is forwarded to the automated-work-flow paper environment and is processed in the same manner as a paper return. (Image display, however, is slightly different: A structured presentation of the electronically filed data is displayed if errors are detected.)

II.B.4 Electronically Filed Remittances

Business taxpayers required to file remittances electronically use Fedwire and Automated Clearing House (ACH) credit and debit transactions submitted through FRB member banks. Identifying information (e.g., TIN) and remittance information are collected by the

[5] Depending on the results of the Level III and Level IV analyses, there might be multiple instances of the CCG in different locations, and the applications to process these receipts might reside at the PCC.

bank and processed through the appropriate mechanism (e.g., a Fedwire system or the ACH), and the results are forwarded to the IRS for processing using IRS-approved formats. The transmissions, collected through the PCC ERIS front-end CCG, are identified, authenticated, and forwarded to SPS Submissions Processing applications for processing.

Each remittance transmitted electronically is assigned a unique ID and validated for format and structure. If errors are detected, the transmission is rejected, and an electronic message is returned to the originator through the PCC ERIS. (Originator, or transmitter, addresses are established when they are approved for electronic filing.) Remittances that do not contain format and structure errors are forwarded to the automated-work-flow paper environment and are processed in the same manner as paper remittances. (Image display, however, is slightly different: A structured presentation of the electronically filed data is displayed if errors are detected.)

II.B.5 Tax Returns and Correspondence through the Internet

Taxpayers who choose to communicate with the IRS through the Internet have the following options:

- ✦ Send electronic mail to the IRS instead of paper correspondence.[6] This type of correspondence is electronically stored and then handled in the same fashion as paper correspondence;
- ✦ Submit applications and registrations related to any IRS issue. This correspondence is handled in the same manner as paper applications and registrations;
- ✦ Use an approved commercial tax-preparation package and transmit the completed tax or information return directly to the IRS through the Internet. Returns filed in this fashion are processed in the same manner as returns received from transmitters as described below[7];
- ✦ Use a tax-preparation package approved by an IRS-approved transmitter to transmit the completed return to the transmitter through the Internet. The transmitter forwards the returns collected in this manner to the IRS; and
- ✦ Include the payment for a tax, penalty, or interest-balance-due condition using the credit- and debit-card payment option described above[8].

[6] Other options might include preformatted forms that the taxpayer fills in for applications and standard form requests.

[7] Specific identification and authentication methodologies are to be determined.

[8] Specific identification and authentication methodologies are to be determined.

Internet-based input is collected on an Internet server that has a firewall between it and the other ERIS components. Information delivered to this server is periodically forwarded to the mainframe environment for processing.

II.C Primary Computing Center

Chart II-3, Primary Computing Center, depicts the flow of work within the PCC and connected sites. Background transmittal data from the SPS is received at the PCC and routed to the appropriate applications, which validate and post the data to the CCDB, the IRDB, the PIDB, and the TRDB. Scheduled mainframe background applications settle the accounts using the TADB in addition to data posted to the other corporate databases. Additional issue and fraud detection business rules are applied, generating issues as needed prior to or following the issuance of notices or refunds. Completed notices are forwarded to the Print Farm[9], completed refunds are forwarded to the RFC, and detected issues are forwarded to corporate case processing for case creation and assignment. Based on business rules, created cases may be selected by corporate case management for the following activities:

- Notice issuance or correspondence;
- Non-face-to-face case analysis and resolution by CSRs;
- Face-to-face office audit by Tax Auditors;
- Telephone follow-up by CSRs; and
- Field contact by Revenue Agents and Revenue Officers.

Telephone follow-up cases are queued to the RCS-based predictive dialing platform and delivered to the next available CSR in a CSS.

The PCC hosts the mainframe computers that provide transaction and data services to all the other sites. For larger sites (e.g., the Large CSS) high capacity (e.g., optical) transmission lines are used for connectivity to the PCC. For smaller sites (e.g., the Small CSS), the connectivity is accomplished through one of the larger sites. In addition, the PCC is connected to the OCC for data and corporate application backup and recovery capabilities.

[9] The site of the Print Farm is to be determined.

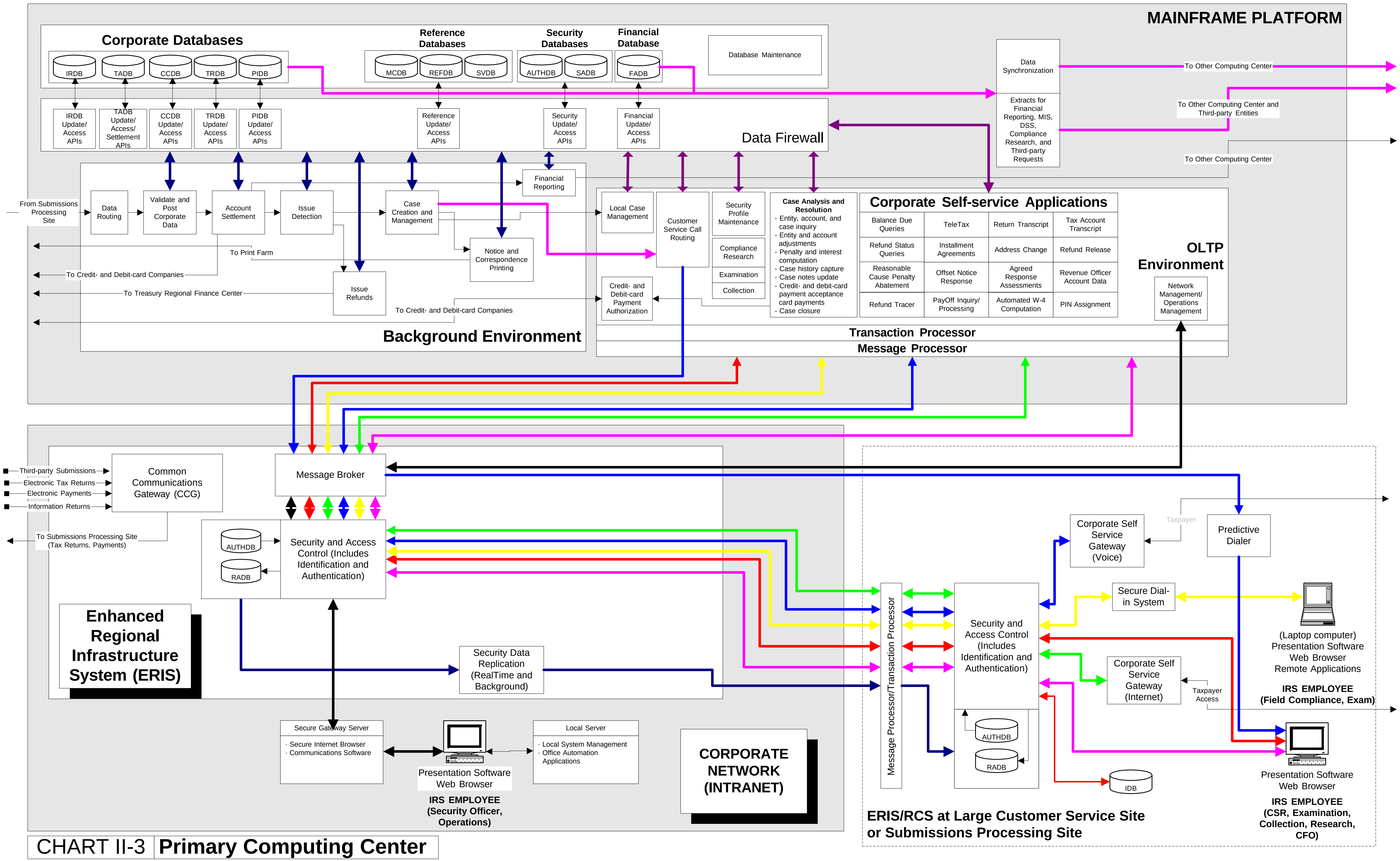
MAINFRAME PLATFORM
Corporate Databases
IRDB
TADB
CCDB
TRDB
PIDB
Reference Databases
MCDB
REFDB
SVDB
Security Databases
AUTHDB
SADB
Financial Database
FADB
Database Maintenance
IRDB Update/ Access APIs
TADB Update/ Access/ Settlement APIs
CCDB Update/ Access APIs
TRDB Update/ Access APIs
PIDB Update/ Access APIs
Reference Update/ Access APIs
Security Update/ Access APIs
Financial Update/ Access APIs
Data Firewall
Data Synchronization
Extracts for Financial Reporting, MIS, DSS, Compliance Research, and Third-party Requests
To Other Computing Center
To Other Computing Center and Third-party Entities
To Other Computing Center
From Submissions Processing Site
Data Routing
Validate and Post Corporate Data
Account Settlement
Issue Detection
Case Creation and Management
Financial Reporting
Notice and Correspondence Printing
Issue Refunds
To Print Farm
To Credit- and Debit-card Companies
To Treasury Regional Finance Center
To Credit- and Debit-card Companies
Background Environment
Local Case Management
Customer Service Call Routing
Security Profile Maintenance
Compliance Research
Examination
Collection
Credit- and Debit-card Payment Authorization
Case Analysis and Resolution
- Entity, account, and case inquiry
- Entity and account adjustments
- Penalty and interest computation
- Case history capture
- Case notes update
- Credit- and debit-card payment acceptance card payments
- Case closure
Corporate Self-service Applications
Balance Due Queries
TeleTax
Return Transcript
Tax Account Transcript
Refund Status Queries
Installment Agreements
Address Change
Refund Release
Reasonable Cause Penalty Abatement
Offset Notice Response
Agreed Response Assessments
Revenue Officer Account Data
Refund Tracer
PayOff Inquiry/ Processing
Automated W-4 Computation
PIN Assignment
OLTP Environment
Network Management/ Operations Management
Transaction Processor
Message Processor
Third-party Submissions
Electronic Tax Returns
Electronic Payments
Information Returns
Common Communications Gateway (CCG)
To Submissions Processing Site (Tax Returns, Payments)
Message Broker
AUTHDB
RADB
Security and Access Control (Includes Identification and Authentication)
Enhanced Regional Infrastructure System (ERIS)
Security Data Replication (RealTime and Background)
Secure Gateway Server
· Secure Internet Browser
· Communications Software
Presentation Software Web Browser
IRS EMPLOYEE (Security Officer, Operations)
Local Server
· Local System Management
· Office Automation Applications
CORPORATE NETWORK (INTRANET)
Message Processor/Transaction Processor
Security and Access Control (Includes Identification and Authentication)
AUTHDB
RADB
IDB
Corporate Self Service Gateway (Voice)
Taxpayer
Predictive Dialer
Secure Dial-in System
(Laptop computer) Presentation Software Web Browser Remote Applications
IRS EMPLOYEE (Field Compliance, Exam)
Corporate Self Service Gateway (Internet)
Taxpayer Access
Presentation Software Web Browser
IRS EMPLOYEE (CSR, Examination, Collection, Research, CFO)
ERIS/RCS at Large Customer Service Site or Submissions Processing Site

CHART II-3 **Primary Computing Center**

II.C.1 Online Transaction Activities

Every online transaction (message) received by the PCC, including one initiated within the PCC, is processed as follows:

- The PCC ERIS receives a message;
- The message processing application on the PCC ERIS determines where the message should be routed (e.g., corporate data inquiry, account update transaction, or automated self-service transaction);
- The transaction processor receives the request on the mainframe platform and launches the appropriate application;
- The application processes the data contained in both the message and the transaction, including the appropriate data access, and updates it through standard application programming interfaces (APIs) layered between the business logic and the physical databases;
- The application returns the results of the transaction to the Message Broker on the PCC ERIS platform; and
- The ERIS transmits the processing results to the ERIS platform that initiated the request for services.

The only variation to this scenario occurs for transactions that require special security (e.g., ASSAs that update corporate data). In those instances, the application may invoke specialized security algorithms to substantiate the requested service.

II.C.2 Background Activities

Background processing consists of the following scheduled, triggered, and ad hoc application executions on the PCC ERIS platform and the mainframe computers:

- Regularly scheduled application executions are managed and scheduled through Operations and include major IRS processing functions such as tax and information returns posting, payments posting, account settlement, refund and notice preparation, document matching and issue detection, financial reporting, and case management functions. The data routing application analyzes the incoming transmissions from the SPSs and pushes the data to the appropriate application;
- Triggered applications are managed through Operations but are automatically executed based on a series of parameters or other background events such as the receipt of uploaded tax return, information return, and payment data from the SPSs; electronically filed tax and information returns and payments from preparers and banking institutions; and security audit data uploads from another sites' ERIS platforms; and

- Ad hoc applications such as special MIS/DSS extracts and requests from external parties are also managed through Operations and are scheduled as resources permit, which is normally in real-time. Ad hoc requests are subjected to comprehensive security and data access scrutiny to ensure the corporate data is not compromised.

The background applications use shared online transaction processing (OLTP) business logic (e.g., subroutines and objects) for many functions, including account settlement, data access, and updates to ensure the uniform application of business rules to transactions, regardless of the source. Exceptions to this principle are high volume extract processes, which may require unique data access algorithms to satisfy performance requirements.

Background output (reports) are printed[10] and distributed from the Print Farm based on business rules supplied by end-user management[11]. Scheduling and Operations Management reports are produced in the PCC along with audit data of the background activities to support security and problem management.

Electronically filed returns and payments are received at the PCC (through the ERIS-based CCG), identified and authenticated, and forwarded to the appropriate SPS for processing. Returns and payments that fail critical edit processes trigger messages that are transmitted to the originators to notify them of the errors and corrective actions that must be taken.

Data for transmission (e.g., security profile data and static files for read-only ASSAs) is queued and scheduled for off-peak processing timeframes (e.g., overnight). Data transmission schedules are managed by Operations with input from site management.

II.C.3 External Drivers

Third-party requests for data processing services (e.g., Social Security Administration (SSA) tapes and 1099 tapes and transmissions) are based on prearranged agreements with other federal, state, or local governments; corporate entities; or foreign governments. As a result of the agreements, applications that have been developed, tested, and implemented are linked to the requests when they are received, and IRS contact points have been established to handle issues and operational problems.

These requests are delivered to the PCC using either electronic transmission mechanisms or electronic media (i.e., tape). The requests are managed by Operations by logging the receipt, purpose, source, and expected response date, if applicable, of each request. (Transmissions may be logged automatically, depending on the arrangement with the transmitter.) Scheduling of the application executions is based on business priority and computer-resource availability. Applicable outputs are distributed through the authorized IRS contact.

[10] Printed material may be delivered in hard or soft copy; the details will be determined during the Level III and Level IV analyses.

[11] The mechanism for transmitting output information to the Print Farm will be decided when the location of the Print Farm has been determined.

Similarly, Operations manages schedules of application executions that create data transmissions and electronic media for distribution to third-party entities based on prearranged agreements. These agreements address timing, content, delivery mechanism, delivery timeframes, and contact points.

Applications to support third-party requests and transmissions use the same common data access and security software as the background activities but also use additional capabilities for generating standard electronic data interchange (EDI)-based data transmissions.

II.C.4 Program Support

Requests for changes to the target environment are submitted in accordance with the Systems Life Cycle and, when approved, are tracked through the development and testing process using configuration management applications. Configuration changes are tracked and audited, and baseline configuration data for commercial off-the-shelf (COTS) and developed software is maintained in the Configuration Management Database (CMDB). Management of hardware and software installation, including status, is also controlled through this support application. Access to this mainframe application, through the OLTP environment, is secured through the security profile.

The corporate help desk receives problem reports from end users and management staff, logs the reports, and distributes them to the appropriate support personnel. The corporate help desk also tracks the resolution process for each report, notifies requestors when reports are complete, and periodically provides management reports on the progress and status of help desk activities. The data and applications reside on the mainframe platform and use the OLTP environment to access the reports, which are secured through the security profile.

Security Management controls the authoritative data stored and managed on the corporate ERIS platform. Profile change requests are received at the PCC, and secure applications are invoked to update approved profile modifications. Periodically (no greater than daily), the corporate profile database is transmitted to each ERIS location to support identification and authentication of system and application users.

Static data is maintained at the corporate PCC on the mainframe and ERIS platforms, depending on the type of information (e.g., notice templates are maintained on the mainframe platform and Automated Tax Law (ATL) management scripts are maintained on the ERIS). Approved updates are applied to the static data and, as required, transmitted to the ERIS locations.

II.C.5 Infrastructure Support

- **CSCR** interfaces with the Public Telephone Network (PTN) to direct calls to appropriate sites based on telephone traffic and business rules; and

- **Security Management** provides services consistent with security and risk management programs, operational plans and procedures, and central oversight and management of security processes. This function provides the capabilities for security administrators to perform day-to-day administration and security management activities across the Modernization system through corporate applications including, but not limited to, the following:

  - Create and manage identification and authentication data (including internal IRS end-user profile data);

  - Create and manage access control data, audit criteria, and audit trail data; and

  - Create and manage cryptographic key data and electronic marking control data.

Audit detection services are also provided at the PCC. The audit data collected from the ERIS locations is scanned and monitored to detect anomalies in resource access logs. Anomalies are reported to security administrators for appropriate follow-up action.

- **Data and Application Synchronization** provides disaster recovery capabilities by maintaining mirror images of the corporate data and applications in the OCC. Periodically, the corporate data and applications resident on the PCC are synchronized with the OCC. The OCC supports over 70 percent of the corporate workload and provides 100 percent data availability in the event of a disaster at the PCC[12];

- **Database Maintenance** includes the activities that support backup and recovery, database performance monitoring and tuning, and database integrity monitoring. These activities are tailored to each of the corporate and support databases depending on availability requirements, data distribution requirements, and the volatility of the data and data structures. Database administrators continuously review the various real-time and background reporting data and take corrective action as necessary; and

- **Network Management** provides local area network (LAN) and data communications backbone network management services; serves as the collection point for management-related data from devices connected to these networks; and monitors and controls LAN-attached and backbone devices. Incoming and outgoing telephone calls, transaction and message processing, data transmissions, and electronic mail are monitored to ensure each event type is receiving the appropriate priority within the telecommunications framework. Bottlenecks are identified and removed, business rules are adjusted depending on the time of year (e.g., heavier loads for incoming telephone calls in March and for returns processing in April), and adjustments to the connectivity between sites are made to ensure optimum performance.

[12] The methods and frequency for replication are to be determined. Options include, but are not limited to: (1) Use the OCC as a “hot site” based on periodic file copies; (2) Share OLTP responsibilities with the PCC; and (3) Occasionally swap OLTP responsibilities between the PCC and the OCC to ensure each site can handle 100 percent of the data and approximately 70 percent of the telecommunications traffic.

Network managers interact with the wide area network (WAN) service provider to perform configuration management, fault management, performance management, and accounting management. Network management functions provide the following:

- ▲ Allow network administrators to query and receive current network status from the WAN service provider;
- ▲ Maintain performance data on WAN service-provider resources;
- ▲ Receive accounting and billing information from the WAN service provider;
- ▲ Receive problem reports; and
- ▲ Create and route WAN service-provider problem reports to the WAN service provider.

✦ **Performance and Capacity Management** provides the capability to manage computing resource performance and use, including databases, networks, and voice systems. Resource utilization data is maintained at the PCC to provide information for reporting about performance and trend analysis;

This function also provides the capability to monitor real-time system performance and instrument systems and applications with performance measuring tools in addition to simulation and modeling to provide predictive system performance results for planned systems support and business applications; and

✦ **Operations Management** provides the capabilities to control and monitor the operation of system resources (e.g., operating systems, mainframe computers, direct access storage devices (DASDs), and tape drives) that enable all Modernization systems to be remotely monitored and controlled from one or more locations.

II.D Customer Service Sites

Chart II-4, Large Customer Service Site, and ***Chart II-5, Small Customer Service Site,*** depict the flow of work within the CSS and connected sites. Taxpayers contact the IRS for three primary reasons: to obtain filing and Tax Law information, to respond to a notice or refund mailed to them by the IRS, and to determine the status of a requested refund not yet received by the taxpayer. Telephone calls from taxpayers are initially directed by the CSCR system based on the originating telephone exchange and the dialed telephone number.

