

# Chapter 9. Appendix

OTCnet Participant User Guide

Table of Contents

[Overview, Topics, and Audience 1](#_Toc94089086)

[Overview 1](#_Toc94089087)

[Topics 1](#_Toc94089088)

[Audience 1](#_Toc94089089)

[Topic 1 Appendix A. Administrative Notes 3](#_Toc94089090)

[Cost 3](#_Toc94089091)

[Minimal Paperwork 3](#_Toc94089092)

[Endpoint Policy 3](#_Toc94089093)

[OTCnet Endpoint Group Management 3](#_Toc94089094)

[User Training 3](#_Toc94089095)

[Customer Support Hours 4](#_Toc94089096)

[Look up Phone Numbers for Financial Institutions 4](#_Toc94089097)

[Topic 2 Appendix B. Password Requirements 5](#_Toc94089098)

[Topic 3 Appendix C. Image Quality 6](#_Toc94089099)

[Topic 4 Appendix D. Central Image Research (CIRA) Query 7](#_Toc94089100)

[Topic 5 Appendix E. CIRA CSV File Overview 8](#_Toc94089101)

[Introduction 8](#_Toc94089102)

[OTCnet Updates 8](#_Toc94089103)

[Layout 8](#_Toc94089104)

[Available Fields 8](#_Toc94089105)

[File Layout 10](#_Toc94089106)

[Sample File Layout 13](#_Toc94089107)

[CSV File Sample 14](#_Toc94089108)

[Topic 6 Appendix F. Master Verification Database (MVD) 16](#_Toc94089109)

[Topic 7 Appendix G. Representment 17](#_Toc94089110)

[Topic 8 Appendix H. Equipment Returns 18](#_Toc94089111)

[Topic 9 Appendix I. OTCnet Check Capture Codes 19](#_Toc94089112)

[ACH Return Reason Codes 19](#_Toc94089113)

[Check 21 Return Codes 20](#_Toc94089114)

[Transaction Status Code Monitoring 21](#_Toc94089115)

[OTCnet Processing Forward Files 22](#_Toc94089116)

[OTCnet Returns 22](#_Toc94089117)

[Topic 10 Appendix J. OTCnet Security 24](#_Toc94089118)

[Purpose 24](#_Toc94089119)

[What is PII? 24](#_Toc94089120)

[Access Control 24](#_Toc94089121)

[Personnel Security and Procedures 25](#_Toc94089122)

[Physical and Environmental Protection 26](#_Toc94089123)

[Contingency Planning 28](#_Toc94089124)

[Configuration Management 29](#_Toc94089125)

[System Maintenance 30](#_Toc94089126)

[System and Information Integrity 31](#_Toc94089127)

[Media Protection 32](#_Toc94089128)

[Incident Response 34](#_Toc94089129)

[Awareness and Training 34](#_Toc94089130)

[Summary 36](#_Toc94089131)

List of Figures

[Figure 1. Poor Image Quality 6](#_Toc94089132)

[Figure 2. Good Image Quality 6](#_Toc94089133)

[Figure 3. Image Quality Failed Message 6](#_Toc94089134)

[Figure 4. CIRA Query Image 7](#_Toc94089135)

[Figure 5. Manage Verification Tab 16](#_Toc94089136)

[Figure 6. Transaction Status Codes 17](#_Toc94089137)

List of Tables

[Table 1. File Layout of CSV Report 10](#_Toc94089138)

[Table 2. Sample File Layout 13](#_Toc94089139)

[Table 3. ACH Return Reason Codes 19](#_Toc94089140)

[Table 4. Check 21 Return Codes 20](#_Toc94089141)

[Table 5. Transaction Status Codes 21](#_Toc94089142)

Glossary

Click this [link](https://www.fiscal.treasury.gov/otcnet/training/wbt/content/course_OTC/glossary.htm) to access the full OTCnet Glossary.

## Overview, Topics, and Audience

### Overview

Welcome to the *Appendix*. In this chapter, you will learn about:

* Administrative detail for cost, paperwork, policy, training and customer service
* Password requirements
* How to resolve check Image quality
* How to query within Central Image Research Archive (CIRA)
* How to access the CIRA Comma Separated Value (CSV) File
* How to access the Master Verification Database (MVD)
* How to establish check representments
* The procedure for returning equipment
* How to verify check capture return codes
* Guidance for OTCnet Security

### Topics

This chapter is organized by the following appendixes:

1. Appendix A. Administrative Notes
2. Appendix B. Password Requirements
3. Appendix C. Image Quality
4. Appendix D. Central Image Research Archive (CIRA) Query
5. Appendix E. CIRA CSV File Overview
6. Appendix F. Master Verification Database (MVD)
7. Appendix G. Representments
8. Appendix H. Equipment Returns
9. Appendix I. OTCnet Check Capture Return Codes
10. Appendix J. OTCnet Security

### Audience

The intended audience for the *Appendix* Participant User Guide includes the following:

* Primary Local Security Administrator
* Check Capture Administrator
* Check Capture Operator
* Check Capture Lead Operator
* Check Capture Supervisor
* MVD Editor
* MVD Viewer
* CIRA Viewer

## Topic 1 Appendix A. Administrative Notes

### Cost

The Agency cost for participating in the program is limited to the purchase of hardware. Scanners, scanner cables, and USB flash drives can be purchased through a vendor of the Agency’s choice. The check scanner models supported are the RDM EC7000i and EC9100i; as well as the Panini MyVision Batch scanner models X-30, X-60, or X-90; Panini Vision X; and Panini I: Deal. All other computer hardware is purchased through another vendor or by contacting an OTCnet Deployment Specialist. The United States Department of Treasury/Bureau of the Fiscal Service (BFS) pays all other fees associated with the program, so there are no hidden software purchase costs or transaction fees.

### Minimal Paperwork

Agencies must submit a signed Agency Agreement (AA), Agency Participation Agreement (APA) and an Agency Site Profile (ASP) for each endpoint, and an interagency agreement, if purchasing hardware using IPAC. Once agreements are signed and received, the Agency can be up and running within 2-4 weeks.

### Endpoint Policy

An endpoint policy supports automation of an Agency check cashing/collection policy. The endpoint policy is based on the agency's overall program or policy to ensure a consistent application of an Agency-wide check verification including returned reason codes, suspension periods, and the inclusion of expired items. As part of the Agency’s participation in OTCnet, the agency provides the Treasury OTC Support Center their check collection policy via the ASP.

The endpoint policy is established during the set-up of an endpoint in the MVD system. Treasury OTC Support Center administers the set-up of all endpoints based on the Agency’s and the endpoint’s ASP. Treasury OTC Support Center administers all edits or modifications to an endpoint, including the endpoint’s policy.

### OTCnet Endpoint Group Management

The MVD restricts the display of data based on the endpoint of the user. A user only sees records that are associated with OTC Endpoints at or below the user’s OTC Endpoint in the hierarchy or at endpoints specified in the OTCnet Endpoint Group. Depending on the type of data being requested, different rules apply, as appropriate.

### User Training

The program offers comprehensive Web-Based Training (WBT), Participant User Guides, and printable job aids. It is recommended that you access the WBT and Participant User Guides before using OTCnet and before contacting your Treasury OTC Support Center Deployment Specialist will work with individuals to determine training type and schedule. To get the most out of the training session, it should be scheduled within two weeks of the Agency conversion date.

