

***Executive Secretariat (Exec Sec)***

Digital Mail SOlution

requirements definition

Version Number: 1.4

Version Date: 04/26/2021

VERSION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Number** | **Revision**  **Date** | **Approved**  **By** | **Approval**  **Date** | **Description of Change** |
| 1.0 | 4/8/2021 | *<name>* | *<mm/dd/yy>* | *First Draft Created* |
| 1.1 | *4/13/2021* |  |  | *Added sections and diagrams* |
| 1.2 | 4/19/2021 |  |  | Included comments |
| 1.3 | 4/22/2021 |  |  | Additional contents |
| 1.4 | 4/26/2021 |  |  | Included comments |

TABLE OF CONTENTS

[1 Introduction 4](#_Toc70333693)

[1.1 Purpose 4](#_Toc70333694)

[1.2 Background 4](#_Toc70333695)

[2 Business Requirements Overview 4](#_Toc70333696)

[2.1 Assumptions / Constraints 4](#_Toc70333697)

[2.2 Current Business Process 5](#_Toc70333698)

[2.3 Target Solution Process Overview 5](#_Toc70333699)

[2.4 User Roles 5](#_Toc70333700)

[2.5 User Types 6](#_Toc70333701)

[3 Functional Requirements 6](#_Toc70333702)

[3.1 Solution Requirements 6](#_Toc70333703)

[3.2 Interface Requirements 7](#_Toc70333704)

[4 Non-functional Requirements 7](#_Toc70333705)

[4.1 Performance, Reliability and Availability Requirements 7](#_Toc70333706)

[4.2 Supportability Requirements 8](#_Toc70333707)

[4.3 User Documentation Requirements 8](#_Toc70333708)

[4.4 Hardware Requirements 8](#_Toc70333709)

[4.5 Software Requirements 8](#_Toc70333710)

[4.6 Security and Privacy Requirements 9](#_Toc70333711)

[4.7 Section 508 Compliance Requirements 10](#_Toc70333712)

[4.8 Records Management Requirements 10](#_Toc70333713)

[5 Business Processes 11](#_Toc70333714)

[5.1 Digital Mail Process Flow “As-Is” 11](#_Toc70333715)

[5.2 Digital Mail Process Flow “To-Be” 12](#_Toc70333716)

[6 Document File Format and Metadata 13](#_Toc70333717)

[6.1 File Format 13](#_Toc70333718)

[6.2 Metadata 13](#_Toc70333719)

[Appendix A: References 14](#_Toc70333720)

# Introduction

## Purpose

This Requirements Definition Document is intended to capture and describe the business needs for the creation of a new Digital Mail Solution needed by the Administration for Children and Families (ACF) Executive Secretariat (Exec Sec). This document provides insight into the ”As-Is” and “To-Be” business environments including the business processes, mail digitalization requirements, user types, and stakeholders of the target solution. It identifies high-level capabilities needed by the target solution through the identification of the functional and non-functional requirements.

This Requirements Definition Document reflects requirements at a level appropriate for an acquisition

## Background

As an operating division within HHS, ACF’s mission is to foster the health and well-being of children, youth, families, individuals and communities to be resilient, safe, healthy, and economically secure by providing federal leadership, partnership and resources for the compassionate and effective delivery of human services.

The pandemic demonstrated a need to explore an electronic solution, not only to address the needs created during the telework scenario created by the pandemic, but also to streamline the process moving forward.

Exec Sec is requesting guidance to identify a solution to scan/digitize all mail/correspondence received at all ACF Program Offices.

# Business Requirements Overview

## Assumptions / Constraints

General assumptions and constraints that impact the requirements or technical design of the solution include:

* The ability of the scanning solution to establish an interface with the SWIFT system and upload data in pre-determined format.
* The proposed solution will reside in the specific location accessible only by the PSC operations personnel with proper security.
* The solution will allow for proper scalability to handle various mail volumes.
* The solution shall have FedRAMP certification.
* The solution shall acquire ATO to operate in production.
* The solution will be maintained by the Government or support contractors.

