### Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Author</th>
<th>Date</th>
<th>Section</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>DCS PMO Engineering</td>
<td>July 23, 2019</td>
<td>All</td>
<td>Initial document</td>
</tr>
<tr>
<td>0.2 and 0.2b</td>
<td>DCS PMO Engineering</td>
<td>July 30, 2019</td>
<td>All</td>
<td>Update based on feedback received from DCS Engineering &amp; Service Manager</td>
</tr>
<tr>
<td>0.2.c</td>
<td>DCS PMO Engineering</td>
<td>July 31, 2019</td>
<td>Pages 10 and 13</td>
<td>Page 10 (changed the wording in the header); Page 13 (changed the wording in item 2)</td>
</tr>
<tr>
<td>0.2.d</td>
<td>DCS PMO Engineering</td>
<td>August 27 and September 4, 2019</td>
<td>All</td>
<td>Corrected the GSD email on page 4; Redacted name on page 5; Updated banners</td>
</tr>
</tbody>
</table>
Table of Contents

Overview ....................................................................................................................................................... 4

Points of Contact (POC)........................................................................................................................................ 4

Welcome to DoD SAFE .................................................................................................................................. 5

Creating a Drop-off (CAC Authenticated User) ............................................................................................. 6

Creating a Drop-off (Non-Authenticated User or Guest) ............................................................................ 10

Request a Drop-off (CAC Authenticated User) ........................................................................................... 12

Pick-up (Authenticated User and Non-Authenticated User or Guest) ....................................................... 13

Outbox (CAC Authenticated User) .............................................................................................................. 14

Search for a Drop-off (CAC Authenticated User) ........................................................................................ 15

Recipient URL List (CAC Authenticated User) ............................................................................................. 17

Delete a Drop-off (CAC Authenticated User) .............................................................................................. 19

Resend a Drop-off (CAC Authenticated User) ............................................................................................. 21

Encryption ................................................................................................................................................... 23

APPENDIX: Acronyms ................................................................................................................................. 27
Overview

DoD Secure Access File Exchange Service, DoD SAFE (https://safe.apps.mil) is an enterprise technical solution that provides the capability of secure data transfer of large files (8 GB maximum). There are no user accounts for SAFE; authentication is performed via common access card (CAC) and notification is done via email. SAFE is available for use by unauthenticated users also; however, a DoD CAC holder must initiate the exchange process. Users are identified as DoD users that authenticate to DoD SAFE using a CAC and non-DoD or non-CAC holders are referenced as Guests.

DoD SAFE services are on the Non-classified Internet Protocol Router Network (NIPRNet) and are accessible via the Internet. Users will need to follow the DoD SAFE Policy and Procedures such as reporting spillages and encrypting PII and PHI data. Users shall not neglect, disregard, nor knowingly circumvent any of the roles and responsibility standards associated with the DoD SAFE Service. DoD SAFE will retain data up to 7 days.

This user guide provides guidance on how to use DoD SAFE.

Points of Contact (POC)

This table summarizes the list of contacts responsible for the implementation of DoD SAFE.

<table>
<thead>
<tr>
<th>POC</th>
<th>Office</th>
<th>Email</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier I Support (8x5)</td>
<td>844-347-2457</td>
<td><a href="mailto:disa.gsd.apps@mail.mil">disa.gsd.apps@mail.mil</a></td>
<td>DISA Global Service Desk (Help Desk)</td>
</tr>
<tr>
<td></td>
<td>DSN: 312-850-0032</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Point of Contacts
Welcome to DoD SAFE
To access DoD SAFE, use the browser of your choice and navigate to https://safe.apps.mil

1. Accept User agreement

2. DoD SAFE homepage is loaded (Authenticated View)
3. DoD SAFE homepage is loaded (Non-authenticated, Guest View)

Creating a Drop-off (CAC Authenticated User)
A drop-off allows you to upload a file and send to a CAC authenticated or non-CAC authenticated user.