### Customer Support Hours

Customer support is available 24 hours a day, 7 days a week. All OTCnet related inquiries should be directed to the Treasury OTC Support Center at 866-945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4, or via email at fiscalservice.OTCChannel@citi.com.

### Look up Phone Numbers for Financial Institutions

For phone numbers and email addresses, go to www.fededirectory.frb.org.

Contact the Treasury OTC Support Center at 866-945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4 or via email at fiscalservice.OTCChannel@citi.com.

## Topic 2 Appendix B. Password Requirements

Password requirements are implemented as a security measure.

* End users will set up their own passwords to login to OTCnet Online application through the Configuration Service Provider (CSP) **ID.me.**
	+ If end users forget their password, and they are not using a **PIV**/**CAC**, they will go through **ID.me** to reset their passwords.
* OTCnet specific passwords only apply to the following:
	+ Logging into OTCnet Offline
	+ Logging into OTCnet Local Bridge
	+ Online and Offline Supervisor Override
	+ Offline authentication to Online passwords to download online data
* Password requirements include:
	+ Passwords must be at least **12** characters long.
	+ Passwords have a maximum limit of **64** characters
	+ Password cannot be the word *password* and cannot be the same as the user login
	+ Passwords are case-sensitive
	+ Passwords must be unique from the previous ten passwords used for each user
	+ Passwords must not have been used in the last 10 days
	+ Passwords must not have more than two repeating characters
	+ Passwords must not be shared with other users or put in a written, unsecured form
	+ Passwords must not be a word in a language, slang, dialect or jargon
	+ Passwords must not be related to personal identity, history, environment or other personal associations
* Single Sign On (OTCnet login window) suspends a user’s access to the system after three unsuccessful login attempts.
	+ The OTCnet system settings default is set to three unsuccessful login attempts before suspension and cannot be customized

## Topic 3 Appendix C. Image Quality

The scanner functionality has a feature that verifies the image quality of every check scanned. Agencies can, however, choose to override a poor quality image. Agencies must be aware that overriding a poor quality image may result in a returned item, depending upon the paying financial institution. Figure 1 illustrates a poor quality image, Figure 2 presents a good image and Figure 3 presents an *Image Quality Failed* message.

Figure 1. Poor Image Quality



Figure 2. Good Image Quality



Figure 3. Image Quality Failed Message



## Topic 4 Appendix D. Central Image Research (CIRA) Query

The Central Image Research Archive (CIRA), as shown in Figure 4, is the central database where all check images are stored for seven years after the initial scan and processing in OTCnet.

Figure 4. CIRA Query Image



As a **CIRA Viewer**, **MVD Viewer** and **MVD Editor**, you are authorized to utilize the CIRA query function in OTCnet to search for and locate checks.

## Topic 5 Appendix E. CIRA CSV File Overview

### Introduction

As an OTCnet user, you may have to download the CIRA CSV file. This user guide contains all of the fields available in the CIRA CSV report in OTCnet. The CSV report provides input data for downstream systems and provides OTCnet users with the ability to download item information in a standard format.

### OTCnet Updates

In OTCnet, the following updates were made to the file format:

1. The column which was titled **Location** in PCC OTC is now called **OTC Endpoint**. This column is now populated with the OTC Endpoint short name.
2. The column which was titled **Check Type** in PCC OTC is now called **Item Type**.
3. Two additional columns were added to the CSV report generated in OTCnet.
	* A column entitled **Agency Location Code plus 2 (ALC+2)**. The ALC+2 column is automatically populated with the ALC+2 that was selected for the submitted item\*
	* A column entitled **Return Settlement Date**. The Return Settlement Date column is automatically populated with the effective date of settlement of the returned check item

\* Endpoints that were migrated from PCC OTC may contain the same value for OTC Endpoint and ALC+2. This is not an error and does not interfere with the data generated by this report.

### Layout

The CIRA CSV report consists of multiple lines, defined as follows:

* Each line is terminated by a carriage return followed by a new line (0D0A)
* The first five lines always existed. The agency’s item data begins on line 6
* The file is terminated by an empty line followed by 0D0A

### Available Fields

All possible fields found in the report are as follows\*:

* **Individual Reference Number (IRN)**
* OTC ENDPOINT
* ALC +2
* CAPTURE DATE
* RECEIVE DATE
* BANK ROUTING NUMBER
* CHECK NUMBER
* ACCOUNT
* AMOUNT
* CASHIER ID
* ITEM TYPE
* PROCESSING METHOD
* BATCHID
* SETTLEMENT DATE
* RETURN SETTLEMENT DATE
* DEBIT VOUCHER NUMBER
* DEPOSIT TICKET NUMBER
* User Field 1
* User Field 2
* User Field 3
* User Field 4
* User Field 5
* User Field 6
* User Field 7
* User Field 8
* User Field 9
* User Field 10
* User Field 11
* User Field 12
* User Field 13
* User Field 14
* User Field 15
* User Field 16
* User Field 17
* User Field 18
* User Field 19
* User Field 20
* User Field 21
* User Field 22
* User Field 23
* User Field 24

\*Some labels in the CSV report appear slightly different than they do in other parts of OTCnet. This does not impact the download.

Location = OTC Endpoint

User Field = User Defined Field

Processing Mode = Processing Method (future)

Check Type = Item Type (future)

### File Layout

This section defines the size of all fields and the order the fields are laid out within the file:

Table 1. File Layout of CSV Report

| Line Number | Field Number | Name | Type | Format/Sample | Description |
| --- | --- | --- | --- | --- | --- |
| 1 | BLANK | Report Title | String | CSV Agency Detailed Item Report | Report Title Constant |
| 2 | BLANK | Date/Time | String | Thu May 05 12:27:53 EDT 2005 | Date that the report was executed |
| 3 | BLANK | Total Amount | String | TOTAL AMOUNT : | Constant String |
| 3 | BLANK | Total Amount Value | Float | 39594.43 | Total dollar amount of the items queried |
| 4 | BLANK | Total number of items | String | TOTAL NUMBER OF ITEMS : | Constant String |
| 4 | BLANK | Total number of items value | Number | 81 | Number of items queried |
| 4a | BLANK | Error message | String | TOTAL NUMBER OF ITEMS EXCEEDS 65000. RETURNING FIRST 65000 ITEMS | Error message displayed if the number of items in the CSV exceeds 65,000 items. |
| 5 | BLANK | IRN | String | IRN | Constant String column header, value of the IRN |
| 5 | BLANK | OTC ENDPOINT | String | OTC ENDPOINT | Constant String column header, ALC+2 |
| 5 | BLANK | ALC + 2 | String | ALC + 2 | Constant String column header, ALC + 2 |
| 5 | BLANK | CAPTURE DATE | String | CAPTURE DATE | Constant String column header, Time the image and data was originally captured |
| 5 | BLANK | RECEIVE DATE | String | RECEIVE DATE | Constant String column header, Time the data was processed by OTCnet |
| 5 | BLANK | TRANSIT NUMBER | String | TRANSIT NUMBER | Constant String column header, Routing number parsed from RAW MICR |
| 5 | BLANK | CHECK NUMBER | String | CHECK NUMBER | Constant String column header, Check number parsed from RAW MICR |
| 5 | BLANK | ACCOUNT | String | ACCOUNT | Constant String column header, Account number parsed from RAW MICR |
| 5 | BLANK | AMOUNT | String | AMOUNT | Constant String column header, Amount of the payment |
| 5 | BLANK | CASHIER ID | String | CASHIER ID | Constant String column header, Value provided by A L C+2 for the operator id |
| 5 | BLANK | ITEM TYPE | String | ITEM TYPE | Constant String column header, Item Type – either “Personal” or “Non-Personal” |
| 5 | BLANK | PROCESSING METHOD | String | PROCESSING METHOD | Constant String column header, Processing Method – 3 options “Customer Not Present”, “Customer Present” or “Back Office” |
| 5 | BLANK | BATCH ID | String | BATCH ID | Constant String column header. Batch containing the IRN |
| 5 | BLANK | SETTLEMENT DATE | String | SETTLEMENT DATE | Constant String column header. Settlement Date |
| 5 | BLANK | RETURN SETTLEMENT DATE | String | RETURN SETTLEMENT DATE | Constant String column header. Return Settlement Date |
| 5 | BLANK | DEBIT VOUCHER NUMBER | String | DEBIT VOUCHER NUMBER | Constant String column header. Debit Voucher Number |
| 5 | BLANK | DEPOSIT TICKET NUMBER | String | DEPOSIT TICKET NUMBER | Constant String column header. Deposit Ticker Number |
| 5 | BLANK | USER FIELD 1 | String | USER FIELD 1 | Constant String column header |
| 5 | BLANK | USER FIELD 2 | String | USER FIELD 2 | Constant String column header |
| 5 | BLANK | USER FIELD 3 | String | USER FIELD 3 | Constant String column header |
| 5 | BLANK | USER FIELD 4 | String | USER FIELD 4 | Constant String column header |
| 5 | BLANK | USER FIELD 5 | String | USER FIELD 5 | Constant String column header |
| 5 | BLANK | USER FIELD 6 | String | USER FIELD 6 | Constant String column header |
| 5 | BLANK | USER FIELD 7 | String | USER FIELD 7 | Constant String column header |
| 5 | BLANK | USER FIELD 9 | String | USER FIELD 9 | Constant String column header |
| 5 | BLANK | USER FIELD 10 | String | USER FIELD 10 | Constant String column header |
| 5 | BLANK | USER FIELD 11 | String | USER FIELD 11 | Constant String column header |
| 5 | BLANK | USER FIELD 12 | String | USER FIELD 12 | Constant String column header |
| 5 | BLANK | USER FIELD 13 | String | USER FIELD 13 | Constant String column header |
| 5 | BLANK | USER FIELD 14 | String | USER FIELD 14 | Constant String column header |
| 5 | BLANK | USER FIELD 15 | String | USER FIELD 15 | Constant String column header |
| 5 | BLANK | USER FIELD 16 | String | USER FIELD 16 | Constant String column header |
| 5 | BLANK | USER FIELD 17 | String | USER FIELD 17 | Constant String column header |
| 5 | BLANK | USER FIELD 18 | String | USER FIELD 18 | Constant String column header |
| 5 | BLANK | USER FIELD 19 | String | USER FIELD 19 | Constant String column header |
| 5 | BLANK | USER FIELD 20 | String | USER FIELD 20 | Constant String column header |
| 5 | BLANK | USER FIELD 21 | String | USER FIELD 21 | Constant String column header |
| 5 | BLANK | USER FIELD 22 | String | USER FIELD 22 | Constant String column header |
| 5 | BLANK | USER FIELD 23 | String | USER FIELD 23 | Constant String column header |
| 5 | BLANK | USER FIELD 24 | String | USER FIELD 24 | Constant String column header |
| 5 | BLANK | AGENCY ACCOUNTING CODE, DESCRIPTION AND CLASSIFICATION AMOUNT | String | AGENCY ACCOUNTING CODE, DESCRIPTION AND CLASSIFICATION AMOUNT | Constant String Column Header, accounting code value, description and classification amount |
| 5 | BLANK | VOUCHER DATE | String | VOUCHER DATE | Constant String column header, Time the voucher was originally created |
| 5 | BLANK | ACR TYPE | String | ACR TYPE | Constant String, column header containing the ACR Type |
| 5 | BLANK | ACR REASON CODE | String | ACR REASON CODE | Constant String, column header containing the ACR Reason Code |
| 5 | BLANK | ACR ALC | String | ACR ALC | Constant String, column header containing the ACR ALC |
| 5 | BLANK | ACR ALC+2 | String | ACR ALC+2 | Constant String, column header containing the ACR Endpoint |
| 5 | BLANK | ACR VOUCHER DATE | String | ACR VOUCHER DATE | Constant String, column header containing the ACR Voucher Date |
| 5 | BLANK | ACR VOUCHER NUMBER | String | ACR VOUCHER NUMBER | Constant String, column header containing the ACR Voucher Number |
| 5 | BLANK | ACR SETTLEMENT DATE | String | ACR SETTLEMENT DATE | Constant String, column header containing ACR Settlement Date |
| 5 | BLANK | ACR CREDIT INDICATOR | String | ACR CREDIT INDICATOR | Constant String, column header containing either Credit or Debit |
| 5 | BLANK | ACR AMOUNT | String | ACR AMOUNT | Constant String, column header containing the ACR amount |
| 5 | BLANK | Legal TRANSACTION AMOUNT | String | Legal TRANSACTION AMOUNT | Constant String, column header containing the Legal Transaction Amount |
| 5 | BLANK | Blank Field (25) | N/A | BLANK FIELD 25 | BLANK |

### Sample File Layout

The following is a sample file layout with details starting at Line Number 5:

* The system shall generate a report that can contain a possible maximum of 65,000 line items. This is an increase in the limit from PCC OTC, which currently caps the report at a possible maximum of 10,000 line items.
* If the CSV file contains more than 65,000 items, the system displays an error message preceding the IRN and is enclosed in quotations.