## Current Business Process [[1]](#footnote-1)

The Program Support Center (PSC) provides official government mail services to all federal agencies, including HHS and ACF. They prepare and dispatch outgoing mail using a “Rate-Shop” system to compare real-time information from mail carriers and identify the most cost-efficient vendor based on weight, destination, and time sensitivity of deliveries. PSC also collects interoffice mail from designated mail stops each business day and performs special “hand carry” services upon request.

Currently, correspondence/mail is manually distributed by PSC to Exec Sec and all ACF program offices, requiring staff to manually scan the mail, send to their computers, then pull into the SWIFT system for processing; or to physically deliver the mail to the appropriate office (walking it from floor to floor, as needed).

The current operational environment has resulted in:

* Mail displacements
* Lost mail
* Delays in mail delivery, and
* Delays in ACF staff responses to direct inquiries

## Target Solution Process Overview [[2]](#footnote-2)

In the target solution process, all ACF incoming correspondence/mail will be properly sorted and based on the priority opened and either hand delivered or scanned and delivered digitally.

In addition, the target solution process proposes a new capability enabling scanning functionality and implementation of an interface to the SWIFT system by which all digitized mail would be uploaded on a planned frequency and schedule.

## User Roles

Defined users are persons who will interact with the digital mail business process and sub-process tasks. A person may be assigned multiple roles, as appropriate, to fulfill the functions permitted under each role. The Solution shall be utilized by the following user types:

| **ID** | **Type** | **Description/Examples** |
| --- | --- | --- |
| UR1 | Mail Room Staff | Responsible for receiving, separating and sorting all incoming mails |
| UR2 | Exec Sec Staff | Responsible for supervising the overall operations |
| UR3 | Scan Room Staff | Responsible for scanning the correspondence/mail |
| UR4 | Help Desk | Responsible for providing Tier 1 technical or operational support |
| UR5 | IT Vendor | Responsible for providing technical support (both hardware and software) if not be provided by Help Desk |

## User Types

| **ID** | **Type** | **Description** |
| --- | --- | --- |
| UT1 | ACF Program Office Staff | All personnel who handle incoming mails shall meet the required security |
| UT2 | Operations Staff | The software (both scanning and interface) shall be accessed by the personnel with proper login credentials. |

# Functional Requirements

## Solution Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| DEL1 | Delivery | All incoming ACF mail shall be delivered to designated PSC location:   * Congressional Letters * Letters from general public * Complaints * Invitations * Thank you, cards, * Campaign cards |
| ML1 | Sort | * Sort and Separate Mail – all delivered mail shall be sorted and separated * Mail shall be separated based on time sensitivity * All mail shall be either hand delivered or scanned |
| ML2 | Hand Delivered | * Checks * Forms requesting services * Reports * Bills * Catalogues * Flyers * Resumes, and * Legal Documents |

The high-level functional requirements for the digital mail solution are as follows:

* Time sensitive (Priority) mails shall include:
* All mails shall be either hand delivered or scanned
* The to-be scanned mails shall be opened and scanned
* The digitized mails shall be scheduled for upload to the SWIFT system.

## Interface Requirements

The requirements for the interface between the digital scanner and the SWIFT system are as follows:

* The solution shall provide an interface so that the digitized mails are uploaded to the SWIFT system.
* The interface application shall be installed on the same device where the scanner software runs.
* The assigned user shall authenticate to the application which interfaces with the SWIFT system.
* The application (interface) shall be part of the Single Sign-On (SSO) profile. This implies that the user shall NOT need to re-authenticate to the SWIFT system for uploading the digitized mail.
* The solution shall provide the capability to upload the digitized mail based on a scheduled time and frequency.
* The interface shall provide a report to include but not limited to the following:
* Start and End date/time of the process
* Number of records read (from scanner) and uploaded (to SWIFT)
* Username of the person(s) and time of their logins.