1. Click Drop-off

1. Enter some identifying information about the recipient(s) (name and email address).
   a. For one recipient; add recipient’s name and email address
   b. Click “Add & Close”
c. For more than one recipient, click “Add Many”
d. Enter one recipient per line using this format: Recipient's Name email@example.com
e. Click “Add & Close”

2. Add a short note to the Recipient(s)

3. As the sender you have two options; select the option you need:
   a. Encrypt file
   b. Send me an email when each recipient picks up the files
4. Click to Add Files or Drag and Drop them

5. Add a description to each file if necessary

6. Click “Drop-Off Files” to send the files to the recipient

7. Confirm the files do not contain classified information and click “Ok”.

8. The file is uploaded and an automated email is sent to the recipient notifying them of the “drop-off”
   a. NOTE: The image below depicts an upload for a hashed and unencrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.
9. As the sender, you are notified the drop-off is complete
   a. The notification displays the filename, file size, the secure hash algorithm – 256 bit (SHA-256) and description. The sender enters the description prior to uploading the file.

10. To view all packages sent, click “Outbox”. NOTE: *The time the package was created is displayed in Zulu Time*
Creating a Drop-off (Non-Authenticated User or Guest)
This type of drop-off allows a non-authenticated user (Guest) to upload a file that has been requested by an authenticated user. An authenticated user must first execute the "Request a Drop-Off" procedure to obtain a "Request Code" for external delivery to the non-authenticated user.

1. Click Drop-off

2. Enter Request Code (12 digits). This request code is sent to you by the requestor

3. Click “Next”

4. Add a short note to the Recipient

5. Click to Add Files or Drag and Drop them

6. Add a description to each file if necessary

7. Click “Drop-Off Files” to send the files to the recipient
8. Confirm the files do not contain classified information and click “Ok”.

9. The file is uploaded and an email will be sent to the recipient notifying them of the “drop-off”
   a. NOTE: The image below depicts an upload for a hashed and unencrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.

10. You are notified the drop-off is complete
Request a Drop-off (CAC Authenticated User)
CAC authenticated users can request a drop-off from another CAC authenticated user or a non-CAC authenticated user (guest).

1. Click “Request a Drop-off”

2. Complete all entries associated with the drop-off request
3. Once complete, click “Send the Request”

4. A “Request Code” is displayed to the sender

   The request for a Drop-off has been sent to [REDACTED] at [REDACTED] civ@mail.mil. It is valid for 14 days.

   If the recipient wants to send files to you before their request arrives, they should
   1. Go to https://safe.apps.mil/
   2. Select “Drop-off Files”
   3. Enter the request code [REDACTED]
   4. Click on the "Next" button

   You may close this window.

5. The recipient will receive an automated email containing the information you entered along with a URL, which allows them to upload the files for you. The URL also includes the request code, which also can be used to “drop-off” / upload a file.

**Pick-up (Authenticated User and Non-Authenticated User or Guest)**

Pick-up a file dropped off for you

1. Click Pick-up

2. Enter the Claim ID, Recipient Code and Passcode.

   These items will be sent you in an automated email or, conveyed to you by the initiator of the transfer. If you select the link in the automatic notification, the Claim ID, Recipient Code and Claim Passcode will be pre-filled automatically.
3. Click “Pick-up Files”

4. The user can either click “Download All Files” to download the package or download each individual file by clicking its hyperlink (i.e., the file depicted below is a hyperlink which can be clicked by the user for individual downloads.

![Image of file download interface]

5. The files are downloaded to your workstation

**Outbox (CAC Authenticated User)**

All drop-offs and files sent are viewed within the Outbox

1. Click “Outbox”

2. Click a package to see its details. NOTE: *The time the package was created is displayed in Zulu Time*
3. The Drop-off Summary is displayed

Search for a Drop-off (CAC Authenticated User)
As an authenticated user, you can search your Outbox to locate previous packages sent. The search criteria is based on claim id, sender, recipient, file size or the date the drop-off was created.

1. Click “Outbox”
2. Enter the search criteria for the package you need to locate.

3. The packages matching your search criteria are displayed.

4. Click on the package you need to view its details. NOTE: The time the package was created is displayed in Zulu Time

5. The Drop-off Summary is displayed
Recipient URL List (CAC Authenticated User)
As the sender of files, you are able to view all of the URLs associated with your drop-offs. You can share this URL with recipients as required.