Table 2. Sample File Layout

| Field Number | Name | Type | Sample value |
| --- | --- | --- | --- |
|  | IRN | String | 111201500244600000608 |
|  | OTC ENDPOINT | String | 0000633502 |
|  | ALC + 2 | String | 0000633502 |
|  | CAPTURE DATE | Date/Time | 2002-07-19 14:11:14 |
|  | RECEIVE DATE | Date/Time | 2002-07-22 07:31:19 |
|  | TRANSIT NUMBER | String | 251480576 |
|  | CHECK NUMBER | String | 4114784 |
|  | ACCOUNT | String | 787910415647 |
|  | AMOUNT | String | $38.81 |
|  | CASHIER ID | String | Patrick |
|  | ITEM TYPE | String | Personal / Non-Personal |
|  | PROCESSING METHOD | String | Customer Not PresentCustomer PresentBack Office |
|  | BATCH ID | String | FF1E9FE2-FB22-4353-A27A-06C86FC3D2AA |
|  | SETTLEMENT DATE | Date/Time | 2002-08-22 07:43:10 |
|  | RETURN SETTLEMENT DATE | Date/Time | 2002-08-23 07:43:10 |
|  | DEBIT VOUCHER NUMBER | String | 24 |
|  | DEPOSIT TICKET NUMBER | String | 8 |
|  | USER FIELD 1 | String | USER FIELD 1 |
|  | USER FIELD 2 | String | USER FIELD 2 |
|  | USER FIELD 3 | String | USER FIELD 3 |
|  | USER FIELD 4 | String | USER FIELD 4 |
|  | USER FIELD 5 | String | USER FIELD 5 |
|  | USER FIELD 6 | String | USER FIELD 6 |
|  | USER FIELD 7 | String | USER FIELD 7 |
|  | USER FIELD 8 | String | USER FIELD 8 |
|  | USER FIELD 9 | String | USER FIELD 9 |
|  | USER FIELD 10 | String | USER FIELD 10 |
|  | USER FIELD 11 | String | USER FIELD 11 |
|  | USER FIELD 12 | String | USER FIELD 12 |
|  | USER FIELD 13 | String | USER FIELD 13 |
|  | USER FIELD 14 | String | USER FIELD 14 |
|  | USER FIELD 15 | String | USER FIELD 15 |
|  | USER FIELD 16 | String | USER FIELD 16 |
|  | USER FIELD 17 | String | USER FIELD 17 |
|  | USER FIELD 18 | String | USER FIELD 18 |
|  | USER FIELD 19 | String | USER FIELD 19 |
|  | USER FIELD 20 | String | USER FIELD 20 |
|  | USER FIELD 21 | String | USER FIELD 21 |
|  | USER FIELD 22 | String | USER FIELD 22 |
|  | USER FIELD 23 | String | USER FIELD 23 |
|  | USER FIELD 24 | String | USER FIELD 24 |
|  | AGENCY ACCOUNTING CODE, DESCRIPTION AND CLASSIFICATION AMOUNT | String | ARMYCODE1: ARMYDESCRIPTION 1: 10.00; ARMYCODE2: ARMYDESCRIPTION 2: 10.00; |
|  | VOUCHER DATE |  | 1/31/2014 07:43:10 |
|  | ACR TYPE | String | Adjustment |
|  | ACR REASON CODE | String | Transaction Amount Correction |
|  | ACR ALC | String | 20004444 |
|  | ACR ALC+2 | String | 2000444422 |
|  | ACR VOUCHER DATE | String | 2/08/2014 07:43:10 |
|  | ACR VOUCHER NUMBER | String | 5864000 |
|  | ACR SETTLEMENT DATE | String | 2/12/2014 07:43:10 |
|  | ACR CREDIT INDICATOR | String | Credit |
|  | ACR AMOUNT | String | $100.00 |
|  | Legal TRANSACTION AMOUNT | String | $138.81 |
|  | Blank Field (25) | N/A | Empty Value |

### CSV File Sample

The text below presents a sample of the CSV file report:

"CSV Agency Detailed Item Report"

"Thu Oct 06 11:17:23 EDT 2011"

"TOTAL AMOUNT : ","38509.00"

"TOTAL NUMBER OF ITEMS : ","2"

"IRN","OTC ENDPOINT","ALC + 2","CAPTURE DATE","RECEIVE DATE","TRANSIT NUMBER","CHECK NUMBER","ACCOUNT","AMOUNT","CASHIER ID","ITEM TYPE","PROCESSING METHOD","BATCH ID","SETTLEMENT DATE","RETURN SETTLEMENT DATE","DEBIT VOUCHER NUMBER","DEPOSIT TICKET NUMBER","User Field 1","User Field 2","User Field 3","User Field 4","User Field 5","User Field 6","User Field 7","User Field 8","User Field 9","User Field 10","User Field 11","User Field 12","User Field 13","User Field 14","User Field 15","User Field 16","User Field 17","User Field 18","User Field 19","User Field 20","User Field 21","User Field 22","User Field 23","User Field 24"

"13154124770015865281","DG1","1000000001","2011-09-07 12:21:17","2011-09-07 12:20:59","044000024","111","111111","11.11","otcqef50","Non Personal","Customer Present","1C111D1E-C111-1111-BC11-1CD11111ADBA","2011-09-12 00:00:00","null","null","000973","345345333","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null"

"13154267000015865281","DG1","1000000001","2011-09-07 16:18:20","2011-09-07 16:18:07","073903503","00000013","1111","11.11","otcqef50","Personal","Customer Present","1C111D1E-C111-1111-BC11-1CD11111ADBA","2011-09-14 00:00:00","null","null","000973","234234223","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null","null"

## Topic 6 Appendix F. Master Verification Database (MVD)

The Master Verification Database (MVD) as shown in Figure 5 provides the information required to ensure a presented check is acceptable. It supports the Agency in determining the history of a particular check writer, managed by a MVD Editor.

Figure 5. Manage Verification Tab



The verification database is an optional online database that maintains the agency hierarchy check cashing policy, dishonored check information, and manually entered blocked items based on Agency policy.

The MVD restricts the display of data based on the endpoint of the user. A user only sees records which are associated with endpoints at or below the user’s endpoint in the hierarchy, or at endpoints specified in the OTCnet Endpoint Group. Depending on the type of data being requested, different rules apply, as appropriate.

## Topic 7 Appendix G. Representment

Figure 6 illustrates the representment flow for checks that are not accepted the first time.

Figure 6. Transaction Status Codes



## Topic 8 Appendix H. Equipment Returns

If there are issues with the OTCnet equipment purchased from the Treasury OTC Support Center, contact the Treasury OTC Support Center. A staff member verifies the warranty and if needed, the dollar valuation on the scanner(s). Otherwise, if the OTCnet equipment was purchased directly from a vendor, contact the vendor for warranty and/or repair information.

Contact OTCnet Customer Service at 866-945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4 or via email at fiscalservice.otcdeployment@citi.com.

If the warranty is active, the representative provides the mailing address for the hardware shipping.

Equipment should be returned either by certified mail with return receipt, or via FedEx. When using either method, purchase insurance for the equipment’s full dollar value. Include a note explaining the reason for return, i.e., describing the damaged or defective equipment.

If the warranty has expired on the check capture equipment, call the Vendor Point-of-Contact for further instructions or discuss the possible purchase of new equipment with your Deployment Specialist.

## Topic 9 Appendix I. OTCnet Check Capture Codes

### ACH Return Reason Codes

ACH return reason codes are used when an item, which has been converted to an ACH entry, is returned. They are used by the paying institution from where the item is drawn, when returning an ACH transaction that was processed by Check Capture. The return reason code for a particular item is listed on the Debit Voucher Report (SF5515) (see Table 3).