The telephone calls are then distributed to the appropriate RCS VRU at a CSS, depending on the Customer Service business rules followed to balance national traffic. Taxpayers are given a number of ASSA options, including account inquiries and updates. ASSAs guide taxpayers through predetermined scripts that provide access to local static data (e.g., filing information or Tax Law material) or through authenticated access and update of corporate account data through applications at the PCC. Calls from taxpayers who choose to speak to a CSR or have issues that cannot be solved by self-service applications are routed back to the CSCR post-routing system. These calls are queued to be delivered, through the ACD, to the next available CSR with the skills and tools to handle the issue regardless of his or her location. (Information about CSR skills and tools is stored in the employees' profiles.) The CSR uses transactions available at his or her universal secure workstation to access and update, as required, corporate data located at the PCC.

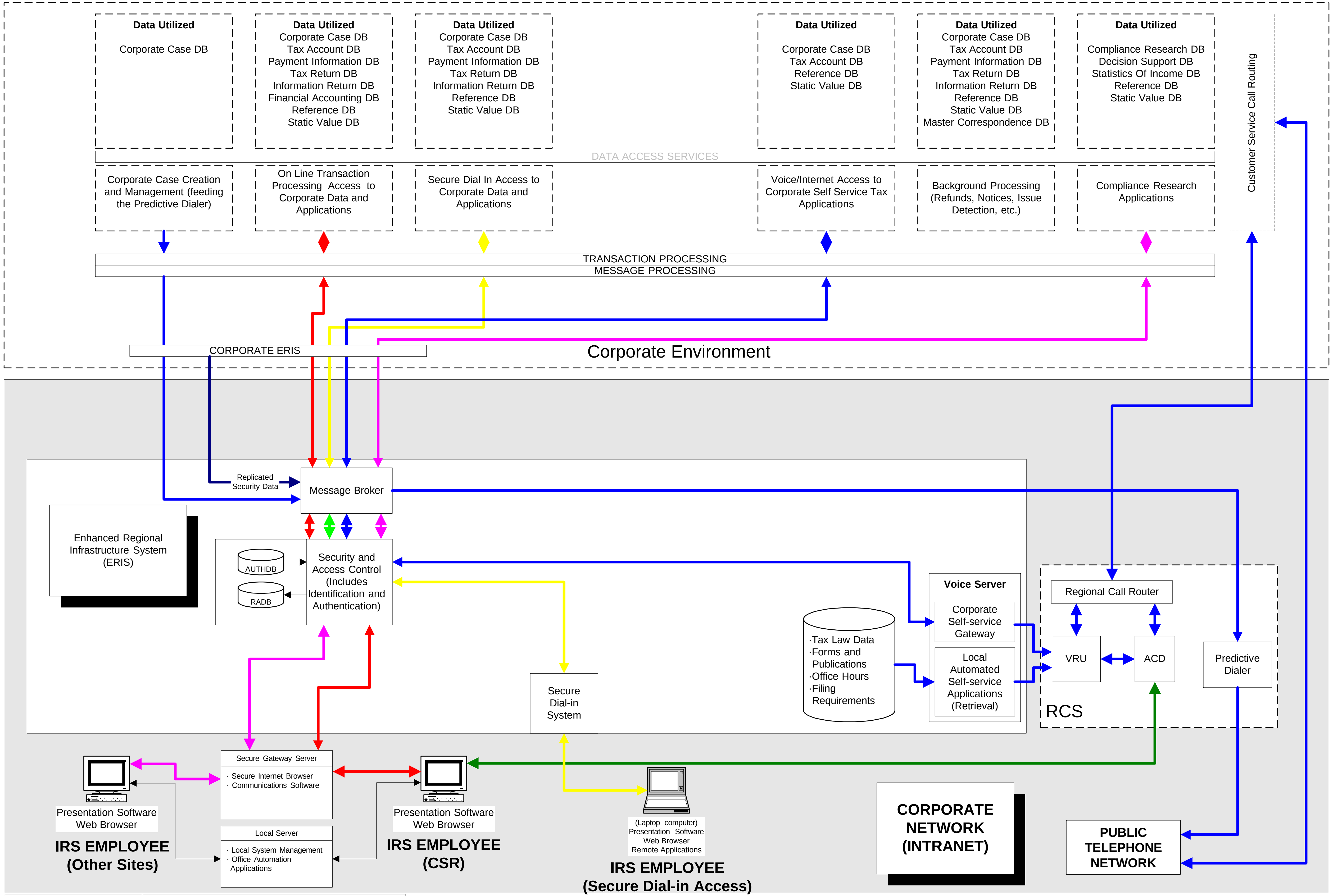

CHART II-4 **Large Customer Service Site**

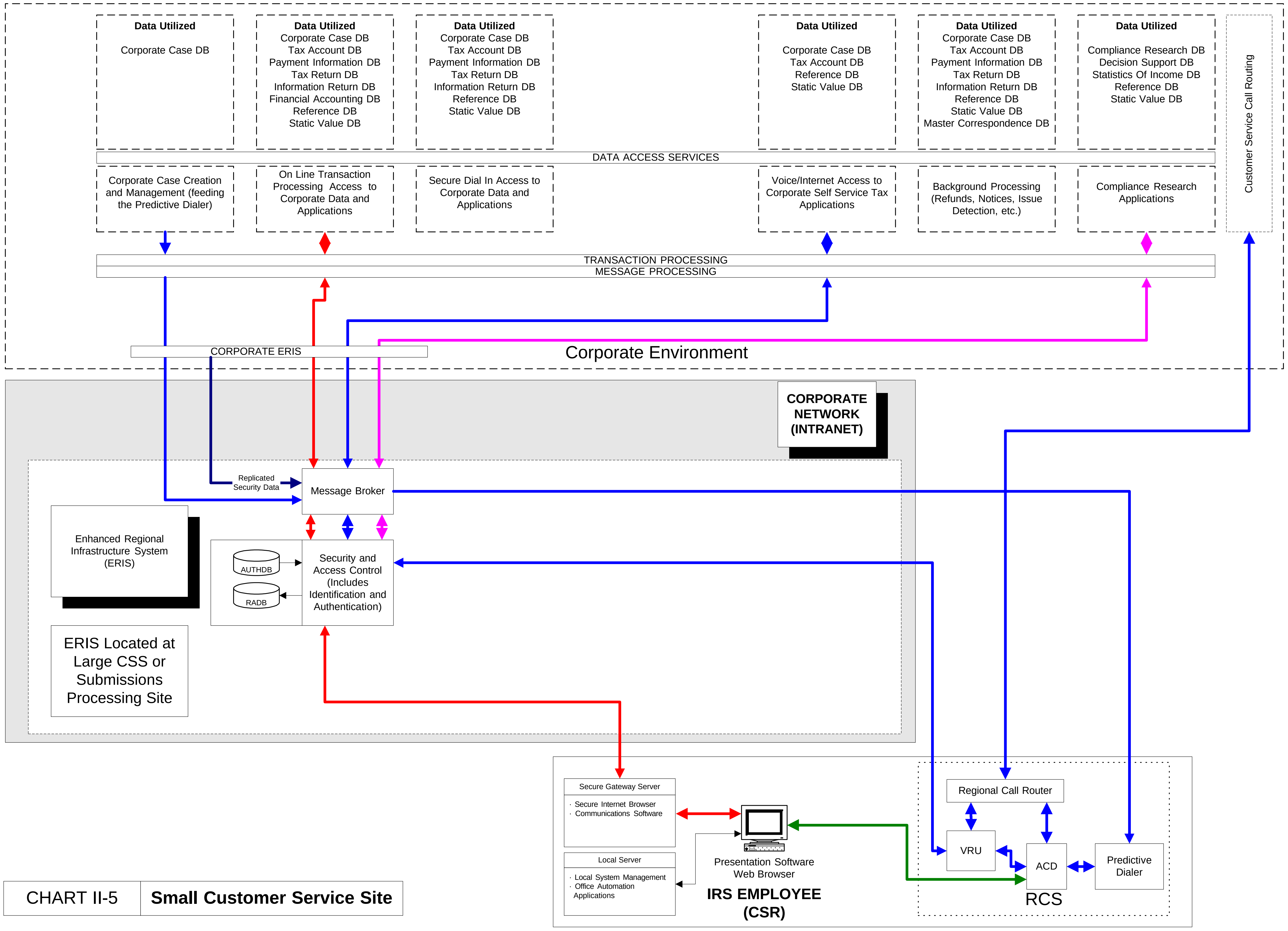

CHART II-5 **Small Customer Service Site**

II.D.1 Incoming Telephone Calls

Incoming telephone calls are initially pushed to the VRU through the RCS at the CSS, where taxpayers are provided a menu of options for self-service applications or, if appropriate, the opportunity to speak to a CSR. VRU self-service applications, also accessible through the Internet, include, but are not limited to, the following:

- ✦ Filing information on filing requirements, personal exemptions, interest income, dependents, filing status, earned income credit, standard deductions, other income, and capital gains and losses;
- ✦ Interactive tax law sessions that cover estimated tax, extension to file, basis of real property, individual retirement account (IRA) distributions, IRA contributions and deductions, social security and railroad retirement benefits, medical expenses, self-employment tax, credit for the elderly or disabled, and adjustments to income;
- ✦ Requests for tax forms, filing locations, and office hours; and
- ✦ If the taxpayer inputs the correct responses to identification and authentication requests, real-time tax account inquiries and adjustments through the VRU for voice balance due, refund inquiry, payoff, transcript request, PIN, refund trace, refund release, and account history (credit and debit).

If the taxpayer chooses, he or she can speak to a CSR by choosing the appropriate menu option during the VRU session. When this situation occurs, the telephone call and its associated entity, account, and case data are forwarded, based on business rules, to a CSR via the ACD.

The CSR, using a universal secure workstation, receives his or her next case or non-account-related telephone call by depressing the “next case” key. The associated corporate and call data is transferred to the CSR’s workstation with the telephone call, and the CSR resolves issues by gathering pertinent information from the taxpayer. Issue resolution is accomplished by using real-time interactive sessions including, but not limited to, the following:

- ✦ Reviewing the taxpayer entity, account, and case information presented to the CSR on his or her workstation;
- ✦ Requesting additional information from and providing additional information to the taxpayer as required;
- ✦ Releasing frozen refunds;
- ✦ Accessing additional information from the corporate databases for the taxpayer’s accounts and case-related data (which is protected from browsing by security browsing prevention);

- Computing payment, penalty, and interest amounts based on what-if scenarios (e.g., the taxpayer asks the CSR what the penalty and interest amounts would be if they were paid in full on a specific date or over a specific time period);

- Determining the appropriate account resolution when the taxpayer is unable to pay the determined amount in full. This includes securing financial information from the taxpayer and deferring payments due to hardship;

- Adjusting the taxpayer's return and account, as necessary;

- Locating and applying missing payments to an account;

- Creating a case in the event that a non-account-related telephone call results in case-related activities;

- Reassigning a case to a Revenue Agent or Revenue Officer for field action;

- Correcting name, address, and other entity-related information;

- Sending forms and instructions to the taxpayer through the Centralized Inventory Distribution System (CIDS);

- Resolving non-account issues such as when to file specific tax forms and other capabilities also available through the ASSAs;

- Updating corporate case history and notes;

- Accepting credit- and debit-card payments through the workstation with automated credit-card authorization capabilities; and

- Closing the case when appropriate.

The quality of the interaction between the taxpayer and the CSR is monitored by management staff and through periodic surveys of service quality, and appropriate actions are taken based on the quality assurance (QA) analysis results.

Following the completion of every transaction (whether it is successful or not), security audit trail data is generated and MIS data is captured and stored.

II.D.2 Automated Self Service Applications

Taxpayers who choose a menu option during a VRU session that requires a request for static data (e.g., ATL, filing locations, or forms orders) are directed to specialized VRU scripts. The scripts, stored at the Large CSS on the RCS VRU, are interactive, prompting taxpayers for menu choices; yes/no answers; and simple, non-account related numeric responses. Taxpayers, at any time, can exit a script and request connection to a CSR. Following completion of a session or telephone call disconnection, MIS data is captured and stored.

Taxpayers who choose a menu option during a VRU session that requires specific account, entity, or case data are linked to VRU sessions that interact with corporate data and applications. Data is collected to identify and authenticate the taxpayer (e.g., using a PIN and public or private keys) prior to any information transfer from the corporate platform.

Depending on the option chosen, the taxpayer can perform functions including, but not limited to, the following:

- Request a balance due amount;
- Request a refund amount;
- Request a printed transcript of his or her account (mailed to his or her current address);
- Obtain a PIN for interactive transactions; and
- Satisfy an account for lien removal.

As the taxpayer responds to automated prompts from the VRU, the applications on the RCS and ERIS (at the Large CSS) interact with corresponding applications at the PCC using transaction processing at each site. Tax account, entity, and case information are presented to the taxpayer during the process, and the taxpayer enters data into the system via the telephone keypad when prompted. At any time, the taxpayer can exit a script and request connection to a CSR. Following completion of a transaction, corporate data is updated (if applicable), security audit trail data is generated, and MIS data is captured and stored.

II.D.3 Internet Mail and Correspondence

Internet mail and paper (imaged) correspondence are handled in the same manner. The CSR receives his or her next case by depressing the “next case” key, and the appropriate mail message or imaged correspondence and its associated tax account, entity, and case data are delivered to the workstation. The CSR reviews the material and takes the appropriate action, which includes all the capabilities described for incoming telephone calls.

Voice mail is processed in the same manner as Internet mail and paper correspondence except the message is delivered through the CSR’s telephone headset in the same manner as incoming telephone calls.

II.D.4 Outbound Telephone Calls

Outbound telephone calls originate during background processing at the PCC, where selected computer-generated cases (based on automated, business-rule-based case management actions that identify cases requiring taxpayer contact) are pushed to the Predictive Dialer (PD) and telephone calls are automatically initiated to taxpayers. When a successful connection has been made, the case is pushed to the next available CSR along with associated entity, tax account, and case data. The cases are selected at the corporate level and assigned to locations based on business rules. The inventory is managed at the site through the PCC-based case management and local case management applications and the CCDB, where adjustments can be made based on local conditions (e.g., staffing levels). The remaining processes and capabilities are identical to the incoming telephone call function.

II.D.5 Case Management

Corporate and local case management activities, performed by IRS headquarters and site managers, use corporate-based applications and data to perform site-related functions including, but not limited to, the following:

- Manage cases (assign cases and manage inventories) to balance workloads based on varying levels of staffing;
- Monitor CSRs during issue- and case-resolution sessions with taxpayers;
- Review and approve cases;
- Generate management reports such as aging inventory and CSR productivity; and
- Perform QA of work performed at the site.

II.E District Office/Post of Duty

Chart II-6, District Office, and ***Chart II-7, Large/Small Post of Duty,*** depict the flow of work within the DO, the POD, and connected sites. Cases in process are managed at the corporate level and assigned to specific organizations within the DO and the POD. Local case management applications located at the PCC are accessed through the universal secure workstation for individual Revenue Agent, Revenue Officer, and Tax Auditor assignment. Cases are worked in these locations by accessing transaction-based applications at the PCC through the universal secure workstation.

The DO hosts the Secure Gateway Server to provide both access to ERIS capabilities at a Large CSS or an SPS and office automation capabilities