# Non-functional Requirements

The high-level non-functional requirements for the digital mail solution are described in the below sections. The System shall meet the following Non-Functional Requirements:

## Performance, Reliability and Availability Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| PR1 | Volume | The scanners must have the efficiency of scanning 50-85 number of mail (both front and back) per minute. |
| PR2 | Time Sensitive | * Congressional Letters * Letters from Children * References to Child Abuse |
| PR3 | Availability | Minimum downtime during business day (M-F, 7:30am-4:30pm EST) |
| PR4 | Reliability | Main Cycle between Failure:   * Main Unit: 300,000 cycles * ADF: 600,000 cycles * Daily Duty Cycle: 8,000 pages per day |

## Supportability Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| SR1 | Training | PSC or other personnel shall be trained to operate the new hardware and resolve minor issues. |
| SR2 | O&M | O&M contract to handle ongoing operations, upgrades, and issues associated with the new solution. |
| SR3 | IT Support | IT support for any ongoing maintenance or issues. |

## User Documentation Requirements

The following documentations shall be developed:

* Operators Manual for the operations personnel,
* Technical Design Document (TDD) for the overall solution, and
* Interface Control Document (ICD) for the software interface between the solution and the SWIFT system.

## Hardware Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| HW1 | Scanner Efficiency | 200 to 300-sheet via Automatic Document Feeder (ADF) |
| HW2 | Scanner Speed – Color/B&W | Process 50-85 pages per min |
| HW3 | Feeder Capacity | 1100 – 5600 sheets |
| HW4 | Interface | USB, Small Computer Standard Interface (SCSI) drive, LAN |

## Software Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| SW1 | OCR Type | Brand specific |
| SW2 | Network Scanning | Use of optional software to scan to any PC on the network |
| SW3 | Searchable PDF | Save scanned documents as PDF Files |
| SW4 | Interface to Cloud Services | Scan to SharePoint or Google Docs |
| SW5 | Optical Resolution | 600 dpi |
| SW6 | Operating Systems | Win, Linux |
| SW7 | Data Security Kit | Ability to send stored scanned documents to a shredder and get a document of proof |

## Security and Privacy Requirements

| **ID** | **Category** | **Solution Requirement** |
| --- | --- | --- |
| SP1 | Account Auditing | Support automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified with details of the account updates. |
| SP2 | Sign-On Help Page | Display a help page with the solution’s Help Desk contact details if the user’s credentials cannot be authenticated. |
| SP3 | Validate User Authentication | Validate that a user is authenticated when the user accesses the solution. |
| SP4 | Multi-factor Authentication | Provide two-factor authentication. |
| SP5 | Alert | Have the capability to automatically alert the solution administration staff if unauthorized access is attempted. |
| SP6 | Lock out and Alert | Lock out users after three failed login attempts and alert the solution administration staff. |
| SP7 | Operating systems | If relevant, be hardened following ACF Hardening Standards for Windows and Linux operating systems. |
| SP8 | End of Life | Solution shall not use components that are End of Life/End of Support, including supporting OS, middleware, or embedded application (e.g. openSSH). |
| SP9 | DoS attacks | Be designed/configured to be resistant to Denial of Service (DoS) attacks as specified in NIST SP 800-54r4 SC5. |
| SP10 | Insecure protocols | Only accept encrypted connections from the solution to SWIFT and drop connection attempts presented over insecure protocols and send alters in that regard. |
| SP11 | Proxy headers | Check for the presence of all proxy headers (forward or reverse) if applicable. |
| SP12 | HSTS | Configure web services with HTTP Strict Transport Security (HSTS) secure protocol enforcement. ([refer to DHS BOD 18-01](https://cyber.dhs.gov/bod/18-01/)) |
| SP13 | DMARC | Comply with DMARC (Domain-based Message Authentication, Reporting, and Conformance. email authentication protocol) configuration standards for all email communications. ([refer to DHS BOD 18-01](https://cyber.dhs.gov/bod/18-01/)) |
| SP14 | TLS 1.2 | Support only Transport Layer Security (TLS1.2) or above with mutual authentication enabled for all message interactions.  ([refer to DHS BOD 18-01](https://cyber.dhs.gov/bod/18-01/)) |
| SP15 | FIPS 140-2 | Support FIPS 140-2 approved ciphers, the list of supported ciphers is ordered by preference:  AES-GCM+EECDH  AES-GCM+EDH  AES256+EECDH  AES256+EDH |