Table 3. ACH Return Reason Codes

| Return Reason Code (RRC) | Description |
| --- | --- |
| R01 | Insufficient funds |
| R02 | Account closed |
| R03 | No account/unable to locate account |
| R04 | Invalid account number |
| R05 | Unauthorized debit to consumer account using corporate SEC Code |
| R06 | Returned per Originating Depository Financial Institution’s request |
| R07 | Authorization revoked by customer |
| R08 | Payment stopped |
| R09 | Uncollected funds |
| R10 | Customer advises not authorized |
| R11 | Check truncation entry return |
| R12 | Branch sold to another Depository Financial Institution |
| R13 | RDFI not qualified to participate a (ACH operator initiated) |
| R14 | Representative Payee (account holder) deceased or unable to continue in that capacity |
| R15 | Beneficiary or account holder (other than a representative payee) deceased |
| R16 | Account frozen |
| R17 | File record edit criteria |
| R18 | Improper effective entry date (ACH operator initiated) |
| R19 | Amount field error (ACH operator initiated) |
| R20 | Non-transaction account |
| R21 | Invalid company identification |
| R22 | Invalid individual ID number |
| R23 | Credit entry refused by receiver |
| R24 | Duplicate entry |
| R25 | Addenda Error |
| R26 | Mandatory Field Error |
| R27 | Trace Number Error |
| R28 | Routing Number Check Digit Error |
| R29 | Corporate customer advises not authorized (CCD) |
| R30 | RDFI Not Participant in Check Truncation Program |
| R31 | Permissible return entry (CCD) |
| R32 | RDFI Non-Settlement |
| R33 | Return of XCK Entry |
| R34 | Limited Participation DFI |
| R35 | Return of Improper Debit Entry |
| R36 | Return of Improper Credit Entry |
| R37 | Source document presented for payment (adjustment entries) (ARC) |
| R38 | Stop payment on source document (adjustment entries) |
| R39 | Improper Source Document  |
| R40 | Non Participant in ENR Program |
| R41 | Invalid Transaction Code (ENR only) |
| R42 | Routing Number/Check Digit Error |
| R43 | Invalid DFI Account Number |
| R44 | Invalid Individual ID Number |
| R45 | Invalid Individual Name |
| R46 | Invalid Representative Payee Indicator |
| R47 | Duplicate Enrollment |
| R50 | State Law Prohibits Truncated Checks |
| R51 | Notice not provided/Signature not authentic/ Item altered/Ineligible for conversion |
| R52 | Stop Pay on Item |
| R53 | Item and ACH Entry Presented for Payment |
| R61 | Misrouted Return |
| R67 | Duplicate Return |
| R68 | Untimely Return |
| R69 | Field Errors |
| R70 | Permissible Return Entry Not Accepted |
| R71 | Misrouted Dishonor Return |
| R72 | Untimely Dishonored Return |
| R73 | Timely Original Return |
| R74 | Corrected Return |
| R75 | Original Return not a Duplicate |
| R76 | No Errors Found |
| R80 | Cross-Border Payment Coding Error |
| R81 | Non-Participant in Cross-Border Program |
| R82 | Invalid Foreign Receiving DFI Identification |
| R83 | Foreign Receiving DFI Unable to Settle |
| R84 | Entry Not Processed by OGO (Originating Gateway Operator) |

### Check 21 Return Codes

Check 21 return codes are used by the paying Financial Institution, where the item was drawn, when a Check 21 transaction, originally processed by OTCnet, is returned. The return reason code for a particular item is listed on the Debit Voucher Report (SF5515) (see Table 4).

Table 4. Check 21 Return Codes

| Return Code | Description |
| --- | --- |
| A | Not Sufficient Funds |
| B | Uncollected Funds Hold |
| C | Stop Payment |
| D | Closed Account |
| E | Unable to Locate Account |
| F | Frozen/Blocked Account |
| G | Stale Dated |
| H | Post Dated |
| I | Endorsement Missing |
| J | Endorsement Irregular |
| K | Signature(s) Missing |
| L | Signature(s) Irregular |
| M | Non Cash Item |
| N | Altered/Fictitious Item |
| O | Unable to Process |
| P | Item Exceeded Dollar Limit |
| Q | Not Authorized |
| R | Branch/Account Sold |
| S | Refer to Maker |
| T | Stop Payment Suspect |
| U | Unusable Image |
| V | Image Fails Security Check |
| W | Cannot Determine Account |
| Y | Duplicate Presentment |
| Z | Forgery - An affidavit shall be available upon request to the OTCnet database  |

Items processed via Check 21 include all non-personal items. Personal items may also be processed via Check 21.

### Transaction Status Code Monitoring

This section of Appendix I lists and describes transaction status codes applied in OTCnet during forward file and return processing (see Table 5).

Table 5. Transaction Status Codes

| Transaction Status Code | Description | System Action |
| --- | --- | --- |
| 000 | Received | In-Process status assigned by Treasury/Fiscal Service |
| 199 | Failed | Change status to Failed. |
| 012 | Paper Draft | Create an image request. |
| 013 | ACH Origination | Does nothing, ignored by system. |
| 412413 | Paper DraftACH Origination | Change status to Settled.Record the Settlement Date and the Deposit Ticket Number. |
| 001 | ACH Redeposit  | Change status to Represented. |
| 017 | Paper Redeposit Draft | Change to status to Represented. |
| 003004 | ACH RetirePaper Retire | Change status to Retired.Return settlement date is updated |
| 401417 | ACH RedepositPaper Redeposit Draft | Change status to Settled. |
| 403404 | ACH RetirePaper Retire | Change status to Retired.Record the Debit Voucher number. Update Return Settlement Date. |

### OTCnet Processing Forward Files

* OTCnet forwards the batches for processing to the back end processor to be settled.
* The back-end system decides how to settle the items based on the following check types:
	+ Corporate check
	+ Consumer POP (customer present)
	+ Consumer ARC (customer not present)
	+ Back Office – BOC
* Items can be settled as one of the following:
	+ ACH – these items are settled electronically and do not require an image
	+ Check 21 – these items are settled electronically using a substitute check. They require an image before settlement can occur
	+ Paper – these items use the physical check for settlement
* A Return Processing File is sent. Codes 199, 012 and 013 are sent in this Return Processing File.
* Codes 012 and 013 items do not have their status updated but for 012’s, an image request is created, 013=ACH origination and 012=Paper Draft.
* 199’s are updated with the status code of ‘failed’.
* A settlement Return Processing File is sent the morning after the files were uploaded, typically around 8:30am. Codes 412, 413, and 199 are sent to OTCnet. Items receiving a 412 and 413 code are updated with the status of ‘settled’. These items receive a settlement date and a deposit ticket number.
* Items receiving a 199 code are failed items and do not receive a settlement date or deposit ticket number.
* Settled items are included in the Deposit Ticket Report for that settlement day.
* Settlement status is a prediction only – the back-end system assumes that all money can be collected for the items sent in a forward file .

### OTCnet Returns

* Once settlement occurs, an item can be returned for various reasons (e.g., insufficient funds, account closed).
* A Return Processing File containing the return reason code is sent. All status codes in the Return Processing File begin with a zero which indicates ‘accepted’. It is NOT in its final state.
* Items with codes 001, 002, 017, 018, & 019 are updated with the status of ‘represented’ and the date is stored in OTCnet and can be viewed using the CIRA Query ‘Show History’ button in the ‘Rep Effective Date’ field.
* If the represented item is not collected within four days from the Rep Effective Date, the item status in OTCnet is updated to a transaction status code of 401 or 417
* An ACH item can usually only be represented twice unless specific arrangements are made. Upon the third representment, the item is retired in OTCnet. Paper items can only be represented once and are retired in OTCnet upon the second representment. Endpoints can also choose not to have items in representment, in which case an item would just retire.
* Code 017 updates the status code to represented and generates an image request.
* Items with codes 003 and 004 are updated with the status of ‘retired’ and the return settlement date is updated.
* Verification records are created for returned items and can be viewed in the Verification Query (based on the endpoints visibility filters).
* A second Return Processing File, the ‘return settlement’ file is sent. This file does not contain return reason codes. Transaction status codes in this Return Processing File start with the number 4, indicating that the item is completed and in its final state.
* Codes 403, 404 and 409 (refer to Table 1) are already in a retired state. The status remains ‘retired’. The return settlement date field in the CIRA Query ‘Show History’ screen are updated, and a debit voucher number is created.
* The Reserve Banks return items drawn on retired routing transit numbers (RTN) directly to the bank of first deposit. This results in the items being returned to the bank of first deposit, generally the same day they are deposited with the Reserve Banks. Debit Gateway uses return reason code **6 – Retired/Ineligible Routing Number**.