1. Click “Outbox”

2. Click a package to view its details. NOTE: The time the package was created is displayed in Zulu Time

3. The Drop-off Summary is displayed
6. Locate “Recipient URL List” and the bottom of the screen and click “Show”

7. The URL and Claim Passcode are displayed. You can use the “Copy” button to copy and paste this URL and share it with the recipient
Delete a Drop-off (CAC Authenticated User)
Users can delete drop-offs

1. Click “Outbox”

2. Click a package to view its details. NOTE: The time the package was created is displayed in Zulu Time

3. The Drop-off Summary is displayed
4. Click “Delete Drop-off”

5. Confirm you want to delete the drop-off, Click “Ok”

6. The drop-off is deleted.
Resend a Drop-off (CAC Authenticated User)

Users can resend drop-off to recipient

1. Click “Outbox”

2. Click a package to view its details. NOTE: The time the package was created is displayed in Zulu Time

3. The Drop-off Summary is displayed
4. Select the file you want to resend.

5. Click “Resend Drop-off”

6. To include Passcode and Claim ID, Click “Yes”.

7. The drop-off is resent with Passcode and Claim ID.

8. The recipient receives an email containing the drop-off details.
Encryption
Both CAC Authenticated and Guest users can encrypt files / packages before they are sent. **NOTE: NO CLASSIFIED INFORMATION IS ALLOWED ON DOD SAFE.** Any files containing PII/PHI must be encrypted prior to uploading or by checking the Encrypt every file box as specified in the following steps.

1. Click Drop-off

![Drop-off](image)

2. Enter some identifying information about the recipient(s) (name and email address).
   a. For one recipient; add recipient’s name and email address
   b. Click “Add & Close”

![Add Recipients](image)

   c. For more than one recipient, click “Add Many”
   d. Enter one recipient per line using this format: *Recipient's Name email@example.com*
   e. Click “Add & Close”
3. Check “Encrypt every file (REQUIRED FOR PII/PHI)”

4. Create and remember your Encryption Passphrase. This passphrase will not be sent to the recipients. You will have to do this yourself. Your passphrase must be at least 10 characters long.

   **Encryption Passphrase**

   **This passphrase will not be sent to the recipients.**
   **You need to do this yourself.**

   **Passphrase:** ****

   **And again:**

   **Must be at least 10 characters**

   

5. Click “Ok”

6. Add a short note to the Recipient(s). NOTE: You may include your passphrase here or send in a separate email.

7. Click to Add Files or Drag and Drop them
8. Add a description to each file if necessary

9. Click “Drop-Off Files” to send the files to the recipient

10. Confirm the files do not contain classified information and click “Ok”.

11. The file is uploaded and an email will be sent to the recipient notifying them of the “drop-off”
    a. NOTE: The image below depicts an upload for a hashed and encrypted file drop-off. Depending on the speed of the upload, each user may or may not view the image depicted below.

12. You are notified the drop-off is complete
a. The notification notifies the sender that an encrypted file with a passphrase was successfully sent. It also notifies the sender of filename, file size, the secure hash algorithm – 256 bit (SHA-256) and description. The sender enters the description prior to uploading the file.

```
Drop-Off Completed

Your files have been sent successfully.

This drop-off is encrypted with a passphrase known only to the sender.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>SHA-256 Checksum</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture.JPG</td>
<td>18.6 KB</td>
<td>20BF08A00350E22E060228663041448</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BEB8ECB335AC73E2018156097455D</td>
<td>1 file</td>
</tr>
</tbody>
</table>
```
APPENDIX: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoD SAFE</td>
<td>Department of Defense Secure Access File Exchange</td>
</tr>
<tr>
<td>NIPRNet</td>
<td>Non-classified Internet Protocol Router Network</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PMO</td>
<td>Program Management Office</td>
</tr>
<tr>
<td>SHA-256</td>
<td>Secure Hash Algorithm – 256 bit</td>
</tr>
</tbody>
</table>