## Section 508 Compliance Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Type** | **Description** |
| 508SC1 | HW Accessibility | Hardware - Must provide a Section 508 Voluntary Product Accessibility Template (VPAT) report for review prior to acquisition |
| 508SC2 | SW Accessibility | Software Must provide a Section 508 Voluntary Product Accessibility Template (VPAT) report for review prior to acquisition |

## Records Management Requirements

| **Data Retention and Records Management** | | |
| --- | --- | --- |
| **ID** | **Category** | **Requirement** |
| RM1 | Records Management | The solution shall maintain and store all records in accordance to NARA disposition schedules. |
| RM2 | Records Management | The solution shall capture all metadata as required by NARA for each record. |
| RM3 | Records Management | The solution shall include a rules engine for defining and configuring the records disposition schedule. The rules engine shall allow for authorized users to change the disposition schedule of records without having to go into the solution code. |
| RM4 | Records Management | The solution shall prevent the alienation or unauthorized destruction of records. |
| RM5 | Records Management | The solution shall allow for authorized users to set litigation and FOIA holds on records. |
| RM6 | Records Management | Reliability: The solution shall provide the controls required to ensure a full and accurate representation of the transactions, activities, or facts within the scope of its operations and can be depended upon in the course of subsequent transactions or activities. |
| RM7 | Records Management | Authenticity: The solution shall provide the controls required to protect against unauthorized addition, deletion, alteration, use, and concealment. |
| RM8 | Records Management | Integrity: The solution shall provide the controls required, such as audit trails, to ensure records are complete and unaltered. |
| RM9 | Records Management | Usability: The solution shall provide the mechanisms required to ensure records can be located, retrieved, presented, and interpreted. |
| RM10 | Records Management | Content: The solution shall provide the mechanisms required to preserve the information contained within the record itself that was produced by the creator of the record. |
| RM11 | Records Management | Context: The solution shall provide the mechanisms required to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity. |
| RM12 | Records Management | Structure: The solution shall provide the controls required to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements. |
| RM13 | Data Retention | The solution shall support the capability to “move” old versions of documents and files to long-term storage, if solution performance becomes an issue. |

# Business Processes

## Digital Mail Process Flow “As-Is”

An “As-Is” process flow (Figure 5.1-1) documents how business process is performed currently. The “As-Is” process flow captures procedures and information to analyze and improve to build a “To-Be” process.