## Topic 10 Appendix J. OTCnet Security

### Purpose

This section provides best practices for the OTCnet system, to guide Agencies toward Federal Information Security Management Act (FISMA) compliance. This document outlines points from the *NIST Special Publication 800-53*. Each Agency’s internal guidelines must take Treasury security best practices into consideration. Refer to *NIST Special Publication 800-53* for complete text of the ‘Recommended Security Controls for Federal Information Systems’.

### What is PII?

Personally Identifiable Information (PII) is information about an individual maintained by an agency, including, but not limited to educational, financial transactions, medical history and criminal or employment history. It includes information which can be used to distinguish or trace an individual’s identity such, as name, social security number, date and place of birth, mother’s maiden name and biometric records (*OMB M-06-19 [July 12, 2006]*).

OTCnet batch information contains PII information. It is critical that this data is secured, to prevent unauthorized access.

### Access Control

***NIST*** ***Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented access control policy that addresses purpose, scope, roles, responsibilities and compliance.
2. Formal documented procedures to facilitate the implementation of the access control policy and associated risk assessment controls.

Effects on OTCnet

* Agencies must identify authorized OTCnet users and specify access rights/privileges. Access is granted to OTCnet based on a valid need-to-know/need-to-share basis, determined by assigned official duties and satisfying all personnel security criteria and intended system usage. Agencies must monitor and remove unnecessary access when users are terminated or transferred and associated accounts must to be removed, or when a user’s access changes.
* Agencies enforce separation of duties through assigned access authorizations by establishing appropriate divisions of responsibility and separates duties as needed. This eliminates conflicts of interest in the responsibilities and duties of individuals who have access to the OTCnet system.
* Agencies employ the concept of least privilege for specific duties.
* Agencies enforce a limit of consecutive invalid access attempts by a user. This limit should be no more than three attempts.
* Agencies must review audit records, i.e., activity logs, of the OTCnet system for inappropriate activities in accordance with organizational procedures. Agencies must investigate any unusual information system-related activities and periodically review change to access authorizations. *NIST Special Publication 800-92* provides guidance on computer security log management.

In Summary

* Access to OTCnet must be given to users at the lowest level available, that still allow the user to perform their job duties.
* Review separation of duties for users’ multiple tasks. Separation of duty can be taken a step further by assigning permission to perform voids, batch close/transmission, and batch input to different individuals.
* Ensure that the maximum number of failed login attempts to the OTCnet computer has not been altered to a number higher than three.
* Review and certify OTCnet users annually. Fiscal Service performs annual certification of users. Local procedures should be established for performing recertification of OTCnet users on each computer. OTCnet Point of Contacts should print out a listing of users and their associated roles/permissions.

### Personnel Security and Procedures

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the personnel security policy and associated personnel security policy and procedure controls.

Effects on OTCnet

* Assign a risk designation to all positions and establish screening criteria for individuals filling those positions. (*NIST Special Publication 800-12* and *5 CFR 731.106(a)* and Office of Personnel Management policy and guidance).
* Screen individuals requiring access to the OTCnet system and OTCnet information before authorizing access. (*5 CFR 731.106(a)* and Office of Personnel Management policy, regulations, and guidance; organizational policy, regulations and guidance; Federal Information Processing Standards ([FIPS] 201 and Special Publication 800-73 and 800-76; and the criteria established for the risk designation of the assigned position)
* Ensures completion of the appropriate access agreements, i.e., Rules of Behavior, Privacy Statement, Accessibility Statement, and all information security access forms for individuals requiring access to OTCnet before authorizing access.
* Establish personnel security requirements for third-party providers, i.e., service bureaus, contractors, and other organizations providing OTCnet information technology services or network management and monitor the provider to ensure adequate security. (*NIST Special Publication 800-35*).
* Establish a formal disciplinary process for individuals that blatantly disregard security procedures. The process can be included as part of the general personnel policies and procedures.
* When employment is terminated, or individuals are reassigned or transferred to other positions within the agency, terminate access to the OTCnet system and to OTCnet information ensure the return of all OTCnet related property, i.e., printouts, flash drives used as secondary storage, etc., and ensure that the appropriate personnel have access to official records created by the terminated employee that are stored on the OTCnet system or paper files.

In Summary

* Assign a risk category or designation to all positions associated to the OTCnet system and screen individuals before granting access to the system.
* Make certain users read and understand the OTCnet ‘Rules of Behavior’, ‘Privacy Statement’ and ‘Accessibility Statement’.
* Ensure that the necessary information security forms have been completed (‘OTCnet Security Contact form’ which is used to designate the OTCnet Security Contact(s), and the ‘OTCnet User Access Request spreadsheet’ which is used to request user access to the ELVIS application). Only authorized users can gain access to OTCnet.
* Exiting users should no longer be in possession OTCnet equipment, i.e., access to or possession of the OTCnet computer, USB flash drive, software or printed materials. Make certain that all OTCnet equipment and printed material is available for the new person filling the position by ensuring that the equipment and material has been relinquished by the former employee.
* When an employee quits or changes their position, delete their access to OTCnet.
* Ensure that third-party service providers have adequate security in place with regard to the OTCnet system.
* Establish procedures to follow when an employee fails to follow the security policies and procedures.

### Physical and Environmental Protection

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection policy controls.

Agencies should control physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facility that are officially designated as publicly accessible) and verify individual access authorizations before granting access to the facility. The agency also controls access to areas officially designate as publicly accessible, as appropriate, in accordance with the agency’s assessment of risk.

Effects on OTCnet

* Agencies control physical access to all OTCnet equipment including the screen display to prevent unauthorized individuals from observing/viewing the screen’s display output.
* Agencies develop and keep current lists of personnel with authorized access to the area containing the OTCnet system. Designated authorized individuals within the agency should review and approve access list at least annually. The agency promptly removes personnel no longer requiring access to the area containing the OTCnet system.
* Agencies control physical access to the OTCnet computer by authenticating visitors before authorizing access to the area that houses the OTCnet system in areas that are not designated as publicly accessible.
* Agencies monitor physical access to the OTCnet system to detect and respond to incidents.
* Agencies protect power equipment and power cabling for the OTCnet system from damage and destruction.
* Agencies provide a short-term, uninterruptible power supply to facilitate an orderly shutdown of the OTCnet system in the event of a primary power source loss. The hardware should be obtained through your internal procurement channels. A long term power supply option should also be considered in the event of an extended loss of the primary power source.
* Agencies control OTCnet system-related items, i.e., hardware, firmware, software, when such items are entering and/or exiting the facility; and maintain appropriate records of those items.
* Individuals within the agency should employ appropriate OTCnet security controls at alternate work sites (*NIST Special Publication 800-46*).
* Agencies are responsible for securing OTCnet scanners, peripheral equipment, checks, and other sensitive information in locked rooms, locked cabinets, or security containers supported by appropriate key control and other physical security controls.
* To the extent that the operational environment allows, OTCnet scanners and check processing should be done in controlled environments such as steel cages, cashier cages, behind glass windows, and within offices where access to the OTCnet system and peripheral equipment can be physically controlled.