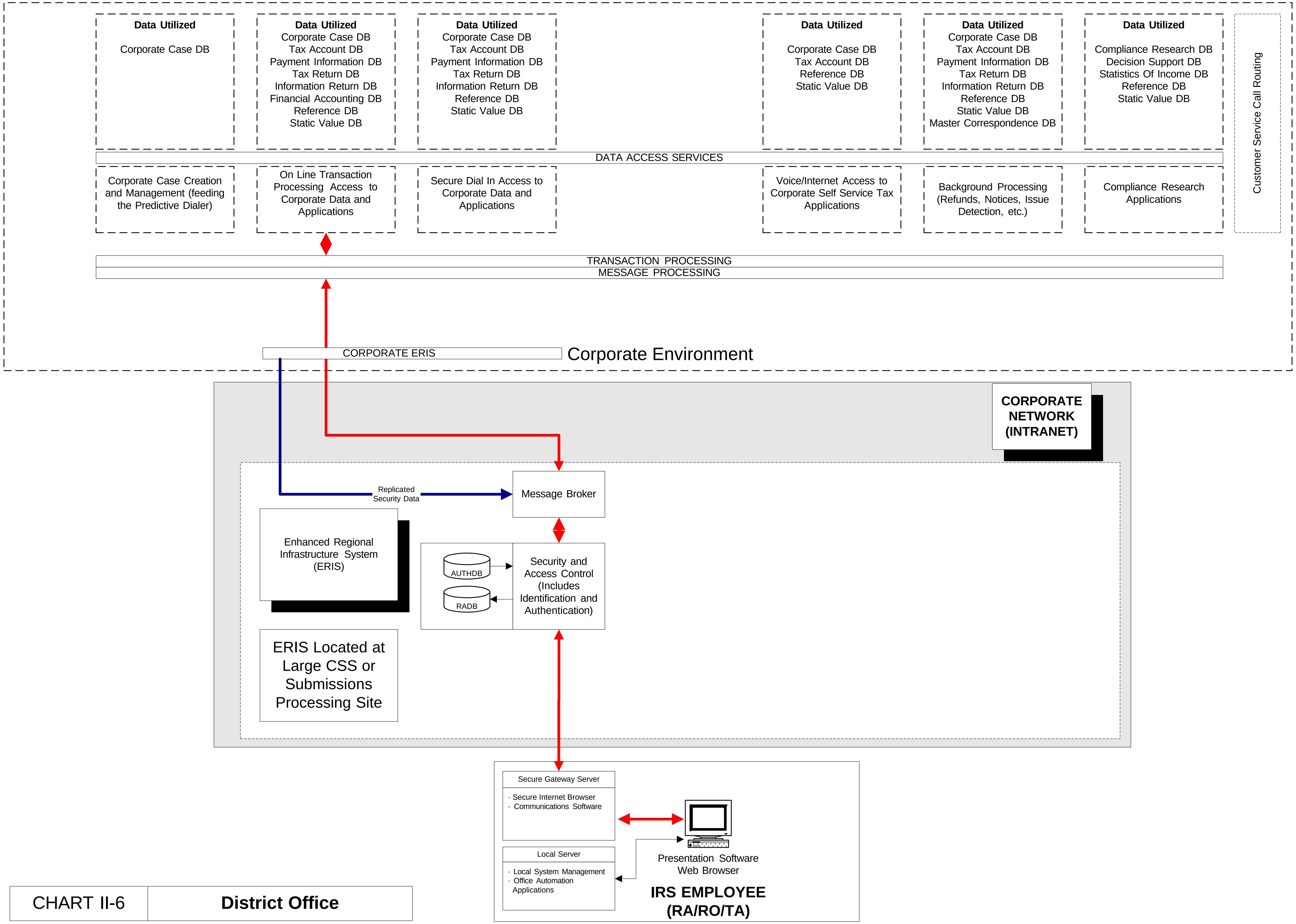

CHART II-6 **District Office**

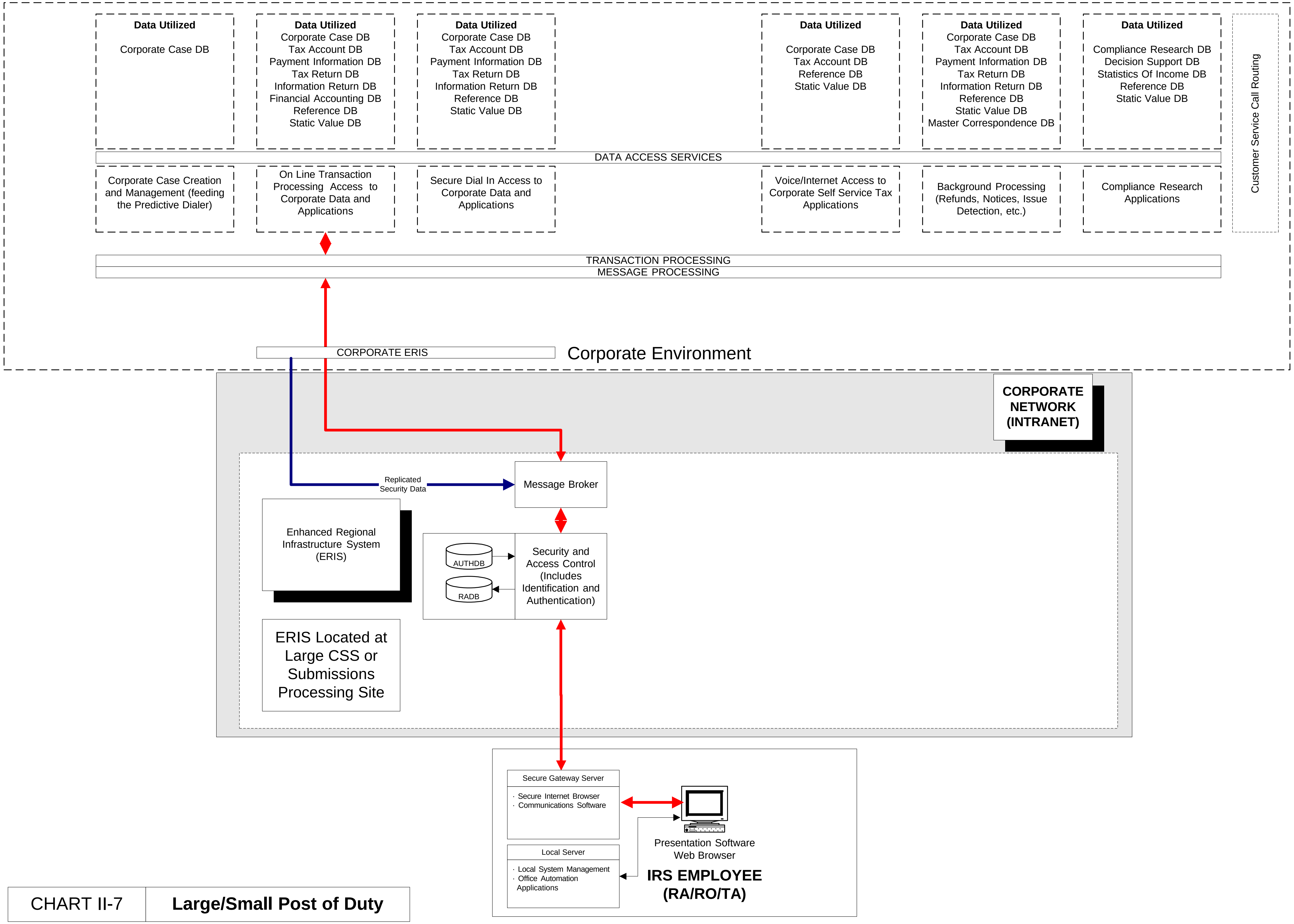

CHART II-7 **Large/Small Post of Duty**

II.E.1 Cases

Cases are initially assigned to a location based on business rules after the case information has been assembled (e.g., made fit for use) at the PCC. The case information includes, but is not limited to, the following:

- ✦ Initial taxpayer contact letters and notices;
- ✦ Tax- and information-return data;
- ✦ Prior case history;
- ✦ Identification of potential case issues;
- ✦ Contact information (e.g., address and phone numbers); and
- ✦ Settlement arrangement changes.

The DO support organizations (e.g., Planning and Special Programs (PSP) for examination and Special Procedures Function (SPF) for collection), stage the workloads for the Revenue Agent, the Revenue Officer, and the Tax Auditor. DO support organizations also create cases on the CCDB, perfect cases, schedule examination cases, provide quality review support of completed cases, maintain seizure inventories, and support mobile staff using corporate local case management tools accessed from the DO.

Desk functions (i.e., office audits), which involve face-to-face contact with the taxpayer at an IRS location (e.g., DO/POD), are controlled through the corporate-based calendar function that schedules cases for the Tax Auditor. Taxpayer appointment schedules are managed at the corporate level by DO/POD support staff (e.g., PSP and SPF) that includes appointment notification to the taxpayer.

The Tax Auditor, using a universal secure workstation, is notified of his or her next case through the automated calendar function. The associated case information, account data, and images are displayed on the Tax Auditor's workstation. He or she works the case using corporate applications to review the information, apply appropriate adjustments, invoke notice processing including the customization of text, update case history and contact information, and forward the case for review and approval. Cases worked in this fashion include, but are not limited to, the following:

- ✦ Overstated deductions or business expenses; and
- ✦ Non-matched information based on business rules[13].

[13] In the existing legacy systems, the business rules are embodied in the discriminate information function (DIF).

Revenue Agents conduct audits at the taxpayer's location using universal secure laptops or, in some cases, universal secure workstations installed by the IRS at the taxpayer's location when an audit will extend over a long time period.

Collection cases are assigned by Revenue Officers who choose them from their inventory (not by automated case delivery). These cases normally require longer time frames to complete, include more information for review (e.g., multiple tax years), and involve field contact with taxpayers. Cases worked in this fashion include, but are not limited to, the following:

- Delinquent tax and information returns;
- Delinquent payments;
- Federal Tax Deposit (FTD) alerts;
- Detected cases of nonfiling; and
- Taxpayer disputes (e.g., appeals of the amount of computed penalties and interest).

Activities supported by the corporate applications used to complete these cases include, but are not limited to, the following:

- Accessing reference data, including third-party data;
- Generating or requesting the generation of correspondence, notices, and reports;
- Computing penalty and interest based on what-if scenarios (e.g., the taxpayer asks the Revenue Officer what the penalty and interest amounts would be if they were paid in full on a specific date);
- Abating tax, penalty, and interest;
- Determining tax module balances and the disposition of any overpayment that results in settlement of the taxpayer's account;
- Adjusting the taxpayers return and account, as necessary;
- Recording case history and notes;
- Capturing additional or updated contact information;
- Generating waivers;
- Requesting and receiving credit- and debit-card authorizations; and
- Forwarding completed cases for approval.

Follow-up action requirements, such as levies and liens, or the results of Revenue Agent, Revenue Officer, and Tax Auditor case activities, are supported by Revenue Representatives and Officer Aides who deliver signed levies and liens and pick up checks from taxpayers.

II.E.2 Walk-in Taxpayer Assistance

Walk-in taxpayer assistance requires a blend of Customer Service and Compliance services. Using a universal secure workstation, the employee accesses both non-account and account-based corporate applications to assist the taxpayer with activities ranging from filing requirements and requesting forms to establishing an installment agreement. Additional activities include, but are not limited to, the following:

- Providing taxpayer outreach programs;
- Providing tax-related education to the taxpaying public; and
- Providing focus groups (e.g., paid preparer associations).

II.E.3 Case Management

Case Management activities use corporate-based applications and data to perform site-related functions including, but not limited to, the following:

- Defining and maintaining the local workload management criteria;
- Identifying cases that require approval before they can be closed or assessed;
- Determining and recording the status of collection and examination cases in inventory;
- Managing cases (assigning cases to groups and individuals and managing inventories) to balance workloads based on varying levels of staffing;
- Maintaining agreements and schedules including closing agreements, settlement agreements, offer-in-compromise agreements, seized asset inventories, litigation action schedules, and appointment schedules;
- Reviewing and approving cases;
- Generating management reports such as aging inventory and staff productivity reports; and
- Performing QA of work performed at the site.

II.E.4 Compliance Research

Research Analysts develop Compliance Research plans to direct the work of the Compliance organization, target opportunities to improve taxpayer compliance, and determine new or modify existing compliance detection criteria. Approved plans provide the basis for extracts from the corporate databases that create research databases at the OCC. The extracts are used for research activities including, but not limited to, the following:

- Making ad hoc queries against the Compliance Research Database (CRDB);
- Applying statistical methods to identify non-compliance cases that require contact with the taxpayer;
- Identifying tax- and information-return discrepancies;
- Determining delinquent tax filing based on historical filing trends of taxpayers;
- Determining patterns of compliance trends in the taxpayer population;
- Developing and testing compliance treatment plans;
- Developing specialized programs based on local conditions and industry-specific activities;
- Monitoring changes in compliance based on treatment plans; and
- Distributing research results to internal and external stakeholders.

These corporate applications are accessed through a universal secure workstation connected to the DO/POD Secure Gateway Server, which communicates with the ERIS at the nearest location and uses the same security profile identification and authentication techniques employed for all OLTP events.

II.F Field

Chart II-8, Field, depicts the flow of work between the Field user and connected sites. Revenue Agents and Revenue Officers who work directly with the taxpayers use universal secure laptops to download encrypted case data and process cases using applications that are identical to the capabilities available to universal secure workstation users. Periodically, the data on the laptop is securely uploaded to the PCC, through the ERIS at a Large CSS or an SPS, for processing.

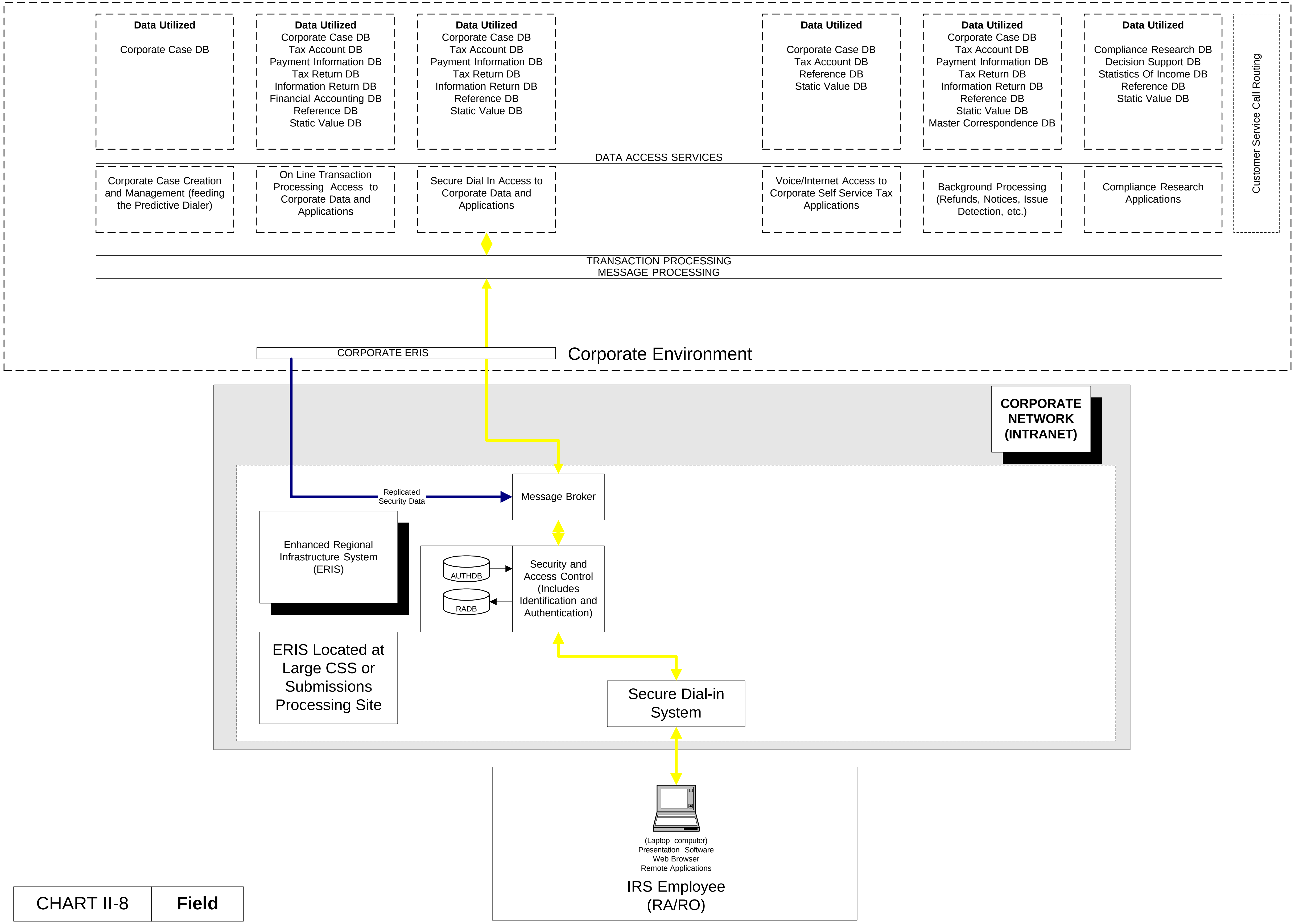

CHART II-8 **Field**

II.F.1 Open Cases

Cases are initially assigned to a location based on business rules after the case information has been assembled (e.g., made fit for use) at the PCC. The case information includes, but is not limited to, the following:

- Initial contact letters and notices;
- Tax- and information-return data[14] that includes the appropriate images of filed paper;
- Return examination results;
- Prior case history;
- Contact information (e.g., address and phone numbers); and
- Settlement arrangement changes.

DO and POD support staff, using corporate local case management tools accessed from the DO or the POD, assign the cases to field users for resolution.

Field cases involve face-to-face interaction with the taxpayer. The field user logs into the nearest Secure Dial-in facility, chooses cases from his or her assigned inventory, and downloads the encrypted assembled case data to a universal secure laptop.

The universal secure laptop contains application software that emulates a universal secure workstation: it provides the same capabilities to the field user as a universal secure workstation provides to a DO and POD Revenue Agent or Revenue Officer. In addition, through the nearest Secure Dial-in facility, static data stored on the ERIS at the Large CSS or an SPS is accessible to the universal secure laptop. Cases worked in this fashion include, but are not limited to, the following:

- Individual, business, and corporate examinations;
- Estate- and gift-tax returns;
- Employee Plan (EP) and Exempt Organization (EO) examinations;
- International examinations;
- Employment- and excise-tax return audits;
- Delinquent tax and information returns;
- Delinquent payments;

[14] Tax and information return data will be retained for a minimum of the current tax year and for up to two prior tax years.

- FTD alerts;
- Detected cases of non-filing; and
- Taxpayer disputes (e.g., appeals of the amount of computed penalties and interest).

Activities supported by universal secure laptop applications used to complete these cases include, but are not limited to, the following:

- Accessing reference data, including third-party data;
- Generating or requesting the generation of correspondence, notices, and reports;
- Computing penalty and interest based on what-if scenarios (e.g., the taxpayer asks the Revenue Agent or Revenue Officer what the penalty and interest amounts would be if they were paid in full on a specific date);
- Abating tax, penalty, and interest;
- Determining tax module balances and the disposition of any overpayment that results in the settlement of the taxpayer's account;
- Adjusting the taxpayer's return and account, as necessary;
- Recording case history and notes;
- Capturing additional or updated contact information;
- Generating waivers;
- Requesting and receiving credit- and debit-card authorizations; and
- Forwarding completed cases for approval.

Periodically, to complete the processing of cases, the field user connects to the Secure Dial-in facility to upload encrypted and updated information to the PCC.

II.F.2 Case Management

Case Management activities use universal-secure-laptop-based applications and data to perform field-related functions including, but not limited to, the following:

- Determining and recording the status of collection and examination cases in inventory;
- Maintaining agreements and schedules, including closing agreements, settlement agreements, offer-in-compromise agreements, seized asset inventories, litigation action schedules, and appointment schedules; and

- Conducting management reporting such as case status, case activity, and aging inventory reporting.

II.G National Office/New Carrollton

Chart II-9, National Office/New Carrollton, depicts the flow of work between the NO/NC and connected sites. Financial reporting, corporate-wide case management, planning, and staff allocation activities are based in the NO/NC sites using corporate applications at the PCC and the OCCs. Financial Reporting collects financial data from every application that affects tax accounts and payments and stores it in the PIDB and the TADB. Summarized data is stored in the FADB and made accessible to the NO/NC sites for reports, adjustments and error corrections, and transmissions to the Department of Treasury. The NO/NC hosts ERIS capabilities to access corporate resources at the PCC, the OCC, and on local servers for office automation capabilities.

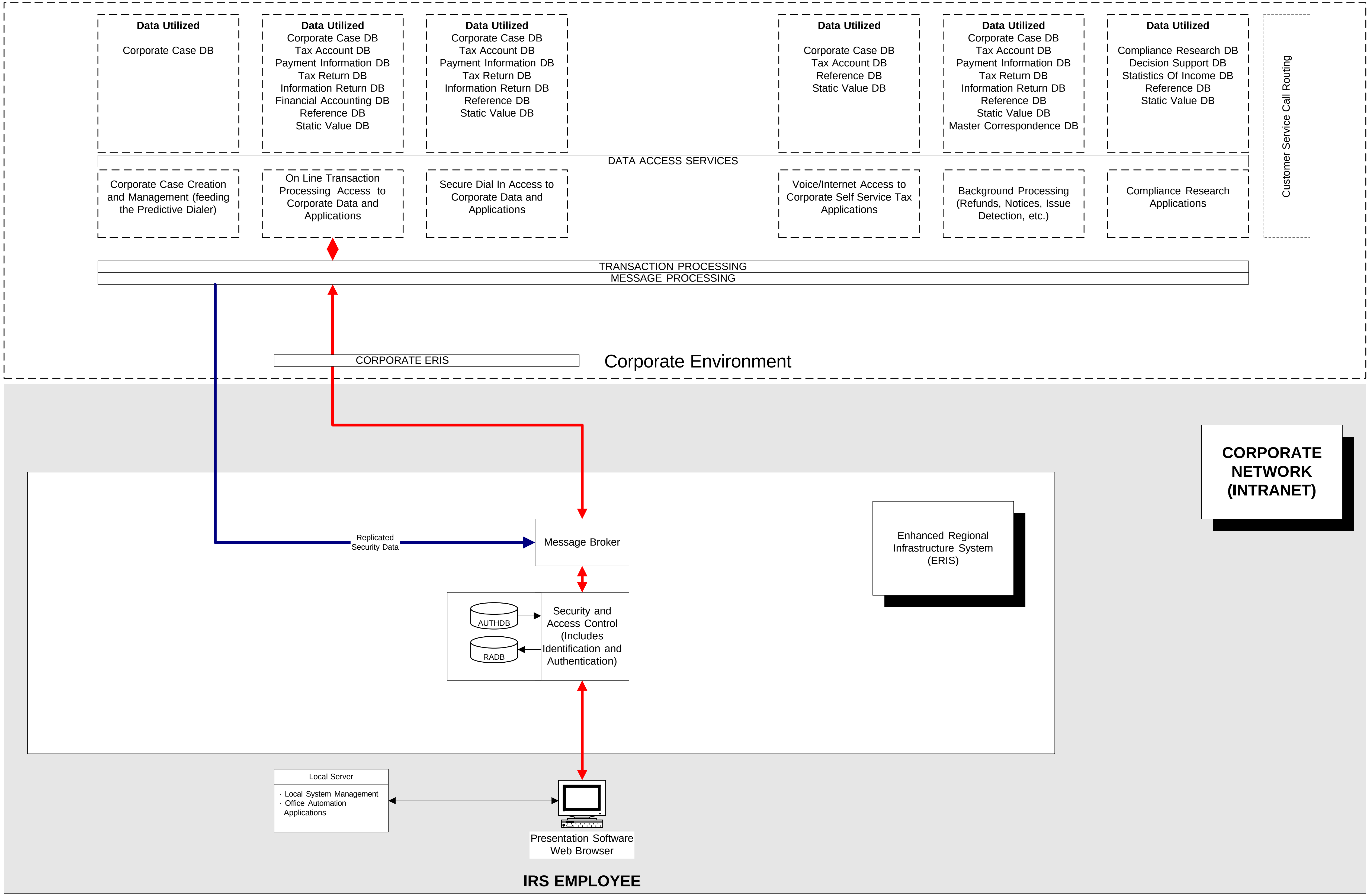

CHART II-9	**National Office/New Carrollton**

II.G.1 Financial Reporting

Background processes at the PCC and the OCC analyze data transmitted to the IRS from FRB member banks and the Department of Treasury and, based on the results, generate an inventory of work items to be addressed by the Chief Financial Officer (CFO). Work items include, but are not limited to, the following:

- Certifying disbursement schedules;
- Authorizing interagency funds transfer;
- Addressing issues related to the Department of Treasury disbursement and deposit confirmations;
- Updating the PIDB with adjustments to the Department of Treasury Financial Management Service deposit confirmations;
- Updating the TADB with disbursement schedule certifications, interagency transfer authorizations, and adjustments to distribution confirmation work items; and
- Resolving issues related to disbursements, deposits, and receipts.