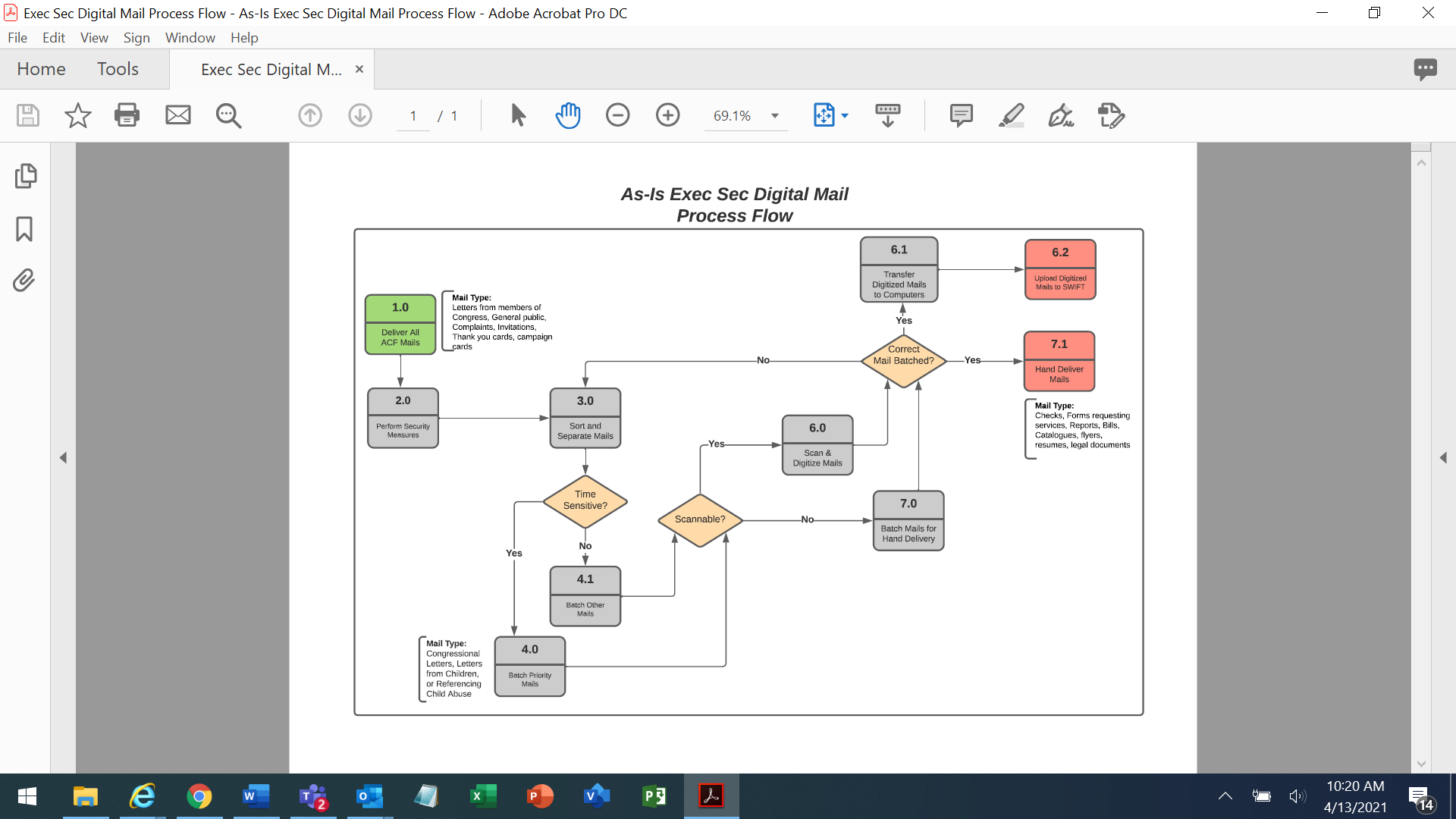
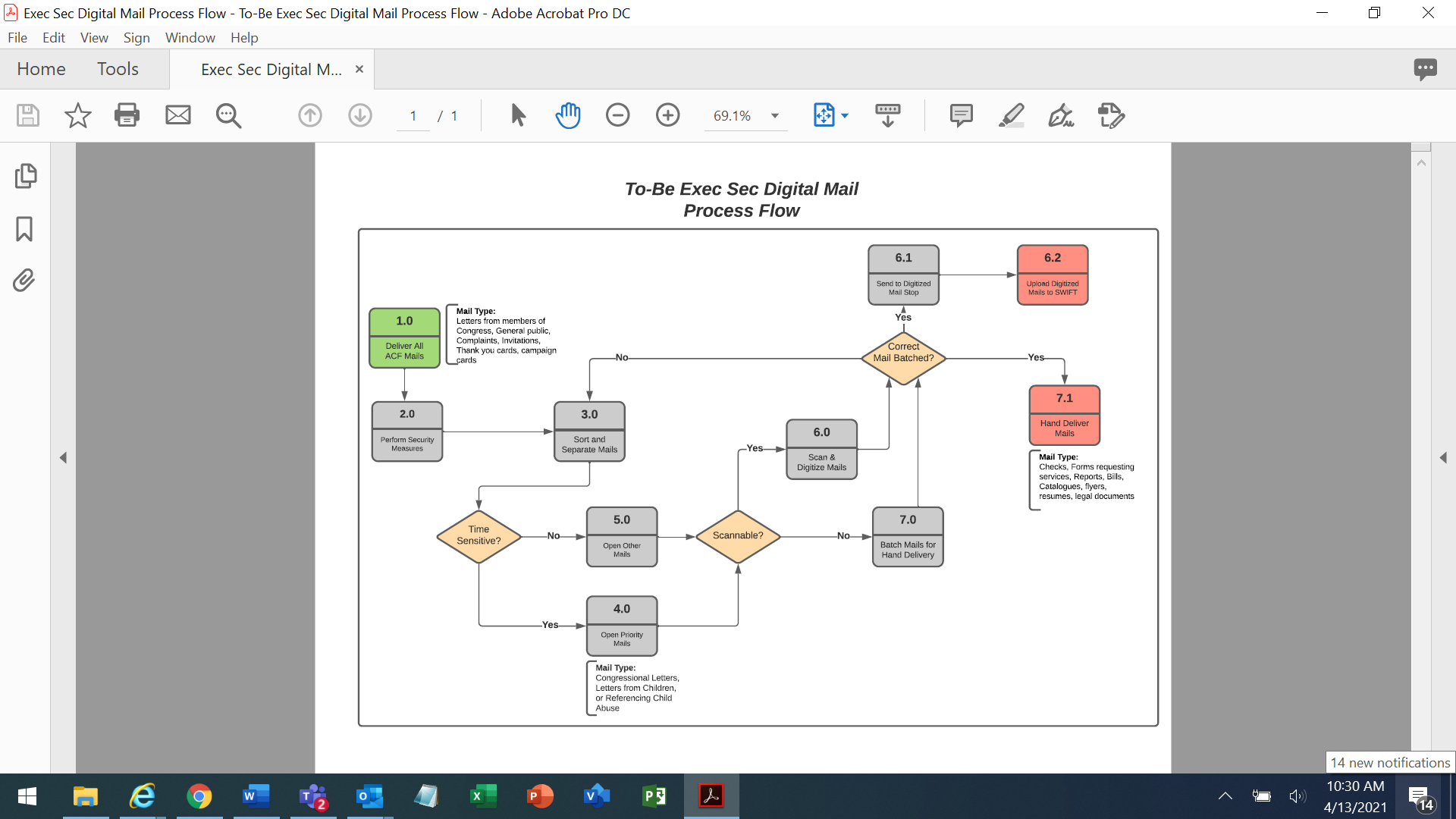