In Summary

* Know who has physical access to the area that houses the OTCnet computer.
* Ensure that unauthorized individuals cannot view the computer screen of the OTCnet computer.
* Ensure that the OTCnet hardware and software is secured, controlled and monitored, when entering or exiting the building.
* If, as in the case of military agencies, a ‘down-range’ environment is necessary, ensure that all security controls are in place to secure the equipment at the alternate work site.
* For military agencies and other agencies operating in remote or field endpoints, deploy appropriate physical security and access controls to limit unauthorized access to, and unauthorized disclosure of, OTCnet processing areas and information.

### Contingency Planning

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning policy controls.

The agency develops and implements a contingency plan for the OTCnet system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the agency review and approve the contingency plan and distribute copies of the plan to key contingency personnel (*NIST Special Publication 800-34* provides guidance on contingency planning).

Effects on OTCnet

* Agencies train personnel in their contingency roles and responsibilities with respect to the OTCnet system and provide refresher training.
* Agencies test the contingency plan for the OTCnet system at least on an annual basis to determine the plan’s effectiveness and the agency’s readiness to execute the plan. The test plan results are reviewed by the appropriate officials at the agency who initiate corrective action.
* Agencies review the contingency plan at least annually and revise the plan to address system/organization changes or issues encountered during plan implementation, execution, or testing.
* Agencies identify an alternate storage site and initiate necessary agreements to permit the secured storage of OTCnet backup information which can include storage of backup hardware, i.e., extra scanners, and backup copies of software, etc.
* Agencies identify an alternate processing site and initiate necessary agreements to permit the resumption of the OTCnet system operations for critical mission/business functions within a pre-determined time period, when primary processing capabilities are unavailable. The alternate site should be geographically separated from the primary processing site so as to not be susceptible to the same hazards.
* Agencies identify primary and alternative telecommunications services to support the OTCnet system. They also initiate necessary agreements to permit the resumption of system operations for critical mission/business functions with a pre-determined timeframe when the primary telecommunications capabilities are unavailable.
* Agencies conduct backups of user-level and system-level OTCnet information and stores backup information at an appropriately secured endpoint. Each agency must determine the appropriate frequency of these backups. Backup and restoration of this data is part of the contingency testing plan.
* Agencies store backup copies of the operating system and other critical OTCnet software in a separate facility, or in a fire-rated container that is not collocated with the operational software.
* Agencies perform backups of the OTCnet hard drive on a regular basis and store the backup in a secured endpoint.
* Agencies employ mechanisms with supporting procedures to allow the OTCnet system to be recovered and reconstituted to the system’s original state after a disruption or failure.

In Summary

* Create a contingency plan and keep it current.
* Ensure people are trained to handle a contingency situation.
* Test the contingency plan annually to ensure that hardware, communication medium and software is in working order and current.
* Consider having a backup OTCnet computer and OTCnet related hardware, i.e., scanner, secondary storage, etc.
* Consider having OTCnet related hardware and/or software backups also located off premises in a secured endpoint. A backup of the OTCnet hard drive must be performed on a regular basis.
* Extra scanners can be ordered and stored at an alternate site as backups in case of a failure or disruption. For addition information on ordering extra scanners, contact the Treasury OTC Support Center at (866) 945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4.
* In the event of a failure or disruption, scanners can be delivered overnight to endpoints within the 48 contiguous states. Delivery takes longer for areas outside of this zone.
* Consider alternate processing sites.

### Configuration Management

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated contingency planning policy controls.

The agency develops, documents, and maintains a current, baseline configuration of the OTCnet system and an inventory of the system’s constituent components.

Effects on OTCnet

* Agencies must keep an inventory of the OTCnet hardware and software. This inventory includes manufacturer, type, serial number, version number, and endpoint (physical and logical within the architecture). Keep this inventory current and document changes.
* OTCnet security settings must default to the most restrictive mode and should not be changed.
* Agencies should restrict access to the configuration information to a select few authorized individuals.

In Summary

* Keep a list of all settings that are set to the recommended defaults, as follows:
	+ Only the designated Point of Contact (POC), or security contacts, are be allowed access to the OTCnet SAT.
	+ The activity log must be regularly reviewed for suspicious activity. You must respond to evidence or indicators of increased risks to the OTCnet system and associated information with aggressive audit monitoring, more frequent reviews of audit logs, and the use of additional monitoring tools, as appropriate.

### System Maintenance

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system maintenance policy and associated system maintenance policy controls.

Effects on OTCnet

* The system maintenance policy ensures that the agency schedules, performs, and documents routine preventative and regular maintenance on the OTCnet components in accordance with the manufacturer or vendor specifications and/or agency requirements.
* All maintenance activities are controlled whether the equipment is serviced on site or removed to another endpoint.
* Removing sensitive information from the OTCnet system components (if feasible) is required when the components must be removed from the facility, when repairs are necessary. This can be accomplished by backing up the OTCnet hard drive to another medium such a CD or an external hard drive, and deleting OTCnet from the computer. Once repairs are complete, the data can be restored. Secondary storage devices that contain sensitive data, i.e., flash drives, zip disks, CD-ROMs, and smart cards, must be removed from the computer prior to servicing and stored in a secure endpoint.
* Agencies approve, control, and monitor the use of maintenance tools used on the OTCnet system, and maintain the tools on an ongoing basis.
* Agencies maintain a list of personnel authorized to perform maintenance on the OTCnet system. Only authorized personnel are allowed access to perform system maintenance.

In Summary

* Regularly scheduled preventative maintenance must be performed on each terminal, i.e., disk optimization tools, virus checking tools, etc., by authorized personnel only. Contact your local IT department for information on the tools authorized for use by your agency.
* If a component needs to be removed for repairs, all sensitive information must be removed. PII may be contained in the form of names, account numbers, social security numbers, etc., within a batch.
* For agencies located in a dusty/sandy environment, OTCnet computer equipment (computers and scanners) must be regularly cleaned with canned air.

### System and Information Integrity

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity policy controls.