Using the universal secure workstation, the end user accesses corporate applications at the NO/NC that are connected to the PCC[15] ERIS. Through these applications, CFO staff access and update corporate disbursement and deposit-related data, general ledger funding and reference data, and tax account data. Corporate case management tools, including inventory management and assignment tools, are available to CFO management to monitor and control the CFO work-item inventories.

Most financial reports are generated automatically from the OCC based on predetermined and agreed-to schedules with stakeholders. Standard reports include, but are not limited to, those made to the Department of Treasury Financial Management Service that include the IRS’s financial position, its collection and disbursement activities, and the use of appropriated funds. Ad hoc report requests from IRS management and other legislative and external organizations are initiated from a universal secure workstation, executed on the mainframe platform at the OCC, printed[16], and distributed to the originator.

[15] The final determination of the location of the authoritative financial databases (the PCC or the OCC) is to be determined.

[16] Printed material can be delivered in hard or soft copy; the details will be determined during the Level III and Level IV analyses.

II.G.2 Corporate Case Management, Planning, and Staff Allocation

The business rules and parameters that support the automated Corporate Case Management function are developed and maintained at the NO/NC. The primary activities supporting this capability include, but are not limited to, the following:

- ✦ Scheduling notice output generation;
- ✦ Maintaining static table data such as Tax Law scripts, business rules for case management, and DSS decision trees;
- ✦ Allocating staff by site and by shift;
- ✦ Evaluating workload delivery;
- ✦ Evaluating staff allocation and effectiveness; and
- ✦ Maintaining revenue collection projections and results.

NO/NC[17] staff develop the appropriate parameters and, using a universal secure workstation, access Corporate Case Management applications at the PCC to maintain the information used to drive the automated case management functions.

II.H Other Computing Centers

Chart II-10, Other Computing Centers, depicts the flow of work within the OCC and connected sites. Financial Reporting activities are based in the NO/NC sites that use corporate applications at the OCC and the PCC. Financial Reporting collects financial data from every application that affects tax accounts and payments and stores it in the PIDB and the TADB. Summarized data is stored in the FADB and made accessible to the NO/NC sites for reports, adjustments and error corrections, and transmissions to the Department of Treasury. Other functions located at the OCC that support the tax administration programs are Program Support, Infrastructure Support, Program Development, SAT, and Disaster Recovery.

[17] Regional involvement in this process is to be determined.

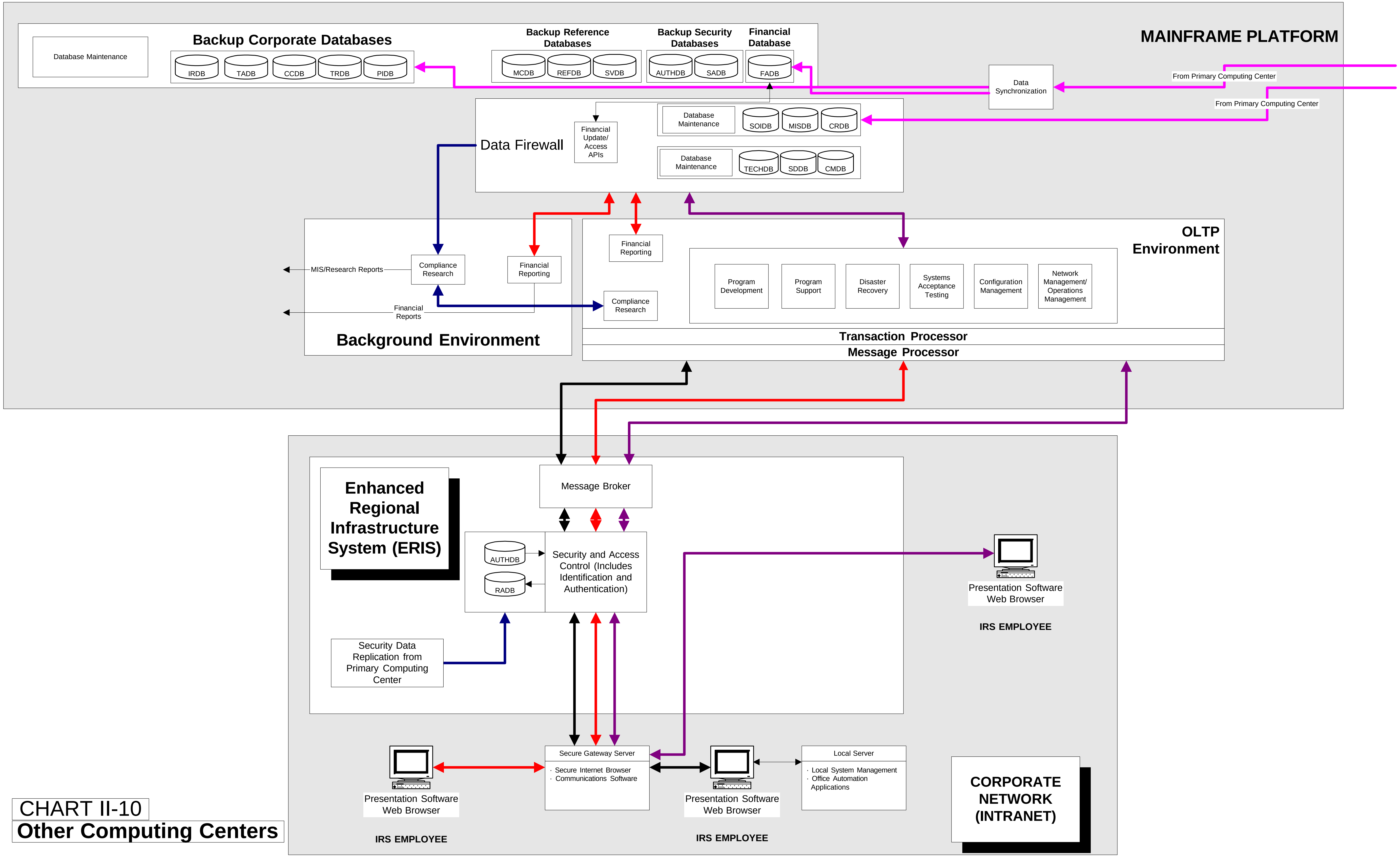
MAINFRAME PLATFORM
Database Maintenance
Backup Corporate Databases
IRDB
TADB
CCDB
TRDB
PIDB
Backup Reference Databases
MCDB
REFDB
SVDB
Backup Security Databases
AUTHDB
SADB
Financial Database
FADB
Data Synchronization
From Primary Computing Center
From Primary Computing Center
Data Firewall
Financial Update/ Access APIs
Database Maintenance
SOIDB
MISDB
CRDB
Database Maintenance
TECHDB
SDDB
CMDB
MIS/Research Reports
Compliance Research
Financial Reporting
Financial Reports
Background Environment
Financial Reporting
Compliance Research
OLTP Environment
Program Development
Program Support
Disaster Recovery
Systems Acceptance Testing
Configuration Management
Network Management/ Operations Management
Transaction Processor
Message Processor
Enhanced Regional Infrastructure System (ERIS)
Message Broker
AUTHDB
RADB
Security and Access Control (Includes Identification and Authentication)
Security Data Replication from Primary Computing Center
Presentation Software Web Browser
IRS EMPLOYEE
Secure Gateway Server
· Secure Internet Browser
· Communications Software
Presentation Software Web Browser
IRS EMPLOYEE
Presentation Software Web Browser
IRS EMPLOYEE
Local Server
· Local System Management
· Office Automation Applications
CORPORATE NETWORK (INTRANET)

CHART II-10
Other Computing Centers

II.H.1 Financial Reporting

II.H.1.a Background Activities

The identification of source documents that occurs during the processing of documents received in all business functions provides traceability to source transactions. As data is posted to the corporate databases in the PCC, revenue accounting summary transactions are built, assigned unique IDs, and linked to the original business transactions.

The revenue accounting summary transactions are transmitted from the PCC to the OCC[18] for journal processing and posting to the FADB. At the OCC, the revenue accounting summary transactions are translated into journal entries, associated, and processed as follows:

- Journal entries are verified for correctness;
- General ledger entries are created for each journal entry, posted to the appropriate general ledger account, and assigned a posted status;
- Each general ledger entry is associated to the corresponding journal voucher number;
- Funding documents are translated into journal entries; and
- Periodically, accounting periods are opened and closed, recurring journal entries are maintained, accrual and reversing journal entries are recorded, and financial data is reconciled.

II.H.1.b Online Transaction Processing

At the NO/NC site, the CFO accesses corporate financial applications to accomplish the following:

- Maintain the available balance of appropriations;
- Monitor funds availability;
- Maintain the general ledger chart of accounts, the accounting classification structure, and the general ledger posting rules;
- Create, review, and approve journal entries; and
- Modify unapproved journal entries.

[18] This might change depending on the outcome of the OCC analysis.

This access, through the OCC ERIS and the PCC, uses messaging and transaction processing services to invoke the financial applications and access to the FADB, the PIDB, and the TADB.

II.H.2 Disaster Recovery

Periodically, the PCC corporate data and applications are replicated[19] at the OCC for disaster recovery purposes. The OCC is configured to support at least 70 percent of the OLTP and background capacity, including network traffic, and 100 percent of the corporate data in the event the PCC is disabled for an extended period of time. Disaster recovery plans, including testing[20], are developed and maintained in off-site locations[21].

II.H.3 MIS Reporting and Compliance Research

Business-rule-based MIS/DSS extracts are created at the PCC and transmitted to the OCC for report generation. Standard reports are scheduled for execution on the mainframe platform as a background activity and the results are printed[22] and distributed. Ad hoc requests are submitted to Operations for scheduling, normally in real time, depending on available resources and capacity.

- ✦ Databases are created at the OCC based on DO requests for Compliance Research that include, but are not limited to, the following:
- ✦ Making ad hoc queries against the CRDB;
- ✦ Applying statistical methods to identify non-compliance cases that require contact with the taxpayer;
- ✦ Identifying tax- and information-return discrepancies;
- ✦ Determining delinquent tax filing based on historical filing trends of taxpayers;
- ✦ Determining patterns of compliance trends in the taxpayer population;
- ✦ Developing and testing compliance treatment plans;

[19] The methods and frequency for replication are to be determined. Options include, but are not limited to: (1) Use the OCC as a “hot site” based on periodic file copies; (2) Share OLTP responsibilities with the PCC; and (3) Occasionally swap OLTP responsibilities between the PCC and the OCC to ensure each site can handle 100 percent of the data and approximately 70 percent of the telecommunications traffic.

[20] The frequency of disaster recovery testing is to be determined.

[21] Off-site storage locations for these materials are to be determined.

[22] Printed material can be delivered in hard or soft copy; details will be determined during Level III and Level IV analyses.

- Monitoring changes in compliance based on treatment plans; and
- Distributing research results to internal and external shareholders.

These corporate applications are accessed through a universal secure workstation connected to the DO Secure Gateway Server, which communicates with the OCC ERIS and uses the same security profile identification and authentication techniques employed for all OLTP events.

II.H.4 Program Support

Requests for changes to the target environment are submitted in accordance with the Systems Life Cycle and, when approved, are tracked through the development and testing process using the configuration management applications. Configuration changes are tracked and audited, and baseline configuration data for COTS and developed software are maintained in the CMDB. Management of the installation of hardware and software, including status, is also controlled through this support application. Access to this mainframe application, through the OLTP environment, is secured through the security profile.

The corporate help desk receives problem reports from end users and management staff, logs the reports, and distributes them to the appropriate support personnel. The help desk then tracks the resolution process for each report, notifies requestors when the reports are complete, and periodically provides management reports on the progress and status of help desk activities. The data and applications that reside on the mainframe platform and use the OLTP environment to access reports are secured through the security profile.

Security Management controls the authoritative data stored and managed on the corporate ERIS platform. Profile change requests are received at the PCC, and secure applications are invoked to update approved profile modifications. Periodically (no greater than daily), the corporate profile database is transmitted to each of the ERIS locations to support the identification and authentication of system and application users.

Static data is maintained at the corporate PCC on either the mainframe or ERIS platform, depending on the type of information (e.g., ATL scripts on the ERIS platform and notice templates on the mainframe platform). Approved updates are applied to the static data and, as required, transmitted to the ERIS locations.

II.H.5 Systems Acceptance Testing

The OCC hosts the SAT environment to support all SAT activities.[23]

[23] Details for the support of SAT will be developed following completion of the SAT plan.

VOLUME VII – CONCEPT OF OPERATIONS

WORK DRIVERS

III. Work Drivers

Work drivers are based on events that trigger manual and automated processes in the modernized environment, providing the baseline information for work- and data-flow analysis.

III.A Level I

The following summarizes the Level I work drivers:

- Paper, electronic, and facsimile receipt of tax and information returns, remittances, applications, and correspondence;
- Taxpayers contacting the IRS through the telephone and the Internet;
- Case-based outgoing telephone calls from the IRS to taxpayers;
- Transaction-based requests for data access and update requests;
- Security events such as logon attempts, audit-trail generation, and data access and update requests;
- Financial Reporting events such as deposit confirmations, distribution confirmations, stop-payment requests, cancelled-distribution confirmations, and funding authorizations;
- Automated issue-detection results (e.g., create cases, issue notices, and collection cases);
- Account settlement results;
- Information exchanges between internal and external trading partners;
- Scheduled and ad hoc requests for data extracts and reports;
- Compliance Research results; and
- System stability.

III.B Submissions Processing Site

Paper and electronically filed tax returns, paper (including facsimile) and Internet-based correspondence, paper and electronically filed payments, and paper information returns are the primary drivers for the Submissions Processing activities performed at the SPS.

a) Paper Tax Returns

Paper tax returns are received at the SPS, scanned, processed through automated data capture engines (e.g., ICR), perfected through automated and manual business-rule-driven activities, and archived. Captured data is forwarded to the PCC for account posting and settlement. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

b) Electronically Filed Tax and Information Returns (from Preparers)

Electronically filed tax and information returns from preparers (e.g., paid preparers and accountants) are received at the SPS (via the CCG located at the PCC), identified and authenticated, perfected through automated business rules, and archived. Data is forwarded to the PCC for account posting and settlement. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

c) Electronically Filed Tax and Information Returns (from TeleFiling)

Taxpayers call a toll-free telephone number and, after identification and authentication, follow a script to provide the IRS with their tax or information return data through the telephone numeric keypad. Data is archived and forwarded to the PCC for account posting and settlement. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

d) Electronically Filed Tax and Information Returns (from the Internet)

Using a COTS tax-preparation package, taxpayers prepare their returns and use an industry-standard Web browser to transmit the results to the SPS through the Internet. After identification and authentication, the data is perfected through automated business rules, archived, and forwarded to the PCC for account posting and settlement. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

e) Paper Correspondence

Paper correspondence (including facsimiles), applications, and registrations are received at the SPS, scanned into the IDB, identified (e.g., linked to a TIN), linked to an existing case or included in the creation of a new case, and archived for retrieval when the case is worked by a CSR. Based on business rules, correspondence received at other sites might be routed through the SPS.

f) Internet Correspondence

Internet correspondence, including applications and registrations, is received at the SPS, identified (e.g., linked to a TIN), linked to an existing case or included in the creation of a new case, and archived for retrieval when the case is worked by a CSR.

g) **Paper Remittances**

Paper remittances, which are received at the SPS as attachments to returns or payment vouchers, are prepared for deposit, scanned, processed through automated data-capture engines (e.g., ICR), verified and perfected through automated business-rule-based algorithms if necessary, deposited, and archived. Data is forwarded to the PCC for posting to the PIDB and the TADB and for account-settlement processing. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

h) **Electronically Filed Remittances**

Electronically filed remittances and associated return or payment-information data are received at the SPS (via the CCG located at the PCC), identified and authenticated, and archived. Data is forwarded to the PCC for posting to the PIDB and for account-settlement processing. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

i) **Credit- and Debit-Card Payments**

Credit- and debit-card payments are received at the SPS as attachments to returns or payment vouchers. They are scanned, processed through automated data capture engines (e.g., ICR), identified and authenticated, verified and perfected through automated business-rule-based algorithms if necessary, electronically processed through the appropriate credit- and debit-card companies, and archived. Data is forwarded to the PCC for posting to the PIDB and for account-settlement processing. Posting and settlement errors detected at the PCC are assigned to an inventory and processed in the same manner as non-face-to-face casework.

j) **Paper Information Returns**

Paper information returns received at the SPS and electronic information returns are received at the PCC are scanned, processed through automated data-capture engines (e.g., ICR), perfected through automated and manual business-rule-driven activities, and archived. Captured data is forwarded to the PCC for posting to the IRDB.

k) **Internet-Based Automated Self Service Applications**

Taxpayers can access ASSAs through the Internet and use applications that are identical to the ASSA services. Instead of voice scripts, however, the taxpayer uses a standard Web browser to interface with the ASSA.

III.C Primary Computing Center

The PCC work drivers can be classified into the following categories:

- Online transaction activities;
- Background activities;

- External drivers;
- Program support; and
- Infrastructure support.

The majority of these work drivers are automated reactions to events occurring in other sites, regularly scheduled events such as data exchanges, and resource-monitoring activities for telecommunications and computing capacity. The remaining drivers include, but are not limited to, the following:

- Requests from users for reports;
- Management reporting;
- Externally provided data-management requests; and
- Configuration management.

III.C.1 Online Transaction Activities[1]

a) **Transaction Processing and Message Brokering**

Online corporate applications are executed based on messages received from other sites through the ERIS. Transaction-processing and message-brokering capabilities are used to manage the application executions.

b) **Data Access Requests**

Online data access is provided to applications through a core of inquiry services based on structured query language (SQL) standards. Each application requests data based on input from the user that has been certified through security algorithms as a valid request.

c) **Data Maintenance Requests**

Data maintenance is a core set of services that create, update, and delete corporate data based on validated requests from applications.

d) **Account Settlement Requests**

Following the application of new data (e.g., new accounts, third-party data, and new assessments) or adjustment of an account, account-settlement applications are invoked to adjust the tax-account balance through a series of settlement algorithms.

[1] Phase and Release versions of this document will address Transition Bridge capabilities.

e) **Account-based Automated Self Service Requests**[2]

Requests for account-based ASSAs are received from telephone calls (through the VRU) and the Internet.

f) **Telephone Call Routing Requests**

Incoming telephone calls from taxpayers are routed to the appropriate site based on data captured during the initial stages of the call and taxpayer account information.

g) **Customer Service Requests**

Transactions generated by Customer Service activities at the other sites (e.g., a Large CSS) are processed at the PCC using corporate data.

h) **Compliance Requests**

Transactions generated by Compliance activities at the other sites (e.g., DO or POD) are processed at the PCC using corporate data.

i) **Submissions Processing Requests**

Transactions generated by Submissions Processing activities at the SPS are processed at the PCC using corporate data.

III.C.2 Background Activities[3]

a) **Tax Return Postings**

Paper tax returns received, edited, and transcribed at the SPSs, as well as electronic tax returns received and edited at the SPSs, are collected and uploaded to the PCC for posting to the appropriate taxpayer and financial accounts. Detected errors are assigned to an inventory and processed in the same manner as non-face-to-face casework.

b) **Information Return Postings**

Paper information returns received, edited, and transcribed at the SPSs are collected and uploaded to the PCC for posting to the appropriate taxpayers records. Electronic information returns are received and processed at the PCC (via the CCG located at the PCC) and processed in the same manner.

[2] ASSA includes Internet and voice requests.