Figure 5.1-1, Digital Mail Process Flow “As-Is”

## Digital Mail Process Flow “To-Be”

A “To-Be” process (Figure 5.2-1) shows proposed future processes with the scan functionality in place.



### Figure 5.2-1, To-Be Digital Mail Process Flow

# Document File Format and Metadata

## File Format

Most scanners have the capability to convert scanned documents to multiple formats. The most commonly used format that allows editability and searchability is Portable Document Format (PDF). In addition, based on the specific scanner type the following formats could also be available:

* JPG or JPEG (Joint Photographic Experts Group) – widely used for capturing digital images
* PNG (Portable Network Graphics) – like JPEG
* TIF of TIFF (Tagged image File Format) – widely used for bitmapped images

## Metadata

Metadata is descriptive or contextual information which refers to or associated with another object or resource. Each scanned document contains metadata which are stored inside the documents. Metadata refer to the properties of the document. This information includes:

* File name
* Title
* Title date
* Date of creation
* Author
* Size
* Copyright information
* The application which was used to create the file.

The above information can be found via Windows Explorer as part of the file property.

# Appendix A: References

The following table summarizes the documents referenced in this document.

|  |  |
| --- | --- |
| **Document Name** | **Description** |
| *CB-NCCAN Intake Document* | *Initial request made by the program office* |
| *Epson – The Workforce DS-70000* | *Technical Specs* |
| *Kodak – S2085f* | *Technical Specs* |
| *Cannon imageFORMULA DR-6010C* | *Technical Specs* |

1. See Section 5.1 for the As-Is Business Process Flow [↑](#footnote-ref-1)
2. See Section 5.2 for the To-be Business Process Flow [↑](#footnote-ref-2)