Effects on OTCnet

* Agencies identify information systems containing proprietary or open source software affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The agency must promptly install new released security relevant patches, service packs, and hot fixes, and test patches, service packs, and hot fixes for effectiveness and potential side effects on the OTCnet before use (*NIST Special Publication 800-40* provides guidance on security patch installation).
* Agencies implement malicious code protection on the OTCnet system that includes a capability for automatic updates. Agency employs virus protection mechanisms at critical information system entry and exit points, i.e., firewalls, electronic mail servers, remote-access servers at workstations, servers, or mobile computing devices on the network and uses the virus protection mechanisms to detect and eradicate malicious code, i.e., viruses, worms, Trojan horses that can be transported by email, email attachments, internet access, removable media such as diskettes, CDs or flash drives, or by exploiting vulnerabilities.
* Virus protection mechanisms must be updated when new updates are available.
* Agencies employ tools and techniques to monitor events on the OTCnet system, detect attacks and provide identification of unauthorized use of the system.
* Agencies implement tools to prevent spam and spyware.
* Agencies restrict information input to the OTCnet system to authorized personnel only.
* Agencies verify the OTCnet information input for accuracy, completeness, and validity. OTCnet information includes the scanned check data, and all input fields such as the dollar amount and user defined fields.
* The agencies identify and handle error conditions in an expeditious manner.
* The agencies handle and retain output, e.g., reports, check images, etc., from OTCnet in accordance with policy and operational requirements.

In Summary

* Protection against viruses, spyware and all other forms of malicious code on both the
OTCnet computer and all removable media used on the OTCnet system (diskettes, CDs, flash drives) must be in place.
* Although the *NIST Special Publication 800-53* document recommends keeping your computer up to date with the latest security patches, hot fixes and service packs, it is up to each agency to determine the feasibility of installing every patch or fix and installation may need to be considered on a case-by-case basis. Consult your network support staff for more information.
* Regular updates to the virus protection software must be applied.
* Only authorized personnel can have access to the OTCnet system. If using backup personnel to perform OTCnet duties, backups must be issued their own unique email address and password. Passwords should never be shared under any circumstances.
* Verification practices must be used to ensure accuracy of input.
* To prevent duplicate check processing, checks may be hand stamped with ‘Electronically Processed’ after the transaction is complete and the check has been scanned. The EC7000i and EC9100i scanners can also be setup to automatically stamp the front of the check with the words, ‘Electronically Presented,’ once the transaction is complete.

### Media Protection

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented media protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated system and information integrity policy controls.

Due to the nature of the transaction information, including check images, the OTCnet media that stores this information is considered PII and must be secured. The OTCnet media that must be protected includes digital media, i.e., diskettes, external/removable hard drives, LAN drives used for OTCnet data retention/storage, flash/thumb drives, compact disks, digital video disks, and non-digital media, i.e., paper, microfilm and checks not returned to the check writer. This control also applies to portable and mobile computing and communications devices with information storage capability, i.e., notebook computers, personal digital media assistants, and cellular telephones.

Effects on OTCnet

* Agencies ensure that only authorized users have access to OTCnet information in printed form or on digital media removed from the information system.
* Agencies affix external labels to removable OTCnet storage media and OTCnet system output indicating the distribution limitations and handling caveats of the information. Certain media may be exempted from this labeling as long as they remain within a secure environment.
* Agencies physically control and securely store the OTCnet system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.
* Agencies sanitize OTCnet system digital media using approved equipment techniques and procedures. Sanitization is the process used to remove information from digital media in the event that information recovery is not possible (*NIST Special Publication 800-36* provides guidance on appropriate sanitization equipment, techniques, and procedures.)
* Agencies sanitize or destroy OTCnet digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using information contained on the media (*NIST Special Publication 800-36* provides guidance on appropriate sanitization equipment, techniques, and procedures).
* Agencies physically control and securely store OTCnet system media within a controlled area.

In Summary

* Only authorized users have access to printed and digital media used for OTCnet. This means all printouts, hard disks, LAN drives, external hard disks, diskettes, CDs, zip disks, smart cards, and USB flash drives.
* Store and label all removable media (both digital and paper) in a secured endpoint. Labeling can include the restrictions on distributing the media and warnings on handling of the media.
* Properly remove all OTCnet related data prior to destruction or reuse. Information stored on the OTCnet hard drive, secondary storage drive, and printed media may contain personally identifiable information (PII) in the form of names, account numbers, social security numbers, etc. within an OTCnet batch.
* OTCnet paper output such as batch lists, report printouts, and scanned checks not returned to customers contain PII information and must be destroyed by shredding. This type of output should never be thrown away with other office trash without shredding.
* Consider additional encryption protection of the information that is contained on the secondary storage drive. OTCnet provides a minimum level of encryption to the data on the secondary storage drive but additional encryption protection may be used. If additional levels of encryption are used, agencies must ensure that the data can be decrypted in the event that the data needs to be restored using the OTCnet ‘Batch Recover’ function. Decryption typically involves the use of a password. If the additional level of encryption cannot be removed, OTCnet is unable to read the batch data and the batch recovery function fails.

### Incident Response

***NIST*** ***Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented incident response policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated system and incident response policy controls.

Effects on OTCnet

* Agencies train personnel in their security incident response roles and responsibilities with respect to the OTCnet system and provide refresher training.
* Agencies track and document OTCnet system security incidents on an ongoing basis.

Agencies expeditiously report all OTCnet system security incidents of theft, loss, or data/PII compromise (known or suspected) to the Treasury OTC Support Center at (866)945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4, and their own internal authorized security personnel.

In Summary

OTCnet Point-of-Contacts and users should monitor the OTCnet system for possible security incidents and report any suspected incidents to the Treasury OTC Support Center at (866)945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4 or via email at fiscalservice.OTCChannel@citi.com.

### Awareness and Training

***NIST Special Publication 800-53 Guidance***

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training policy controls.

Security awareness and training ensures that all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to OTCnet system and thereafter, at least yearly. Appropriate content of security awareness must be determined and based on the specific requirements of the OTCnet system. The Agency’s security awareness program should be consistent with the requirements contained in *5 CFR Part 930.301* and with the guidance in *NIST Special Publication 800-50*.

Effects on OTCnet

* Users must be familiar with the password requirements.
* Users must be familiar with the OTCnet Security Guidelines.

In Summary

Information that is covered in the OTCnet Security Awareness Training must include:

* Entering new passwords - prevent others from watching. Prevent others from guessing your password - do not use names of persons, places, or things that can be easily identified with you.
* Passwords - they must never be shared.
* Compromised passwords - must be changed immediately.
* Unauthorized use of the system must be reported to Treasury OTC Support Center at (866)945-7920, or 302-323-3159, or military DSN at 510-428-6824, option 1, option 3, option 4 or via email at fiscalservice.OTCChannel@citi.com.
* Logging off from the system must be completed when you leave your computer unattended. Click on the ‘Logout’ button on the menu or click the ‘X’ at the upper right corner of the screen to prevent unauthorized access to the system.
* Security contacts or POCs must be kept current. As soon as an agency is aware of a change in personnel, a new person should be assigned the duties of the security contact to take the place of the exiting person. The exiting person’s access should be deleted.
* OTCnet security personnel, or POC’s must be trained on the proper handling of a user and its associated password. Proper handling includes writing down the password and locking it up. It should only be available to the POC.
* Users must be familiar with the Rules of Behavior, Privacy Statement, and Accessibility Statement prior to using the system. They can be found as links on OTCnet.

## Summary

In this chapter, you learned:

* Administrative details for costs, paperwork, policy, training and customer service
* Password requirements
* How to resolve check Image quality
* How to query within CIRA
* How to access the CIRA CSV File
* How to access the MVD
* How to establish check representments
* The procedure for returning equipment
* How to verify check capture return codes
* Security best practices for the OTCnet system
* Guidance for OTCnet Security