[3] Phase and Release versions of this document will address Transition Bridge capabilities.

c) **Payment Postings**

Most payments are received, edited, and processed at the SPSs and uploaded to the PCC for posting to the appropriate taxpayer and financial accounts. Errors detected are assigned to an inventory and processed in the same manner as non-face-to-face casework.

d) **Account Settlements**

Following the posting of tax returns and payments, new account creation, and new assessments, account settlement is invoked to adjust tax account balances through a series of settlement algorithms that include the computations of refund and balance due. Detected errors are assigned to an inventory and processed in the same manner as non-face-to-face casework.

e) **Refunds**

Refund-due data is accumulated and processed periodically (as often as daily but not less than weekly) to generate refund checks and electronic deposits.

f) **Notices**

Notice data is accumulated, subjected to QA measures, and processed periodically (as often as daily but not less than weekly) to generate consolidated notice files to be transmitted to the Print Farm for printing and distribution.

g) **Document Matching**

The periodic matching of tax returns; spouse, dependent, and partner responsible-party data; information returns; and third-party data (e.g., SSA files) are performed and the results are forwarded to issue-detection processing.

h) **Issue Detection**

Document match results and other applied algorithms (e.g., TIN analysis and dependent-data analysis) are applied periodically, depending on the type of analysis, to determine non-filing, under reporting, duplicate filing, and other anomalies. The results are forwarded to the Corporate Case Processing applications.

i) **Financial Transactions**

Each transaction that affects a payment receipt or the financial status of a tax account generates a financial transaction that is forwarded to Financial Reporting processing.

j) **Financial Reporting**

Collected Financial Reporting transactions are processed daily and applied to the financial database (e.g., general ledger accounts). Reports are generated daily.

k) **Security Data Collection and Distribution**

Security audit data is collected daily from each regional site and posted to the Security Audit Database (SADB).

l) **Corporate Extracts for MIS/DSS**

Periodically, and on an ad hoc basis, information is extracted from the authoritative databases and loaded to offline MIS/DSS databases. In some cases, Compliance Research and Financial Reporting data is extracted and transmitted to other sites for use.

m) **Corporate Case Creations, Assignments, and Updates**

Based on data collected from issue detection and business rules, cases are created and loaded to the CCDB and assigned to, at a minimum, a site for case processing. Case updates are applied based on return and payment postings that might satisfy outstanding issues.

III.C.3 External

a) **Third-Party Data Processing Requests**

Electronic transmissions (via the CCG) and media are received daily from other government agencies (federal, state, local, and foreign) and corporations (e.g., telephone number and directory data) for loading to corporate support databases and use in various corporate processes (e.g., document matches).

b) **Extracts to Third Parties**

Electronic transmissions and media are prepared daily for transmission (through the CCG) to government agencies (federal and state) to provide financial information (e.g., the Department of Treasury) and return information to the requesting parties.

III.C.4 Program Support

a) **Configuration Modifications**

Changes in computer hardware, systems software, telecommunications, and applications are managed at the corporate level and include software version control and distribution.

b) **Problem Management**

System hardware, software, application, and telecommunications problems are reported to the corporate help desk for resolution, tracking, auditing, and reporting.

c) **Security Profile Management**

Profile data is maintained at the corporate level and distributed (when changes are applied) to sites that house local security databases for identification and authentication.

d) **Static Data Maintenance**

Static data is maintained at the corporate level and distributed to appropriate sites when modifications are applied.

III.C.5 Infrastructure Support

Infrastructure Support consists of the following capabilities:

- ✦ National contact manager (i.e., CSCR);
- ✦ Security management;
- ✦ Data and application synchronization;
- ✦ Database maintenance;
- ✦ Network management;
- ✦ Performance and capacity management; and
- ✦ Operations management.

The single driver for Infrastructure Support is the requirement to provide a secure and stable computing environment for tax administration data and systems.

III.D Customer Service Sites

Incoming telephone calls, Internet mail, and paper correspondence from taxpayers and outbound calls to taxpayers (for open cases) are the primary drivers for the activities performed at the Large CSS.

a) **Incoming Telephone Calls**

Incoming telephone calls from taxpayers, including calls from taxpayers with disabilities, are routed to the Large CSS through the corporately managed CSCR process after basic information (e.g., TIN) is collected from the taxpayer through VRUs. Automated data-directed routing using business rules (e.g., the type of call, the location from which the call originates, and the type of transaction requested) and real-time data (e.g., site and staff availability) are applied to determine which location will receive the call. Case and account data are collected from the corporate databases and linked to the telephone call, and the information is assigned to the appropriate location. The telephone call and entity data (if available) are linked and assigned to the appropriate location when a case does not exist for the TIN provided during the initial stage of the taxpayer contact.

b) **Internet Mail**

Internet mail is collected on the Internet server located in the SPS. Periodically, the information is forwarded to the PCC where a case is created for each item and, based on business rules, assigned to an appropriate location.

c) **Voice Mail**

Voice mail is collected on the VRU server located in the Large CSS. Periodically, the information is forwarded to the PCC where a case is created for each item and, based on business rules, assigned to an appropriate location.

d) **Paper and Facsimile Correspondence**

Paper and facsimile correspondence is received at the SPS, scanned, stored and indexed on the IDB, and forwarded to the PCC for case processing and the creation of a case for each item. Based on business rules, the cases are assigned to the appropriate location.

e) **Case Inventory**

Outbound telephone calls are pushed from the PCC to a CSS chosen based on case inventory, business rules (e.g., staff availability), and case type (e.g., notifications, letters, and levies).

III.E District Office/Post of Duty

Open examination and collection cases, walk-in taxpayer assistance, case management activities, and Compliance Research are the primary work drivers at a DO/POD.

a) **Examination and Collection Cases**

Based on business rules, the PCC selects returns for examination and creates collection field cases using background activities, including fit-for-use criteria. After these cases are systemically assembled and assigned to specific locations based on corporate priorities, the location of the DO/POD, and workload, they are added to the CCDB.

b) **Walk-in Taxpayer Assistance**

The DO/POD provides walk-in service to taxpayers who wish to interact directly with IRS staff. Taxpayers who choose this option are afforded the same capabilities for issue resolution as taxpayers who call or correspond with the IRS.

c) Case Management Activities

Cases assigned to a DO/POD are reviewed by management and assigned to groups or individuals. Inventories are monitored for aged cases, follow-up actions, and reassignments. Cases are identified for approval. Agreements and schedules are maintained, and seized asset inventories are tracked and managed.

d) Compliance Research

Compliance Research conducts studies using corporate and other data to develop criteria to be used throughout the IRS to detect issues with tax filings before refunds are generated (early noncompliance) or subsequent to refund processing (e.g., delinquent returns and discrepancies with information return data). The data-specific studies involve specialized processing of selected cases to identify potential processing and procedural changes to enhance national and local compliance activities and productivity.

III.F Field

Open collection cases and case management activities are the primary work drivers for field users.

a) Collection Cases

Based on business rules, the PCC selects returns for examination (audit) and creates balance-due non-filer account (collection) cases using background activities including fit-for-use criteria. After these cases are systematically assembled and assigned to a specific location based on service priorities, workload, and the location of the DO/POD, they are added to the CCDB.

b) Case Management Activities

Cases assigned to a DO/POD are reviewed by management and assigned to field users who use local case management activities to manage and monitor their cases.

III.G National Office/New Carrollton

a) Corporate Management

To achieve the greatest efficiencies provided by the automated case management functions, enterprise-wide workload and staffing parameters are developed and maintained at the NO/NC.

b) End-User Financial Transactions

Most financial transactions are systematically generated during the processing of tax returns, payments, and deposits. End-user financial activities include, but are not limited to, the following:

- Certifying disbursements;
- Authorizing interagency transfers;
- Resolving the Department of Treasury deposit and disbursement confirmation-related issues;
- Maintaining funds allocation and general ledger reference data; and
- Confirming deposits.

c) **Financial Report Requests**

Requests for standard and ad hoc reports are generated from the NO/NC sites.

III.H Other Computing Centers

a) **Financial Reporting**

Most financial transactions are systematically generated during the processing of tax returns, payments, and deposits. Activities that require end-user interaction include, but are not limited to, the following:

- Certifying disbursements;
- Authorizing interagency transfers;
- Resolving the Department of Treasury deposit and disbursement confirmation-related issues;
- Maintaining funds allocation and general ledger reference data; and
- Confirming deposits.

b) **Disaster Recovery**

The OCC provides for the recovery of over 70 percent of the IRS workload capacity and 100 percent data availability in the event the PCC is disabled.

c) **MIS Reporting and Compliance Research**

The OCC provides the data storage and computing resources to support MIS reporting (standard and ad hoc) and Compliance Research activities directed from the other sites.

d) Program Support

- **Configuration Modifications**

  Changes in computer hardware, systems software, telecommunications, and applications are managed at the corporate level and include software version control and distribution.

- **Problem Management**

  Systems hardware, software, application, and telecommunications problems are reported to the corporate help desk for resolution, tracking, auditing, and reporting.

- **Security Profile Management**

  Profile data is maintained at the corporate level and distributed (when changes are applied) to sites housing local security databases for identification and authentication.

- **Static Data Maintenance**

  Static data is maintained at the corporate level and distributed to the appropriate sites when modifications are applied.

- **Systems Acceptance Testing**

  SAT, which is managed and controlled through the OCC, provides services to the NO/NC sites for SAT coordination and execution.

VOLUME VII – CONCEPT OF OPERATIONS

DATA

IV. Data

All corporate data is managed in the Modernization architecture following the principle of centrally stored, managed, and authoritative data.

IV.A Level I

Corporate data residing in locations other than the computing centers is either static data for read-only access (managed and transmitted from the computing centers) or collected data to be transmitted to the PCC for further processing. Access and updates to the corporate data are controlled through standard data access and update APIs and executed in the mainframe environment at the PCC based on message-based transaction requests from other sites. Background data access and updates, also performed at the PCC, use the same APIs except in special circumstances where custom access methods are employed to support performance requirements (e.g., MIS/DSS extracts). Periodically, the corporate databases are replicated at the OCC to support recovery capabilities[1].

Chart IV-1, Modernized Target - Data Topology Model, identifies each of the corporate databases as described in the technical architecture. For additional database structure material, please refer to the *Modernization Blueprint* - Volume IV, Technical Architecture.

[1] The exact method of replication is to be determined in the Level III analysis.

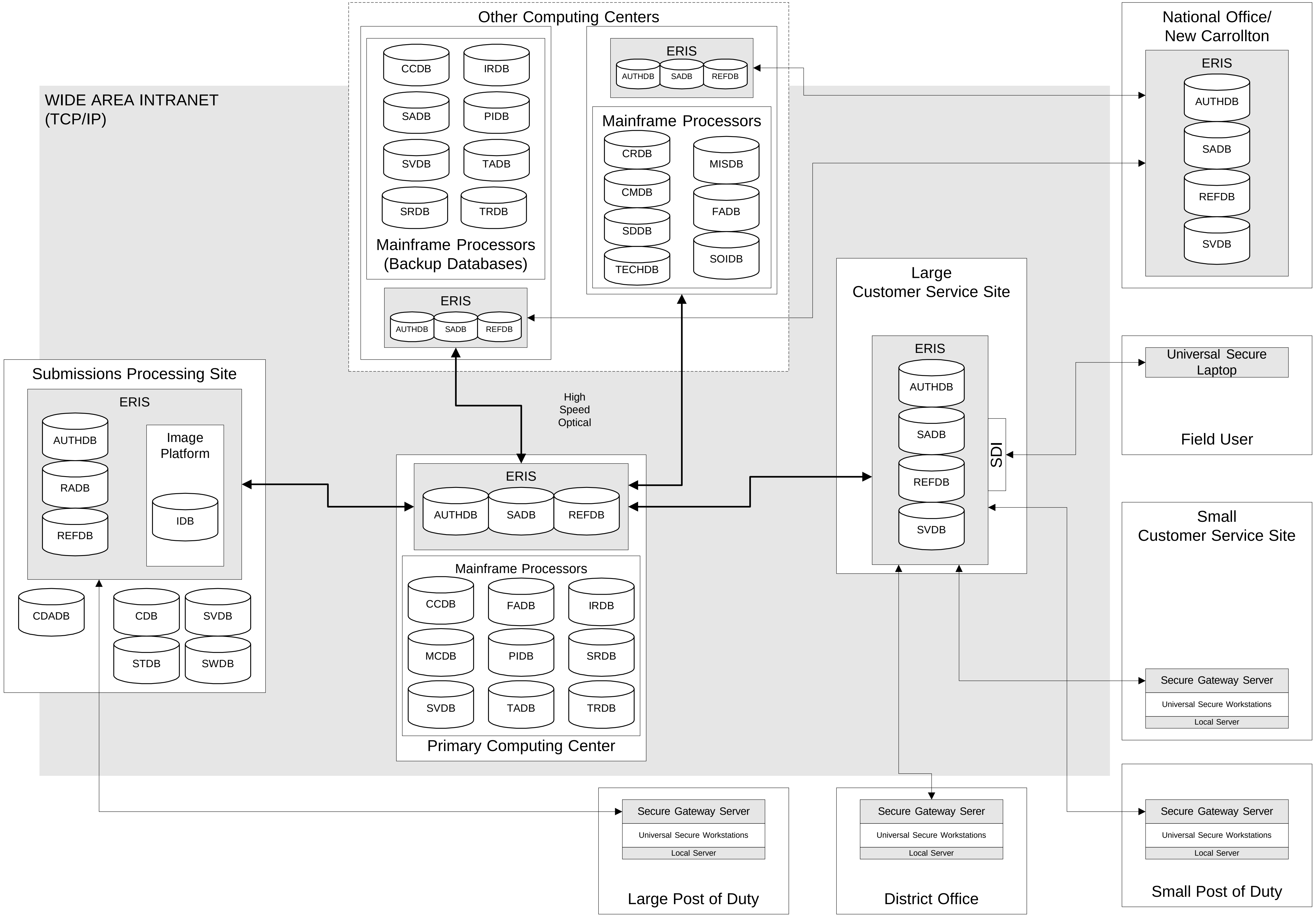

CHART IV-1 | Modernization Target - Data Topology Model

IV.B Submissions Processing Site

Data used to support the SPS for Submissions Processing are categorized as follows:

✦ Security data;

✦ Image data;

✦ Reference data;

✦ Submissions data; and

✦ MIS data.

Security audit-trail data is managed locally at the SPS in data structures identical to the corporate structures. Audit-trail information is captured for every business event and transaction and stored at the SPS until it is transmitted successfully to the SADB. Security profile data, managed in the PCC and transmitted to the SPS as updates are applied, is stored locally to control access to applications. The Authentication Database (AUTHDB) is located on the PCC ERIS and is used to identify and authenticate incoming messages and transactions from the Internet and approved transmitters.

After tax and information returns, remittances, and correspondence are identified and assigned unique tracking numbers (IDs), the Submissions Tracking Database (STDB) at the SPS is updated, and each item is tracked throughout the processing performed at the SPS. Scanned images of tax and information returns, remittances, and correspondence are stored on the SPS IDB and made accessible as needed from any end-user location. The image locations are forwarded to the PCC and stored on the appropriate corporate database (e.g., the TRDB for returns, the PIDB for remittances, and the CCDB for correspondence). Data collected through the automated data capture engines (e.g., ICR) and the verification process (using reference data stored on the Static Value Database (SVDB)) is stored in the CDB and the Character Data Archive Database (CDADB) to establish an audit trail of the data originally collected versus downstream data modifications.

IV.C Primary Computing Center

The PCC is the warehouse for all corporate data. The location of the data (mainframe or ERIS) is dependent on the use of the information throughout the enterprise. All corporate-mainframe-based databases are maintained in relational data structures. Static data that supports ASSAs, Customer Service, and Compliance is maintained on the PCC ERIS platform and distributed to the ERIS sites when approved modifications have been applied. State tax-return data that is submitted electronically through the Joint Federal/State Electronic Filing program is stored at the PCC in the SRDB.

Security data is organized into the following major databases:

✦ AUTHDB, which consists of the data required to protect data, validate users (including taxpayers), restrict system resources and data accesses, and manage certificates; and

- SADB and the regional audit databases, which, together, consist of the collected audit-trail data used to track and audit behaviors observed by technical mechanisms that secure sensitive data and other system resources.

The AUTHDB is maintained at the corporate level and managed on the ERIS platform. IRS user data is updated periodically (at a minimum, daily) and delivered to each ERIS location within the enterprise, where logon by IRS employees is controlled and managed. In addition, real-time updates and the distribution of IRS employee AUTHDB information is available for events that require immediate update.

Taxpayer data stored on the AUTHDB is located only at the PCC and is replicated, for disaster recovery purposes, at the OCC. Taxpayer account transactions through ASSAs use AUTHDB information to identify and authenticate taxpayers taking advantage of these automated applications.

The SADB is the centralized repository of all security audit data collected from the ERIS-based regional audit databases.

Appendix B of the *Modernization Blueprint* - Volume IV, Technical Architecture, details the structure and content of the corporate databases. All the databases defined in the technical architecture are maintained at the PCC except those maintained in the SPS (the CDADB, the CDB, the IDB, the STDB, and the Submissions Workload Database (SWDB)) and those maintained in the OCC (the MIS/DSS databases).

IV.D Customer Service Sites

Data used to support the Large CSS are categorized as follows:

- Security audit trail information (from the regional audit databases) and profile information (from the AUTHDB);

- Static data supporting ASSAs, reference material data (e.g., penalty and interest computations) for CSRs, and ATL data;

- Corporate authoritative data for tax accounts, cases, entities, tax and information returns, payments, and images; and

- MIS data.

The regional audit databases are managed locally at the Large CSS in data structures identical to the corporate structures. Audit-trail information is captured for every business event and transaction and then stored at the Large CSS until it is transmitted successfully to the SADB. AUTHDB information, which is managed in the PCC and transmitted to the Large CSS as updates are applied, is stored locally to control access to applications.

Data in the SVDB including the scripts for VRU sessions, ATL scripts and reference data, filing locations, and hours is stored at the Large CSS within the RCS and the ERIS. This data is managed at the corporate level and transmitted to the Large CSS when updates occur.

Corporate data is located in the PCC and accessed as it is needed. This data is not stored locally within the Large CSS: transactions that update corporate data are processed against the corporate databases using corporate data service applications. Critical corporate data used to support issue resolution includes, but is not limited to, the following:

- Taxpayer entity data including TIN, name, and address;
- Taxpayer account data including current balances, account transactions, applied payments, and adjustments;
- Case data including status, history, notes, agreements, appeals, open and closed issues, work investigations, and litigation;
- Tax-return and information-return data;
- Payment data, including source of payment, received date, and deposit date; and
- Images of tax returns and correspondence controlled through the PCC and maintained in the SPSs.

MIS data is located in the PCC and updated for each transaction processed from the Large CSS.

IV.E District Office/Post of Duty

Data used to support the DO/POD is categorized as follows:

- Security audit trail and profile data;
- Static data supporting non-account-related cases for walk-ins, reference material data (e.g., penalty and interest computations), and ATL data;
- Corporate authoritative data for tax accounts, cases, entities, tax and information returns, payments, and images;
- MIS data; and
- DSS data.

The regional audit databases are managed locally at the Large CSS in data structures identical to the corporate structures. Audit trail information is captured for every business event and transaction and stored at the Large CSS until it is transmitted successfully to the SADB. AUTHDB information, managed in the PCC and transmitted to the Large CSS as updates are applied, is stored locally to control access to applications.

Data on the SVDB including ATL data and reference data such as filing locations and hours is stored at the Large CSS or SPS within the RCS and the ERIS. This data is managed at the corporate level and transmitted to the Large CSS and the SPS when updates occur.

Corporate data is located in the PCC and accessed as it is needed. This data is not stored locally within the DO/POD: transactions that update corporate data are processed against the corporate databases using corporate data service applications. Critical corporate data used to support case processing includes, but is not limited to, the following:

- Taxpayer entity data including TIN, name, and address;
- Taxpayer account data including current balances, account transactions, applied payments, and adjustments;
- Case data including status, history, notes, agreements, appeals, open and closed issues, work investigations, and litigation;
- Tax-return and information-return data;
- Payment data, including source of payment, receipt date, and deposit date; and
- Images of tax returns and correspondence controlled through the PCC and maintained in the SPSs.

MIS data is located in the PCC and updated for each transaction processed from the DO/POD.

DSS data is located at the OCC and accessed through the Large CSS or the SPS ERIS from the Secure Gateway Server at the DO/POD.

IV.F Field

Data used to support the field user is categorized as follows:

- Security audit trail and profile data;
- Static data supporting non-account-related cases for reference material data (e.g., penalty and interest computations) and ATL data;
- Corporate authoritative data for tax accounts, cases, entities, tax and information returns, payments, and images; and
- MIS data.

Regional audit database information is encrypted and stored on universal secure laptops in data structures identical to the corporate structures. Audit-trail information is captured for every business event and transaction and stored on the universal secure laptop until it is transmitted successfully to the SADB. Transmittal is accomplished through the Secure Dial-in facility connected to the ERIS at the nearest Large CSS or SPS. AUTHDB information is established when the universal secure laptop is assigned to the field user.

Data on the SVDB including ATL data and reference data such as filing locations and hours is stored at the Large CSS or SPS within the RCS and the ERIS. This data is managed at the corporate level and transmitted to the Large CSS and the SPS when updates occur. Access to this data is supported through the Secure Dial-in facility.

Corporate data located in the PCC is encrypted and downloaded to the universal secure laptop through the Secure Dial-in facility on request. Case management controls at the corporate level notify other users of the status of this downloaded data to minimize data integrity issues. Critical corporate data used to support case processing includes, but is not limited to, the following:

- Taxpayer entity data including TIN, name, and address;
- Taxpayer account data including current balances, account transactions, applied payments, and adjustments;
- Case data including status, history, notes, agreements, appeals, open and closed issues, work investigations, and litigation;
- Tax-return and information-return data;
- Payment data, including source of payment, receipt date, and deposit date; and
- Images of tax returns and correspondence controlled through the PCC and maintained in the SPSs.

MIS data is located in the PCC and updated for each transaction processed from the universal secure laptop.

IV.G National Office/New Carrollton

Data used to support the field user is categorized as follows:

- Security audit trail and profile data;
- Corporate data;
- Static data;
- Financial accounting data; and
- MIS and DSS data.

The regional audit databases are managed locally on the NO/NC ERIS in data structures identical to the corporate structures. Audit trail information is captured for every business event and transaction and is stored at the NO/NC until it is transmitted successfully to the SADB at the PCC. AUTHDB information, managed in the PCC and transmitted to the NO/NC as updates are applied, is stored locally to control access to applications.

Corporate and static data used for Financial Reporting and processing that is located at the PCC includes, but is not limited to, the following:

- SVDB;
- TADB (filer accounts and revenue disbursements);
- PIDB (revenue receipts);
- CCDB (adjustments pending review, workload and staffing parameters, and scheduling); and
- TRDB (tax returns).

Financial data is located in the OCC and is composed of centralized corporate data that consists of the following key components:

- General ledger;
- Journal entries and summaries;
- Accounting statistics; and
- Administrative transactions.

MIS data is located in the PCC and is updated for each transaction processed from the NO/NC through the OCC. This data is used for national level program and priority management reporting such as the execution and monitoring of the enterprise-wide compliance plan.

DSS data is located in the OCC and is built from extracts of the CCDB, the Information Returns Database, the PIDB, the TADB, and the Tax Returns Database, which are located in the PCC.

IV.H Other Computing Centers

The OCC is used as a central warehouse for the following:

- Replicated corporate databases, located primarily at the PCC, support disaster recovery. One hundred percent of the mission-critical databases, including the security databases, the CCDB, the IRDB, the PIDB, the TADB, and the TRDB, are available in a recovery situation;
- MIS/DSS databases (the CRDB, the Management Information Systems Database (MISDB), and the Statistics of Income Database (SOIDB)) are created by extracting data from the replicated corporate databases. These databases are used for standardized and ad hoc management reporting, research, statistical reporting, and performance monitoring and measurement;

- FADB[2] supports Financial Reporting capabilities including standardized and custom reporting and data maintenance functions (e.g., G/L accounts); and

- Program support databases, which manage program-critical functions such as the CMDB, the Software Development Database (SDDB), and the Technical Support Database (TECHDB).

Secure access to this data is provided through the universal secure workstation, the AUTHDB, and the security infrastructure components within the ERIS.

[2] The location of this database is to be determined during the Level III and Level IV analyses.

VOLUME VII – CONCEPT OF OPERATIONS

SECURITY

V. Security

The *Modernization Blueprint* security framework builds on existing systems to provide a practical approach to migrate from today's environment to an integrated system supported by the modernized mainframe-centric platform. The target framework includes centrally managed privacy and security access controls, a single universal secure workstation for user access connected by a standardized network infrastructure, and the secure transport of information regardless of the source and destination of the data. This approach ensures full security is integrated in all applications and data access paths within the architecture.

V.A Level I

The *Modernization Blueprint* provides security management capabilities consisting of the following major elements at all levels of the architecture:

- Access-authorization capabilities that facilitate universal logon and the management of all identification and authentication data and role-based access control data that restrict access to taxpayer data and corporate resources to enable consistent access control based on a need-to-know basis. In addition, access authorization capabilities provide real-time security event handling that defines patterns of behavior to be monitored by the browsing and intrusion detection technical applications, manages thresholds used to trigger security alarms, and initiates corrective action such as the shutdown of input devices for selected violations;

- Secure Dial-in remote access control through a secure modem bank on the ERIS required for dial-up access to Modernization subsystems by remote IRS employees[1],

- Intrusion-detection capabilities that enable the detection of system intrusion or attempted system intrusion by external unauthorized sources;

- Browsing prevention, based on case assignment data, that prevents end users from browsing tax information for TINs and accounts not associated with cases assigned to them;

- Cryptographic management capabilities that manage cryptographic parameters and algorithms, the use of protocols between communicating entities, and cryptographic keys that perform encryption and decryption processes to protect sensitive but unclassified information in transport or storage (e.g., universal secure laptops);

- Digital signature management capabilities that manage all IRS electronic marking control data, such as signature certificates received from third-party certification authorities for nonrepudiation, and validate public keys through certificate services; and

[1] SDI may include specialized access tokens such as the Secure ID cards.

- Audit capabilities that manage the security audit process from setting and distributing audit criteria through audit analysis and the generation of audit reports.

V.B Submissions Processing Site

Authorization for end-user access to Submissions Processing systems through the universal secure workstation is invoked during the logon process using the security profile data and security applications on the ERIS. End-user access is based on the user's logon ID and is limited to applications approved by his or her manager. After the end user is logged into an application (e.g., correct tax return), the workflow management application automatically delivers the next item in the queue to the workstation. Because the end user cannot select an item to process the risk of unauthorized staff viewing or changing of returns or payments is eliminated. In addition, negative and positive TIN-list enforcement is used to limit access to specific TINs by specific end users. This information is stored and maintained in the AUTHDB.

Internet security is based on the interaction types that follow: [2]

- Internet tax-return filing;
- Internet correspondence submission;
- ASSAs for non-account-related activities; and
- ASSAs for account-related activities.

V.C Primary Computing Center

Messages and transactions received at the PCC have been authorized at the originating location through the nationwide ERIS connections. Further security algorithms are applied at the PCC based on the type of event and the data affected by the event. For example, taxpayer identification information resident on the corporate databases is used to verify the request for data; the verification algorithm returns its results to the originating application.

Browsing prevention algorithms are located on the mainframe processor and invoked whenever an inquiry transaction is executed. These algorithms use a combination of business rules and CCDB information to ensure the end user is accessing appropriate data. Unauthorized browsing attempts are prevented, logged, and reported to security administration personnel for follow-up action.

[2] Any request that requires account-related activities, including the submission of a tax return, will use a number of identification and authentication techniques to be determined. Non-account-related activities will be protected by the firewall between the Internet server and the other ERIS components. Access to static data (e.g., Automated Tax Law) will be initiated from the Internet server and use peer-to-peer security techniques to prevent the Internet user from unauthorized access of corporate assets.

Identification and authentication COTS products are used to support external data transmissions (e.g., electronic tax- and information-return filings) to the IRS through the CCG.

Background applications are secured through the operating system's COTS[3] products.

Audit trail data is stored on each ERIS platform and transmitted periodically to the SADB at the PCC. Extensive security reporting capabilities, including ad hoc queries, provide audit reports to the security administrators for review and follow-up action.

V.D Customer Service Sites

Taxpayers who access the CSS through the telephone do not invoke security algorithms *unless* they choose an ASSA that requires access or update capabilities with corporate data. When one of these applications is invoked, identification and authentication algorithms accessing the AUTHDB at the PCC are used to ensure the data access and update requests are appropriate for the taxpayer initiating the telephone call.

Authorization for CSRs to access the systems through the universal secure workstation is invoked during the logon process using the security profile data and security applications on the ERIS. The CSR can only access applications that have been approved and stored in his or her employee profile. After the CSR is connected, case data is used during issue resolution processing to ensure the CSR does not browse through unrelated data. In the event a CSR is working a non-account case, detection mechanisms are used to detect unauthorized browsing of corporate information.

V.E District Office/Post of Duty

Authorization for DO/POD employee (e.g., Revenue Agent, Revenue Officer, and Tax Auditor) access to the systems through the universal secure workstation (connected to the local Secure Gateway Server) is invoked during the logon process using the security profile data and security applications on the ERIS. The employee can only access applications that have been approved and stored in his or her employee profile. After a Revenue Agent, a Revenue Officer, or a Tax Auditor is connected, case data is used during issue resolution processing to ensure he or she does not browse through unrelated data. In the event the employee is working a non-account case, detection mechanisms are used to detect unauthorized browsing of corporate information.

V.F Field

Authorization for field users to access systems from the universal secure laptop is established when the universal secure laptop is assigned. In addition to a universal logon

[3] COTS products have not been selected.

ID, the field user is issued a token[4] for unique identification while accessing corporate data and applications through the Secure Dial-in facility.

When the field user has successfully logged in, encrypted downloads and uploads are limited to the assigned cases from his or her DO/POD. Data stored on the universal secure laptop is encrypted to prevent unauthorized access to sensitive taxpayer and account data in the event a universal secure laptop is lost or stolen.[5]

V.G National Office/New Carrollton

Authorization for NO/NC employees to access the systems through the universal secure workstation is invoked during the logon process using the security profile data and security applications on the ERIS. The end user can only access applications that have been approved and stored on his or her employee profile. Once connected, financial and account data is used during issue resolution processing to ensure employees do not browse through unrelated data. In the event a CFO staff member is working a non-account case, detection mechanisms are used to detect unauthorized browsing of corporate information. Corporate Case Management functions used to manage the nationwide parameters supporting automated case management capabilities are accessed in the same manner.

V.H Other Computing Centers

Messages and transactions received at the OCC have been authorized at the originating location through the nearest ERIS connection. Further security algorithms are applied at the OCC based on the type of event and the data affected by the event. For example, taxpayer identification information resident on the corporate databases is used to verify the request for data; the verification algorithm returns its results to the originating application.

Browsing prevention algorithms are located on the mainframe processor and invoked when an inquiry transaction is executed. These algorithms use a combination of business rules and CCDB information to ensure the end user is accessing appropriate data. Unauthorized browsing attempts are prevented, logged, and reported to security administration personnel for follow-up action.

Identification and authentication COTS products are used to support external data transmissions (e.g., electronic tax- and information-return filings) to the IRS through the CCG.

Background applications are secured through the operating system’s COTS products.

Audit-trail data is stored on each ERIS platform and transmitted periodically to the SADB at the PCC. Extensive security reporting capabilities, including ad hoc queries, provide audit reports to the security administrators for review and follow-up action.

[4] Specific tokens will be determined during Level III and Level IV analysis and design.

[5] The specific nature of the encryption and keys is to be determined.

VOLUME VII – CONCEPT OF OPERATIONS

INFRASTRUCTURE

VI. Infrastructure

The infrastructure architecture that supports Modernization is comprised of multiple tiers: mainframe processors at the computing centers; the ERIS, RCS, and LAN servers at the remaining sites; and the universal secure workstations and universal secure laptops that provide end-user access to corporate resources. Internet access for taxpayers is provided through Internet servers on the ERIS platform that are separated from the other ERIS components by a firewall. Bulk data transmissions from external sources (e.g., electronic tax returns from paid preparers and electronic information returns from taxpayers) are received through the CCG, which is also resident on the ERIS platform. The following configurations are based on the modeled topology; many different combinations of components and sites will exist when the Modernization architecture is fully deployed.

VI.A Level I

The mainframe processors, located in the computing centers, support all corporate OLTP as well as background applications, data management capabilities, disaster recovery services, and program management services such as configuration management, operations management, and performance and capacity management.

The ERIS and RCS platforms, located in the larger regional and computing center sites, provide data and voice communication and messaging services to the sites and between them. They also provide security identification, authentication, role-based access control, audit trails, ACD, VRU, predictive dialing capabilities, data interchange services, Internet connectivity, and Secure Dial-in facilities. ***Chart II-1, Modernization Target - Geographic Topology Model,*** includes examples of the various ERIS and RCS configurations by modeled site type.

The local servers provide both data communication support between the universal secure workstations and an ERIS location (for smaller sites), a LAN, and office automation products and support for local users.

“Universal secure workstation” is the generic term used to describe the following six classes of workstations:

- Class 1: Network Personal Computer (PC) is a very thin client hosting a Web browser (or generic graphical display software) used to access corporate applications. In the target environment, most workstations will be Class 1;

- Class 2: Thin Client PC is a transitional workstation used to access corporate applications while the architecture is being deployed to handle both target and legacy application access;

- Class 3: Office Automation is a workstation that also provides Class 1 services;

- Class 4: Development Workstation supports NT and UNIX platforms;

- Class 5: Computer-aided Design/Computer-aided Manufacturing (CAD/CAM) Workstation supports specialized document design functions; and

- Class 6: Universal Secure Laptop is used by field personnel to perform face-to-face Compliance activities and download and upload encrypted case and account data from the corporate platform through the Secure Dial-in facility on the ERIS.

Telecommunications is comprised of differently sized pipes between the sites and the WAN, depending on the message traffic and performance requirements. Gateways on the RCS and the local servers provide the interface based on transmission control protocol/interface protocol (TCP/IP) and systems network architecture (SNA) protocols to the WAN. Devices connected to RCS and local servers typically incorporate the 100baseT protocol.

VI.B Submissions Processing Site

The primary infrastructure components of the SPS described in Appendix A are as follows:

- **ERIS** to support telecommunications and security between SPS, the PCC, and other sites (e.g., the DOs) (for Submissions Processing, the ERIS supports the image platform for the scanning of material, image-based data capture of return and payment information, and workflow management tools);

- **Secure Dial-in** to support secure dial-in communications from IRS employee laptops for communications with the PCC;

- **Local Server** to support local office automation and network management capabilities;

- **Universal Secure Workstation** to interface with the applications; and

- **Internet Server** to accept Internet-based transactions (return filing, correspondence, and ASSAs).

VI.C Primary Computing Center

The primary infrastructure components of the PCC described in Appendix A are as follows:

- **Mainframe Processors** to support corporate data management, corporate applications, enterprise-wide transaction and message processing, and program support capabilities;

- **ERIS** to support telecommunications and security between the PCC and the other sites, data transmissions from external sources, and the mainframe computers (from the universal secure workstations used at the PCC);

- **Local Server** to support local office automation and network management capabilities; and

- **Universal Secure Workstation** to interface with the applications.

VI.D Customer Service Sites

The primary infrastructure components of the CSS described in Appendix A are as follows:

- **ERIS and RCS** to support telecommunications and security between Large CSS and the PCC, other sites, and the telephone systems;
- **Secure Dial-in** to support secure dial-in communications from IRS employee laptops for communications with the PCC;
- **VRU** to process ASSA requests based on stored scripts;
- **ACD** to distribute calls throughout the CSS;
- **PD** to use case data from the PCC to contact taxpayers and, when connected, deliver the calls and data to the CSRs;
- **Local Server** to support local office automation and network management capabilities.
- **Secure Gateway Server** (at the Small CSS) to provide connectivity between the universal secure workstations and the nearest ERIS; and
- **Universal Secure Workstation** to interface with the applications.

VI.E District Office/Post of Duty

The primary infrastructure components of the DO/POD described in Appendix A are as follows:

- **Local Server** to support local office automation and network management capabilities;
- **Secure Gateway Server** to provide connectivity between the universal secure workstations and the nearest ERIS; and
- **Universal Secure Workstation** to interface with the applications.

VI.F Field

The primary infrastructure component of the field described in Appendix A is as follows:

- **Universal Secure Laptop** that provides the field user with the same capabilities as DO and POD users.

VI.G National Office/New Carrollton

The primary infrastructure components of the NO/NC described in Appendix A are as follows:

- **ERIS** to support telecommunications and security between the NO/NC, the PCC, and the OCC;
- **Local Server** to support local office automation and network management capabilities; and
- **Universal Secure Workstation** to interface with the applications.

VI.H Other Computing Centers

The primary infrastructure components of the OCC described in Appendix A are as follows:

- **Mainframe Processors** to support corporate data management, corporate applications, enterprise-wide transaction and message processing, and program support capabilities. Configurations of the OCC are similar to the PCC but have capacities tailored to support the capabilities at each center;
- **ERIS** to support telecommunications between the OCC, the other sites (e.g., NO/NC) and the mainframe computers (from the universal secure workstations used at the PCC); and
- **Universal Secure Workstation** to interface with the applications.

VOLUME VII – CONCEPT OF OPERATIONS

APPLICATIONS

VII. Applications

A fundamental concept of the Modernized architecture is insulation, whenever it is practical and cost-effective, of the data from the applications and of the applications from the infrastructure. To achieve this goal, message services technology, integrated with transaction processing, is employed to obtain the optimum efficiencies and performance.

VII.A Level I

The application architecture consists of COTS and custom software components integrated on the mainframe, ERIS, and RCS platforms within the corporate domain. In the target environment, the only software on the universal secure workstations (except the universal secure laptops) is a Web browser (or generic graphical display software). Universal secure laptops that support remote field activities use applications that simulate the corporate environment.[1]

Appendix C provides a complete list of the modernized applications, at the subsystem level, and the platforms on which they reside.

VII.B Submissions Processing Site

The ERIS-based applications are as follows:

- Security profile maintenance;
- Security audit reporting;
- General document imaging;
- Remittance document imaging;
- Input and correction;
- Electronic filing;
- Interactive telephone filing;
- Financial submissions processing;
- Submissions validation and perfection; and
- Submissions tracking and management.

[1] The applications might be delivered through a CD-ROM that contains encoded applications requiring specialized "keys" to invoke them in the remote environment. The specific details are to be determined during the Level III analysis.

VII.C Primary Computing Center

The applications and software services supported in the PCC are categorized as follows:

- Business applications; and
- Infrastructure support services.

VII.C.1 Business Applications

The mainframe-processor-based applications are as follows:

- Validate and post corporate data;
- Account settlement;
- Issue refunds;
- Issue detection;
- Telephone call management;
- Case creation and management;
- Notice and correspondence printing, review, and correction;
- Case analysis and resolution;
- Local case management;
- Financial reporting;
- Refund status queries;
- Assessment statute expiration;
- Collection statute expiration;
- Combined annual wages;
- Credit- and debit-card payments;
- Cross-reference relationships;
- Exam unallowables;
- Federal/state agreements;
- Federal unemployment tax;

- FTD payment schedules;
- Filing requirement determination and changes;
- Foreign tax;
- Tax treaty;
- Foreign income;
- Hardship pleas;
- Interest computation expert;
- Payment tracer;
- Problem resolution program;
- Questionable tax issues;
- Refund and abatement statute expiration;
- Return-free filing;
- Return delinquencies;
- Settlement agreements;
- Extension of time to pay;
- Tax-return adjustments;
- Underreporter;
- User fees;
- Withholding-at-source;
- Installment agreements;
- Balance due queries;
- TeleTax;
- Transcript: order copy of a return;
- Transcript: order copy of taxpayer account transcript;
- Payoff inquiry and processing;

- PIN assignment;
- TIN assignment, validation, and correction;
- Refund tracer;
- Reasonable cause penalty abatement;
- Refund release;
- Address change;
- Offset notice response;
- Agreed response assessments;
- Automated W-4 computation;
- Levies;
- Liens;
- Revenue Officer account data updates;
- Revenue Agent examination data updates;
- MIS extracts;
- DSS extracts;
- Reference data maintenance;
- Third-party processing; and
- Compliance research.

VII.C.2 Infrastructure Support Services

The ERIS-based services are as follows:

- Operations management;
- Security management;
- Operating system services;
- Data interchange services;
- Telecommunications services;

- Transaction processing and messaging services; and
- Network management.

The mainframe-processor-based services are as follows:

- Operations management;
- Security management;
- Operating system services;
- Data interchange services;
- Telecommunications services;
- Transaction processing and messaging services;
- Corporate data routing;
- Print Farm;
- Data archive; and
- Migration, backup, and recovery.

VII.D Customer Service Sites

VII.D.1 Large Customer Service Site

The ERIS-based applications are as follows:

- Security profile maintenance; and
- Security audit reporting.

The RCS-based applications are as follows:

- ASSA; and
- ATL.

VII.D.2 Small Customer Service Site

The Small CSS provides the same capabilities as the Large CSS except for ERIS capabilities.

The Small CSS uses the Secure Gateway Server to provide the connectivity between the universal secure workstations and an ERIS location (an SPS or a Large CSS) that provides full security services for the Small CSS. Through this connection, Small CSS end users interact with the PCC to access corporate data and applications.

VII.E District Office/Post of Duty

The local-server-based applications are as follows:

- Office automation products.

VII.F Field

The universal-secure-laptop-based applications are as follows:

- Compliance tools; and
- Office automation products.

VII.G National Office/New Carrollton

The ERIS-based applications are as follows:

- Security profile maintenance; and
- Security audit reporting.

The local-server-based applications are as follows:

- Office automation products.

VII.H Other Computing Centers

The applications and software services supported in the OCC are categorized as follows:

- Business applications; and
- Infrastructure support services.

VII.H.1 Business Applications

The mainframe-processor-based applications are as follows:

- Financial Reporting; and
- Corporate research.

VII.H.2 Infrastructure Support Services

The ERIS-based services are as follows:

- Operations management;

- Security management;
- Configuration management;
- Operating system services;
- Data interchange services;
- Telecommunications services;
- Transaction processing and messaging services; and
- Network management.

The mainframe-processor-based services are as follows:

- Operations management;
- Security management;
- Configuration management;
- Operating system services;
- Data interchange services;
- Telecommunications services;
- Transaction processing and messaging services;
- Corporate data routing;
- Data archive; and
- Migration, backup, and recovery.

VOLUME VII – CONCEPT OF OPERATIONS

APPENDIX A

Appendix A: Principles

A. Background

The principles for the CONOPS state the preferred architectural direction and guidance for the following four primary architectural models:

- ✦ Work processes and data flows (work);
- ✦ Data (information);
- ✦ Applications; and
- ✦ Security and infrastructure (technology).

These principles establish the context for architectural design decisions throughout the IRS, providing direct statements of how the IRS will use technology and technology-enabled processes (e.g., business process reengineering) for target modernization efforts. At each level of the CONOPS, the principles provide direction and guidance to all levels of requirements development and engineering activities. Exceptions to the principles, if required, may be obtained through the change control process governed by the Systems Life Cycle.

B. Principles

- ✦ **Work Processes and Data Flows**
  - ▲ Information shall be captured in computer-readable form as close to the source of origin as possible, including external resources and forms prepared and submitted by the public.
  - ▲ Electronic exchange of data (e.g., EDI) between trading partners shall be used when information is received from or transmitted to external agencies, taxpayers, and third-party stakeholders.
  - ▲ Automated image-based data capture technology shall be used to capture data from paper documents.
  - ▲ Paper and electronic submissions shall be subject to identical edits and controls.
  - ▲ Common business processes shall be implemented consistently to provide interoperability and reusability.
  - ▲ Telephone- and Internet-based self-service tax applications shall use the same script structure and data as automated interaction with taxpayers.
  - ▲ Incoming telephone calls from taxpayers shall be routed to the appropriate application and the CSR in a timely manner regardless of the work location of the CSR.

  - Field personnel (e.g., Revenue Agents and Revenue Officers) shall be provided with the same capabilities as office-based personnel.

- **Data**

  - Corporate authoritative data shall be available for secure, nationwide access regardless of the origin or method of contact by the taxpayer or IRS employee.

  - Corporate data access shall be isolated from business application logic and external trading partners.

  - All data assets shall be centrally managed and controlled.

  - Authoritative data shall be archived and purged as soon as its required retention period(s) is reached.

- **Infrastructure**

  - Information systems shall be designed to comply with the Modernization architecture as described in the *Modernization Blueprint*.

  - The Modernization infrastructure shall provide for cost-effective business recovery capabilities.

  - The Modernization infrastructure components shall be designed and implemented to facilitate monitoring and measurement.

  - The Modernization infrastructure shall minimize the use of proprietary technology, using standards-compliant system components.

  - Technology investments shall leverage existing investments.

  - The Modernization architecture shall use modular components with standardized interfaces to support flexibility, scalability, reusability, and evolution.

  - The end user shall use the universal secure workstation and the universal secure laptop to access corporate assets.

  - Applications that provide interactive services to IRS employees, taxpayers, and stakeholders shall be provided through a common, secure graphical presentation interface.

- **Security**

  - The security framework shall conform to the Department of Treasury's information system security policies.

- The security infrastructure shall ensure the security of all corporate information and resources.
- The security infrastructure shall protect information resources commensurate with the risk and magnitude of harm resulting from their loss, misuse, or unauthorized access or modification.
- The security infrastructure shall proactively (prevention and detection) protect the privacy of information about individuals.
- Security shall conform to appropriate government and industry specifications and standards.
- Work processes, data flows and access, infrastructure components, and applications shall provide privacy and non-disclosure capabilities that warrant public confidence.
- Access to corporate resources (i.e., infrastructure, data, and applications) shall be provided on a need-to-know basis.
- Corporate authoritative data shall be separated from research and decision support data.
- Each business transaction shall be tracked and maintained and made available for review through automated audit trails.

✦ **Applications**

- Modernization applications based on existing business requirements shall use the best-in-breed legacy applications currently providing these capabilities.
- Application components shall be designed and implemented to facilitate monitoring and measuring.
- Common user interface components and applications standards shall be used to provide user interface services.
- Applications shall be based on shared, reusable components.
- Applications shall be platform independent.
- Applications shall not be based on proprietary components.
- Application distribution shall be centrally managed and controlled.

VOLUME VII – CONCEPT OF OPERATIONS

APPENDIX B

Appendix B: Infrastructure Components

Many Modernization infrastructure components are used in multiple locations. This section presents a summary of the general component capabilities for Level II and placeholders for Level III and IV components. The hardware, software, and applicable standards for each component will be developed during Levels III and IV.

- **ERIS**
  - Capabilities
    - Security Services
      - IRS employee identification and authentication
      - Access control
      - Auditing
      - Public and private key encryption
      - Internet- and intranet-secure firewall
      - Secure docking
      - Secure dial-in
      - File encryption
      - Token encryption
    - Telecommunication Services
      - TCP/IP
      - Routing/data communication utility (DCU)
      - Universal wiring
      - LAN/WAN
      - CCG (in the PCC)
      - Intranet service-provider capabilities
      - Transaction processing and monitoring services
      - Message brokering and monitoring services

  - X.400 message services
  - X.500 directory services

- Application Services
  - Non-account ASSA interface from the Web server(s) and telephone client
  - Universal secure workstation software (e.g., Web browser interface)
  - Image-based data-capture services
- System Services
  - Database management (for ASSA application access to static data)
  - Resource utilization and monitoring services
  - Capacity planning and modeling services
  - Network management services
  - Hardware
  - Software
  - Applicable Standards

- ✦ **Internet Server**
  - ▲ Capabilities
    - Gateway for corporate-account-based ASSA
    - Platform for non-account-based ASSA
  - ▲ Hardware
  - ▲ Software
  - ▲ Applicable Standards

- **Secure Gateway Server**
  - Capabilities
    - Connectivity between the smaller sites and an ERIS location for access to corporate assets
  - Hardware
  - Software
  - Applicable standards
- **Local Server**
  - Capabilities
    - Office automation and other administrative capabilities
  - Hardware
  - Software
  - Applicable standards
- **Mainframe Processors**
  - Capabilities
    - Security Services
      - Taxpayer identification and authentication (through the AUTHDB)
      - Resource utilization auditing
      - Corporate security maintenance (AUTHDB)
      - Security audit trail consolidation (SADB)
    - Telecommunication Services
      - TCP/IP
      - SNA
      - CSCR

  - Transaction processing and monitoring services
  - Message brokering and monitoring services
- Application Services
  - ASSA interface to corporate applications from the Web server and telephone client
  - Data synchronization services between the PCC and the OCC
- System Services
  - Database management (for corporate data)
  - Resource utilization and monitoring services
  - Capacity planning and modeling services
  - Network management services
  - Operations management services
  - Configuration management services
  - SAT services
  - Problem management services
  - Disaster recovery services
- Hardware
- Software
- Applicable standards

- **National Contact Manager (i.e., CSCR)**
  - Capabilities
    - Nationwide call routing services and load balancing for incoming telephone calls to Customer Service and Compliance
  - Hardware

  - Software
  - Applicable standards
- **RCS**
  - Capabilities
    - VRUs provide the initial link with taxpayers calling into the IRS, obtaining basic information from the taxpayer for call routing purposes. They also provide the ASSA scripts and interaction with the corporate platform for account-based transactions and an option for taxpayers who prefer to leave a voice mail message.
    - Automated call distribution
    - Predictive-dialing services
    - Regional call routing
  - Hardware
  - Software
  - Applicable standards
- **Universal Secure Workstation - Class 1 and Class 2**
  - Capabilities
    - Secure end-user access to corporate applications
  - Hardware
  - Software
  - Applicable standards
- **Universal Secure Workstation - Class 3**
  - Capabilities
    - Office automation services for desktops not requiring access to corporate assets
  - Secure end-user access to corporate applications
  - Hardware

  - Software
  - Applicable standards

- **Universal Secure Workstation - Class 4**
  - Capabilities
    - Software development capabilities to Information Systems (IS) employees and contractors
  - Hardware
  - Software
  - Applicable standards
- **Universal Secure Workstation - Class 5**
  - Capabilities
    - CAD/CAM and application capabilities for specialized, high-end program support requirements
  - Hardware
  - Software
  - Applicable standards
- **Universal Secure Workstation - Class 6**
  - Capabilities
    - Full field capabilities for Compliance end users
  - Hardware
  - Software
  - Applicable standards
- **Telecommunications**
  - Capabilities
    - WAN and LAN support for nationwide access to corporate data regardless of the requestor's location

  - Integrated voice and data support for Customer Service and Compliance telephone activities

- Hardware

- Software

- Applicable standards

VOLUME VII – CONCEPT OF OPERATIONS

APPENDIX C

Appendix C: Subsystem Environment Summary

The *Modernization Blueprint* - Volume IV, Technical Architecture, describes each of the Modernization subsystems in detail. The following tables summarize all of the subsystems and the general technical environments in which they reside.

		Environments				
Subsystem Name	**Subsystem ID**	**Corp**	**Reg**	**End User**	**Laptop**	**Notes**
Decision Support	CO.03.01	OLTP				
Interactive Decision Support	CO.03.02			X		
Portable Case Analysis and Resolution	CO.07.01				X	
Accept, Validate, and Store TRDB Data	CP.01.01	Batch				
Accept, Validate, and Store TADB Data	CP.01.02	Batch				
Accept, Validate, and Store PIDB Data	CP.01.03	Batch				
Accept, Validate, and Store IRDB Data	CP.01.04	Batch				
Accept, Validate, and Store CCDB Data	CP.01.05	Batch				
Corporate Data Update Services	CP.01.06	OLTP			X	
Corporate Data Routing	CP.01.07	Batch				
Online Transaction Account Settlement Services	CP.02.01	OLTP			X	
Account Settlement	CP.02.02	Batch				
Issue Detection	CP.03.01	Batch				
Generate Notices and Correspondence	CP.04.01	OLTP				
Data Archive	CP.05.01	Batch				
Corporate Data Synchronization	CP.05.02	Batch				
Migration, Backup, and Recovery	CP.05.03	Batch				

		Environments				
Subsystem Name	**Subsystem ID**	**Corp**	**Reg**	**End User**	**Laptop**	**Notes**
Issue Control and Maintenance	CP.06.01	Batch				
Manage Workload and Cases	CP.06.02	Batch				
Corporate Data Access Services	CP.07.01	OLTP			X	
Reference	CP.07.02	OLTP				
Entity Search	CP.07.03	Batch				
Data Extract	CP.08.01	Batch				
MIS Reporting	CP.08.02	OLTP Batch				
Reference Data Maintenance	CP.09.01	OLTP Batch				
MIS Data Maintenance	CP.09.02	OLTP Batch				
Telephone Client Application	CS.01.01		X			
Predictive Dialer Management	CS.01.02		X			
Internet Client Application	CS.01.03		X			
National Contact Manager	CS.04.01	OLTP				
Automated Tax Law Management	CS.05.01		X			
Non-Account Taxpayer Assistance	CS.05.02	OLTP				
Case Analysis and Resolution	CS.06.01	OLTP				
Case Processing Presentation	CS.06.02			X	X	

		Environments				
Subsystem Name	**Subsystem ID**	**Corp**	**Reg**	**End User**	**Laptop**	**Notes**
Local Case Assignment and Management	CS.07.01	OLTP				
Revenue General Ledger Interface	FR.05.01	Batch				
Revenue General Ledger	FR.06.01	Batch OLTP				Period ending processing Online data capture
System Development Toolkit	IS.01.01	DEV				
Corporate Platform Development Toolkit	IS.01.02	DEV				
Regional Platform Development Toolkit	IS.01.03		DEV			
User Platform Development Toolkit	IS.01.04			DEV	DEV	
Integration and Test Toolkit	IS.02.01	INT	INT	INT	INT	
Capacity Management	IS.03.01	X				
Operations Management	IS.03.02	X	X	X	X	Monitoring capabilities
Configuration Management	IS.03.03	X				
Problem Management	IS.03.04	X				
Network Management	IS.03.05	X	X	X	X	
Security Management	IS.04.01	X	X	X	X	
Operating System Services	IS.05.01	X	X	X	X	Operating systems
Computer-Human Interface Services	IS.05.02			X	X	
Data Management Services	IS.05.03	X	X			

		Environments				
Subsystem Name	**Subsystem ID**	**Corp**	**Reg**	**End User**	**Laptop**	**Notes**
Data Interchange Services	IS.05.04		X			
Telecommunications Services	IS.05.05	X	X			
Transaction Processing Services	IS.05.06	X	X			
Workflow Management Services	IS.05.07	X	X			
Automated Call Distributor	IS.05.08		X			
Secure Dial-in	IS.05.09		X			
Voice Response	IS.05.10		X			
Print Farm	IS.05.11		X			
High-Volume Image Processing	IS.05.12		X			
Networks	IS.05.13	X	X	X	X	
Corporate Platforms	IS.05.14	OLTP Batch				
Regional Platform	IS.05.15		X			
User Platforms	IS.05.16			X	X	
Office Automation	IS.05.17			X	X	
National Call Router	IS.05.18	X	X			
Predictive Dialer	ISA.05.19		X			
Distributed Process Computing	IS.05.20	X	X			
Regional Call Router	IS.05.21		X			
Manual Operations	ManOps					N/A

		Environments				
Subsystem Name	**Subsystem ID**	**Corp**	**Reg**	**End User**	**Laptop**	**Notes**
Open Issue	Open Issue					N/A
General Document Imaging	SP.01.01		X			
Remittance Document Imaging	SP.01.02		X			
Submission Data Storage	SP.01.03		X			
Input and Correction Facility	SP.01.04			X		
Submission Electronic Filing	SP.02.01		X			
Interactive Telephone Filing	SP.02.02		X			
Financial Submissions	SP.03.01		X			
Submission Validation and Perfection	SP.04.01		X			
Submission Tracking and Management	SP.05.01		X			

VOLUME VII – CONCEPT OF OPERATIONS

APPENDIX D

Appendix D: Glossary of Business Terms

Abatement—A reduction or cancellation of an assessed tax.

Access Control—A range of security mechanisms, such as administrative procedures, physical hardware, and software, designed to limit sensitive system assets accessibility to only authorized users and processes.

Account Data—Administrative and tax related data associated with the filers' accounts such as entity data, tax return data (including the legal representation of electronic return data), information return data, receipt data (including user fees), data captured from miscellaneous submissions (e.g., correspondence and applications) case data (case administrative and case history data), statistics derived from the analysis of filer accounts, and any other data elements that require association with the entity, tax, or non-tax account modules.

Account Identifier—A Taxpayer Identification Number (TIN) that is used to uniquely identify a taxpayer's account, i.e., Social Security Number (SSN), Employer Identification Number (EIN), or Individual Taxpayer Identification Number (ITIN).

Account Module—An aggregation of a type of data for a specific filer; can be an entity, tax or non-tax module.

Accounting Classification Structure (ACS)—An information classification structure which provides the means for categorizing financial information along several dimensions as needed to support financial management and reporting functions.

Activity—The actual work, task, or step performed in producing and delivering products and services. An aggregation of actions performed within an organization useful for activity - based costing.

Amended Return—A return or claim submitted by a filer that updates or replaces information on the original return.

Application—A paper or electronic form that is completed by a business or an individual and submitted to the Internal Revenue Service (IRS) for review, verification and action. Examples of applications include Employee Plan (EP) applications, Exempt Organization (EO) applications, filer election forms, reporting agent forms, representative forms and paid preparer forms.

Assertion—A legal term for determination of a liability for a non-tax-related charge.

Assessment—Enforceable claims for non-exchange revenue for which specific amounts due have been determined and the person from whom the tax or duty is due has been identified. They include both self-assessments made by persons filing tax returns and assessments made by the collecting entities as a result of audits, investigations, and litigation. Specifically excluded from the definition of assessments, as used in this statement, are compliance assessments. Compliance assessments, as defined by the Internal Revenue Service (IRS) and Customs, do not represent financial receivables.

Audit—An independent review and examination of records and activities. An audit may be conducted in order to test the adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedure.

Authentication—The means used to verify that users are who they claim to be (by password) and identify equipment such as workstations (by system tags).

Authorization—The granting of rights to a user, program, or process. Also, the rights held by a user, program, or process.

Backup—To store operational data into a secondary storage to make it available in case of system failure.

Budgetary Accounting—Budgetary accounting measures and controls the use of resources according to the purposes for which budget authority was enacted; and that records receipts and other collections by source. It tracks the use of each appropriation for specified purposes in separate budget accounts through the various stages of budget execution from appropriation to apportionment and allotment to obligation and eventual outlay. It is used to set priorities, to allocate resources among alternative uses, to finance these resources, and to assess the economic implications of federal financial activity at an aggregate level.

Budget Authority—The authority provided by Federal law to incur financial obligations that will result in immediate or future outlays. Specific forms of budget authority include:

- Appropriations, which may be provided in appropriations acts or other laws and which permit obligations to be incurred and payments to be made;

- Borrowing authority, which permits obligations to be incurred but requires funds to be borrowed to liquidate the obligation;

- Contract authority, which permits obligations to be incurred but requires a subsequent appropriation or offsetting collections to liquidate the obligations; and

- Spending authority from offsetting collections, which permits offsetting collections to be credited to an expenditure account and permits obligations and payments to be made using the offsetting collections (the offsetting collections credited to an account are deducted from gross budget authority of the account).

Budget authority may be classified by period of availability (1-year, multiple-year, or no year), by nature of the authority (current or permanent), by the manner of determining the amount available (definite or indefinite), or as gross (without reduction of offsetting collections), and net (with reductions of offsetting collections).

Case—A uniquely identifiable collection of issues that require resolution and must be tracked and managed by the system.

Case History—A record of case activity and status such as specific worker actions, status history, case assignee history, resolution site/location history, data requested, and quality assurance status/resolution.

Case Notes—Narrative descriptions of steps taken during case resolution. They can be input by the worker or systematically generated.

Chart of Accounts—The list of general ledger account numbers that subdivide basic accounting equations, with associated titles and definitions, used by an entity for posting to its general ledger. See also U.S. Government Standard General Ledger.

Check Digit—Two alphabetic characters that the system generates by applying a mathematical formula to the Social Security or Employer Identification Number. The check digit is used to ensure that the Taxpayer Identification Number (TIN) corresponds with the proper filer.

Container—An envelope, box, or other enclosure used to mail paper documents.

Corporate Data—Includes both account data and non-account data.

Correct Submission—A submission that passes all validations and posts without causing any issues to be generated.

Corrected Submission—A submission with correction issues that have been corrected, either by the system or an operator, so it can be processed like a correct return.

Correction—The process of *automatically* rectifying errors, to the extent possible, contained in a submission. This may include entity validation, inter-field checking, tax rate determination, and other calculations.

Correction Issue—An error (e.g., math error, missing mandatory data) detected in the contents of a submission that requires correction.

Correspondence—Any letters, notices, e-mail, facsimile transmissions received or sent by the Internal Revenue Service (IRS).

Cryptography—Principles, means, and methods for presenting plain information in a manner which renders the information unrecognizable and for restoring encrypted information to recognizable form.

Customer Service Representative (CSR)—Customer Service Representatives (CSRs) perform all customer service and compliance operations at the customer service site that do not require face-to-face contact with the taxpayer.

Deposit record—Records of deposits made by taxpayers or third parties into Internal Revenue Service (IRS) bank accounts. Deposit records sent to the IRS include summary and header data containing bank information, the tax type or fee code of the deposit, and the total amount of the deposit. Deposit records also include receipt and receipt adjustment records that identify the entity to which the receipt is applied, the tax type or fee code of the receipt, the amount of the receipt and, if applicable, the tax period of the receipt.

Deposit-in-Transit—Information which is stored during the initial processing of a receipt, received directly by the Internal Revenue Service (IRS), that indicates the amount, date, tax type, and tax period of the receipt. It is used to record "fact of payment" on a filer's account.

Disbursement—A payment made by the Internal Revenue Service (IRS), such as refund payments to taxpayers, interagency transfers, and payments for goods and services received. Methods of payment include cash, check and electronic funds transfer.

Disbursement schedule—A schedule of payments to recipients requiring certification by a Certifying Officer prior to disbursement.

District Office—A site type that is responsible for face-to-face taxpayer contact case processing, including office and field examinations, field collection activities, appeals, criminal investigations, education and outreach, and face-to-face taxpayer assistance.

Electronic Signature/Authorization—Electronic marking control data (e.g., signature certificate, public and private keys, checksum routines, digitized hand signatures, and digitized voice signatures) to provide non-repudiation, data integrity, and authentication.

Entity—In reference to filers or taxpayers, refers to the identifying information associated with the filer or taxpayer, such as name, address and taxpayer identification number.

Exchange Revenue—Inflows of resources to a governmental entity that the entity has earned. They arise from exchange transactions, which occur when each party to the transaction sacrifices value and receives value in return.

Exempt Organization—An organization that has applied for and received approval from the Internal Revenue Service (IRS) as being exempt from paying income taxes, in accordance with current tax laws. Examples of organizations that may be approved as exempt are charities, religious groups, and not-for-profit foundations.

Fact of Filing—The recording on the Internal Revenue Service (IRS) database of record, of the official receipt of a valid tax return.

Fact of Payment—The recording on the Internal Revenue Service (IRS) database of record, of the official receipt of a valid payment.

Failure—Result or fact that does not meet the system's normal behavior.

Fault—Defects that cause a system to malfunction.

Federal Accounting Standards Advisory Board (FASAB)—A board established by the Secretary of the Treasury, the Director of the Office of Management and Budget (OMB), and the Comptroller General to recommend federal accounting principles and standards.

Fee Code—A code representing a specific source of revenue. Sources of revenue include penalty, interest, photocopy fees, determination fees, Employee Plans (EPs)/Exempt Organization (EO) application fees, chief counsel fees, and installment agreement fees.

Filer—An individual, business, or third party that has a legal obligation to file a tax return, information return, or other required tax documents, per Internal Revenue Code.

Filer Account—The aggregation of a filer's entity information, financial account, tax return, and information reports spanning multiple tax periods. It has one entity module and multiple tax and non-tax modules.

Financial Account—The cumulative financial data for all tax modules for a specific taxpayer.

First Read—The process of determining the contents of white mail, electronic representations (i.e., facsimile), voice mail, and electronic mail/Internet mail.

Federal Reserve Board (FRB) Member Bank—A financial institution designated under 31 CFR 202 as a depositary and financial agent of the U.S. Government and authorized by Treasury to perform lock box services for Federal agencies. FRB member banks are a limited subset of third party processors, consisting of only a handful of commercial institutions, which consolidate all of the third party processor receipts and deposit them in the appropriate Treasury funds through the FRB.

General Ledger—The ledger that contains all of the financial accounts of a business, organization, or government agency; contains offsetting debit and credit accounts (including control accounts); organized by the Chart of Accounts (COA) and subsidiary ledger(s). Represents the highest level of summarization of accounting data for a financial system, supported by subsidiary ledgers at varying levels of detail. All transactions to record financial events must post, either individually or in summary to the General Ledger.

Hardware Resources—Processing environments hosting applications and network devices.

Information Return—Documents required by the Internal Revenue Service (IRS) to be submitted by third parties (e.g., banks, employers, other government agencies) that provide tax-related information regarding taxpayers, such as wages, other income, payments, or cash transactions.

Information System—An assembly of hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Inquiry—Customer-initiated requests or questions that are received in the form of written (e.g., correspondence) or oral (e.g., telephone) communication.

Inquiry Case—A case that is a taxpayer assistance-oriented system workload. An inquiry case addresses workload associated with taxpayer-initiated contacts whether written, telephonic, or electronic. Inquiry cases do not contain issues. See also case.

Individual Taxpayer Identification Number (ITIN)—A taxpayer identification number given by the Internal Revenue Service (IRS) to a non-US resident who does not qualify for a Social Security Number (SSN).

Investigation Issue—A condition detected in a taxpayer account indicating that the taxpayer may not be compliant with the Internal Revenue Code (IRC). Investigation issues are converted into cases and assigned to Customer Service Representatives (CSRs) or field service personnel for resolution.

Issue—A detected condition that causes specialized error resolution or investigation processing to be performed on a submission or account. Types of issues include perfection issues, posting issues, and investigation issues. One or more issues may be included in a single case.

Joint Financial Management Improvement Program (JFMIP)—Joint cooperative undertaking of the Office of Management and Budget (OMB), General Accounting Office (GAO), the Department of Treasury, and the Office of Personnel Management (OPM); working in cooperation with each other and with operating agencies to improve financial management practices throughout the government.

Journal—A record of accounts, in which is entered a condensed and grouped statement of the daily transactions.

Journal Entry—An entry record which contains the appropriate debit(s) and credit(s) to reflect the financial event of a business operation.

Ledger Account—A detailed record of related financial transactions.

Legal Representation—A picture, depiction or copy of a document that fulfills all requirements to be accepted as an equivalent original document for the purpose of evidence in a Federal court.

Levy—To notify a third party to pay to the Internal Revenue Service (IRS) amounts owed to the taxpayer. The third party is liable for the amount if it is not paid to the IRS. Can be a one time event or a recurring request, as in garnishing wages.

Lien—A legal claim, filed in the appropriate jurisdiction, to the property of a debtor taxpayer as security for payment of tax debts. Establishes the Internal Revenue Service (IRS) as a creditor.

Lockbox—A collection and processing service provided by financial institutions that accelerates the flow of funds to Treasury's General Account. This services includes collecting the agency's mail from a specified post office box, sorting, totaling, and recording the payments, processing the items, making the deposit and transferring the funds. Agencies receive remittance data either in hard copy or via electronic format.

Management Controls—IRS-wide controls embedded in the computer security and risk management programs. The management controls are based on public law, Office of Management and Budget (OMB) circulars, Treasury directives, and official Internal Revenue Service (IRS) policies. They are applicable to both current and future systems.

Management Information System (MIS) Data—Operational data consisting of and used to compile statistics regarding tax processing systems activity. Does not include statistics derived from values contained in filer accounts.

Mechanism—Security mechanisms for information systems are selected based on identified risks and cost/benefit analysis, where the cost includes acquisition, operational, and performance costs throughout the system's life cycle.

Modernization—An ongoing effort to modernize the Internal Revenue Service (IRS) information systems that deal with tax processing, tax administration, and management and administrative functions through business reengineering, streamlining, automation, and state-of-the-art technology.

Name Control—The first four letters of the taxpayer's last name (for individuals) or the first four letters of the business name. The name control is used to assure that the Taxpayer Identification Number (TIN) corresponds with the proper taxpayer.

Need-to-Know—The term given to the requirement that the dissemination of controlled information be limited strictly to those persons whose duties require access to, knowledge of, or possession of the information to perform official tasks or services.

Non-Account data—Tax processing data that is not associated with a specific filer; such as reference data (from both internal and external sources), workload management data (employee/site skills, resource availability), Management Information System (MIS) data (data describing the effectiveness of processing and the statistics computed on this data), and processing rules/algorithms (computational tools).

Noncompliance—A situation in which a taxpayer has not conformed to the tax regulations, either intentionally or unintentionally.

Non-Disclosure—The ability to prevent the viewing of information by unauthorized users or processes.

Nonexchange Revenue—Inflows of resources to the Government that the Government demands or that it receives by donations. The inflows that it demands include taxes, duties, fines, and penalties.

Notice—A predefined, system-generated letter that contains tax information specific to a filer's account.

Offsite storage—Storage that is located away from the operational site.

Operational Controls—Controls that are implemented and executed by individuals responsible for a particular application or group of applications. The operational controls are based on public law, Office of Management and Budget (OMB) circulars, Treasury directives, and official Internal Revenue Service (IRS) policies. They are applicable to both current and future systems.

Original Return—The first return submitted by a filer or transmitter for a specific tax type and tax period.

Partial Return—A return from which necessary data is missing.

Payment Voucher—A preprinted voucher which accompanies remittances made to the Internal Revenue Service (IRS). The voucher includes taxpayer entity information, tax type or fee code, amount of payment, and tax period covered by the payment.

Perfection—The process of *manually* identifying, to the extent possible, errors on a submission; such as missing schedules, missing signatures, or incomplete information.

Posting—The process of updating the taxpayer's account with incoming information received from the taxpayer, information received from a Customer Service Representative (CSR), or information derived after analyzing the taxpayer's account.

Posting Issue—A detected condition that prevents the update of a filer's account with newly received information.

Privacy—(1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. (2) The right to insist on adequate security of, and to define authorized users of, information or systems.

Privacy Act—PL 93-579, Privacy Act of 1974, a federal law intended to prevent unwarranted disclosure of personal and organizational information.

Published Products—Refers to either documents (products for internal consumption), publications (products for external consumption), or both.

Quicknote Form—Form sent to the taxpayer to request additional information on unprocessable submissions.

Receipts—A financial term describing the collections received by the Internal Revenue Service (IRS) from the public that result primarily from the exercise of the Government's sovereign or governmental powers. Examples of receipts are individual and corporation income taxes, Social Security taxes, excise taxes, penalties, interest, fee for service user charges, gifts, and contributions.

Remittances—Analogous to receipts; used only for Submissions Processing purposes.

Research Case—A case that addresses research-type tax system workload performed by compliance personnel, including special agents. A research case could result in the identification of issues or in some tax-related investigation activity that is not issue related. A research case becomes an issue case when an issue is identified for the research case. See also case.

Responsible Organizational Unit—An organizational entity defined by the Internal Revenue Service (IRS) (e.g., computing center, submissions processing site, customer service center).

Return of Record—The legally recognized tax return stored by the Internal Revenue Service (IRS). The return of record may be a composite view of the original return as well as corrections, adjustments, or amendments to the return.

Revenue Accounting Summary Transaction—Net summarization of business operations activities for a particular transaction code and tax type/fee code.

Seized Assets—Property/money taken from delinquent taxpayers to recoup back taxes owed to the Internal Revenue Service (IRS).

Seizure—The physical act of seizing real or personal property.

Settlement—The process of determining the outstanding tax liability of a tax module or the offset or refund of an overpaid tax module. It is performed periodically to incorporate updates to financial data in the tax module resulting from the posting of new data or from the adjustment of existing data.

Software Resources—Business and technical applications, databases, and communication applications.

Split Submission—A submission whose pieces have been physically split apart for processing.

Submission—Any incoming information, such as tax returns, payments, correspondence (including white mail), applications, and information reports (including currency transaction reports), that is directly related to filers and is used to determine the proper filing obligations and tax liabilities for filers. Submissions may be received either in paper or electronic format.

Substitute for Return—A procedure by which the Internal Revenue Service (IRS) is able to establish an account and examine the records of a taxpayer, and submit an IRS completed return for a taxpayer who refuses or is unable to file a tax return and information received indicates that a return should be filed.

Suspended Return—A return that cannot be further processed due to a condition in the return or the associated account. Processing is halted while awaiting additional information from the taxpayer or notification from Criminal Investigation to proceed.

Tax Module—The aggregation of all the tax financial information for a specific taxpayer, tax period, and tax class.

Taxpayer—An individual, partnership, corporation, organization or other entity that pays taxes.

Tax Period—The period of time for which a tax return is filed and the associated taxes are due. The Internal Revenue Service (IRS) uses a four digit code to indicate the end of the tax period for a given tax return. (The first two digits represent the year and the second two digits represent the month).

Tax Return—A document provided by a filer (or third party on behalf of a filer) to report information relative to income, deductions, or investments; to determine a tax liability or other information.

Tax Service User—Customer Service Representative, Field Compliance personnel, Compliance Research personnel, Submissions Processing personnel, or Chief Financial Officer (CFO) personnel.

Tax Type—Represents a specific source of revenue. Personal income, social security income, unemployment, gift, estate and gasoline taxes are examples of tax types.

Technical Controls—Controls that are executed by a computer system. The set of identified security services are technical controls based on Treasury Directive TD P 71-10, Treasury Security Manual. This set of services is required for both current and future systems.

Third Party—A person, financial institution or other organization that provides data to, or receives data from the Internal Revenue Service (IRS) for use in tax processing.

Third-Party Payment Processor—A financial institution under contract with the Department of the Treasury (Financial Management Service) to process tax remittances (e.g., checks, credit cards, cash, money orders, electronic funds transfers), deposit the proceeds in the Federal Reserve Bank, and provide the Internal Revenue Service (IRS) with information about the transaction.

Transaction Codes—Codes used to identify, categorize, and organize discrete units of information processed by an information system consistency.

Transmitter—An entity responsible for the electronic transmission of filer submissions.

Turnaround Document—A form sent to taxpayers for return to the Internal Revenue Service (IRS) with requested information (e.g., missing schedules, payments). It contains internal routing information and/or taxpayer identifying information to facilitate routing and processing.

U.S. Government Standard General Ledger (SGL)—A uniform chart of accounts and pro forma transactions used to standardize federal agency accounting and to support the preparation of standard external reports required by central agencies. Office of Management and Budget (OMB) and Treasury-FMS regulations require agencies to use the SGL to accumulate and report standard financial data. The SGL chart of accounts identifies and defines budgetary, proprietary, and memorandum accounts to be used in agency's accounting systems. The SGL is generic for the federal government, and is not intended to reflect any single federal agency's accounting system. The Federal Financial Management Improvement Act of 1996 requires agency financial management systems to comply with the SGL at the transaction level.

Unpostables—Transactions which cannot be posted to the filers' accounts.

Unprocessable—A condition where the data essential to processing is absent or corrupted, thus causing the processing to be aborted with an error condition. Primarily used in conjunction with forms processing.

Validation—Error identification performed on files and records, utilizing data contained within the file or record, tax rules, and other preexisting data.

Version Control—Process that uniquely identifies different releases and keeps track of the changes.

White Mail—Incoming correspondence (e.g., a letter from a taxpayer that is not on an approved Internal Revenue Service (IRS) form), whose contents cannot be determined until read by an IRS employee.

Work Item—A uniquely identifiable component of the Internal Revenue Service (IRS) tax processing system workload that is tracked by the system for management purposes. Work Items are the fundamental unit for the assignment of work to available resources. Work items encompass cases, correspondence, inquiries, research, certification and notice reviews.

VOLUME VII – CONCEPT OF OPERATIONS

APPENDIX E

Appendix E: List of Acronyms

ACD	Automated Call Distributor
ACH	Automated Clearing House
ACS	Accounting Classification Structure
API	Application Programming Interface
ASSA	Automated Self Service Application
ATL	Automated Tax Law
AUTHDB	Authentication Database
CAD/CAM	Computer-aided Design/Computer-aided Manufacturing
CCDB	Corporate Case Database
CCG	Common Communications Gateway
CDADB	Character Data Archive Database
CDB	Character Database
CD-ROM	Compact Disc Read-Only Memory
CFO	Chief Financial Officer
CIDS	Centralized Inventory Distribution System
CMDB	Configuration Management Database
COA	Chart of Accounts
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CRDB	Compliance Research Database
CSCR	Customer Service Call Routing
CSR	Customer Service Representative
CSS	Customer Service Site
DASD	Direct Access Storage Device
DCU	Data Communication Utility
DIF	Discriminate Information Function
DO	District Office
DSS	Decision Support System
EDI	Electronic Data Interchange
EIN	Employee Identification Number
EO	Exempt Organization
EP	Employee Plan
ERIS	Enhanced Regional Infrastructure System
FADB	Financial Accounting Database
FASAB	Federal Accounting Standards Advisory Board
FRB	Federal Reserve Board
FTD	Federal Tax Deposit

ICR	Intelligent Character Recognition
ID	Identifier
IDB	Image Database
IRA	Individual Retirement Account
IRC	Internal Revenue Code
IRDB	Information Returns Database
IRS	Internal Revenue Service
IS	Information Systems
ITIN	Individual Taxpayer Identification Number
JFMIP	Joint Financial Management Improvement Program
LAN	Local Area Network
MCDB	Master Correspondence Database
MIS	Management Information Systems
MISDB	Management Information Systems Database
NO/NC	National Office/New Carrollton
OCC	Other Computing Center
OLTP	Online Transaction Processing
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PC	Personal Computer
PCC	Primary Computing Center
PD	Predictive Dialer
PIDB	Payment Information Database
PIN	Personal Identification Number
POD	Post of Duty
PSP	Planning and Special Programs
PTN	Public Telephone Network
QA	Quality Assurance
RA	Revenue Agent
RADB	Regional Audit Databases
RO	Revenue Officer
RCS	Regional Call Services
RFC	Regional Finance Center
SADB	Security Audit Database
SAT	Systems Acceptance Testing
SDDB	Software Development Database
SGL	Standard General Ledger
SNA	Systems Network Architecture

SOIDB	Statistics of Income Database
SPF	Special Procedures Function
SPS	Submissions Processing Site
SQL	Structured Query Language
SRDB	State Return Database
SSA	Social Security Administration
SSN	Social Security Number
STDB	Submissions Tracking Database
SVDB	Static Value Database
SWDB	Submissions Workload Database
TA	Tax Auditor
TADB	Tax Accounts Database
TCP/IP	Transmission Control Protocol/Interface Protocol
TDD	Telecommunications Device for the Deaf
TECHDB	Technical Support Database
TIN	Taxpayer Identification Number
TRDB	Tax Return Database
VRU	Voice Response Unit
WAN	Wide Area Network