Federal Trade Commission
Privacy Impact Assessment

Epiq Class Action ClaimsMatrix and Online Claim Submission Website (ECA)

October 2016

Table of Contents

1 System Overview 1
2 Data Type, Sources, and Use 2
3 Data Access and Sharing 3
4 Notice and Consent 5
5 Data Accuracy and Security 7
6 Data Retention and Disposal 9
7 Website Privacy Evaluation 9
8 Privacy Risks and Evaluation 10
9 Approval and Signature Page 13

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) brings law enforcement actions that can result in the recovery of redress money from defendants that is to be returned to injured consumers or businesses. The FTC distributes money pursuant to a distribution plan that is either approved by a court or an administrative law judge or delegated to the FTC's discretion. The FTC Redress Administration Office (RAO) is responsible for administering and coordinating redress activities, and Epiq Class Action (ECA), an FTC claims administration contractor, supports RAO's activities. This PIA explains what personally identifiable information (PII) RAO and ECA collect throughout the redress administration process, who is allowed to use this information and for what purposes, and what steps are taken to identify, secure, and reduce any privacy risks to that information.

ECA's ClaimsMatrix system stores consumer and business data provided by RAO or obtained directly from individuals who submit redress claims in a proprietary database. The ECA ClaimsMatrix system also has a public interface that permits individuals and businesses to complete and submit an electronic claim form via a website. ECA uses the data from the system to fulfill its role as the redress claims administrator, which includes the following duties: (i) to intake and process claims filed; (ii) to answer questions from FTC and other authorized parties; (iii) to answer questions from claimants and potential claimants as to eligibility and status of materials filed; (iv) to route claims to the claims administrator; and (v) to issue and track payments to authorized claimants.

ECA maintains physical systems in their secure on-site location in Kansas City, KS, and their secure off-site location in Las Vegas, NV.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC collects this information in order to provide redress to injured consumers as part of its law enforcement activities pursuant to the FTC Act, 15 U.S.C. §§ 41-58, and other applicable statutes.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☐ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Business name, unique claimant ID, customer account number
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The claimant information that is collected, used, disseminated, or maintained either within RAO or within ECA's ClaimsMatrix proprietary database varies depending upon the redress matter. In routine redress matters, the data elements selected in 2.1 are collected and maintained. Additional non-PII data elements include: business name (if needed), transaction data, transaction dates, product type, company selling product, loss amount, and notes of claimant contact with ECA, including any subsequent change requests, updates, corrections, etc. These notes may potentially contain PII; for example, a customer may call to update their current address or phone number, etc.

In instances where a consumer calls ECA regarding a redress matter, the Epiq Interactive Voice Response and Contact Center systems record the number from which the individual calls and the date/time/length of call. In addition, all consumer calls to live agents are recorded, including any

[1] Per OMB M-07-16, personally identifiable information (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date or place of birth, mother's maiden name, etc.

escalations that may take place. Details of calls may be summarized in the Epiq claims management system by claims processing staff.

2.3 What is the purpose for collection of the information listed above?

Claimant information is collected, used, disseminated, or maintained by RAO staff and ECA to identify potential claimants, to validate claimants and their claims, and to distribute redress payments to appropriate claimants.

ECA's system is used to maintain claimant information for verification and record-keeping purposes relating to redress in FTC matters, as well as to calculate and distribute redress payments. These activities may include printing and mailing claim forms, processing claims and corrections submitted by claimants, issuing checks or other forms of payment, and providing consumer education.

Data collected by ECA in a specific FTC matter may also be used by the FTC and ECA to identify potentially fraudulent claims submitted in other FTC redress matters. For each redress matter managed by ECA on behalf of the FTC, ECA sends a complete list of claims filed to the FTC prior to the scheduled distribution. In an effort to identify potentially fraudulent claims, the FTC may analyze that information, refer back to data received in all redress matters past and present, and provide information regarding potentially fraudulent claims back to ECA.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Individual Members of the Public	Initial source data is found in defendants' files and in consumer complaints submitted to the FTC and transferred to ECA; this includes the data elements listed in 2.1. Claimants also provide data directly to ECA via phone or mail as part of the redress administration process.
Third party	Mailing address updates and corrections may be provided by third-party data sources such as the United States Postal Service (USPS) and Lexis/Nexis.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

FTC staff do not have direct access to ECA's databases; ECA shares claimant information and reports with the FTC via secure encrypted mail. RAO staff, managers, and supervisors of ECA staff who have access to claimant information have completed FTC-approved background checks and

clearance. In addition, all ECA employees who have access to claimant information receive background checks conducted by ECA.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC RAO Staff & ECA Staff	Authorized ECA IT professionals have access to the data for the purpose of importing, validating, updating, and storing claimant data. ECA claims processors have access to data for the purpose of validating eligibility, communicating with claimants, and updating their contact information. Both FTC and ECA management staff need to access the data for reporting purposes, as well as to supervise technology and processor resources, and ensuring accuracy and adherence to data handling standards.
Claimants	No external entities other than claimants will have direct access to claimant information. Individual claimants may submit information directly on the claims website; once submitted, however, claimants cannot view or change their information online.
Other External Parties	The FTC may share claimant information with law enforcement and other government agencies, courts, and defendants, or as otherwise authorized by law. RAO and ECA securely download and transmit required data in response to authorized requests.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

ECA employs formal, documented procedures to facilitate security awareness training, including a specific course related to PII. This training is managed and implemented by ECA's Security Team and Human Resources. Additionally, all users involved with this and other Federal Information Security Management Act (FISMA) moderate client data are required to use ECA's Electronic Governance Risk and Compliance (eGRC) portal to read and acknowledge all relevant policies and control standards.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

ECA has developed a comprehensive Incident Response Plan ("IRP") to help support continuity of critical ECA business operations in the event of an incident. The plan contains a framework for responding to information security incidents, which include but are not limited to system intrusions, system misuse, or any situation where confidentiality of sensitive data, integrity of data, or availability of business critical systems may have been compromised. The primary goal of the IRP is to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations and FTC data. In the event an incident is identified either by ECA's IT staff or

in-place utilities, ECA has a response team in place to quickly respond and rectify the situation. An added layer of security is provided by Mandiant Managed Incident Response and Managed Defense solutions to address Advanced Persistent Threats (e.g., state sponsored hacking). Mandiant uses a multi-layered approach that includes individual agents installed on all endpoints in the environment, network listeners staged at all egress points in the environment, and centralized appliances to coordinate the service. Numerous layers of security controls are in place. Breach notification timeframe is governed by contractual and legal requirements; Epiq must immediately report to the FTC all breaches of FTC materials and information. Mandiant also provides support to ECA in the event of a security breach, providing first responders, forensic investigators and Incident managers.

☐ Not Applicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

For redress cases that require ECA to collect claimant information via a claim form, a Privacy Act statement is included on both paper and web-based forms, which are compliant with the Paperwork Reduction Act (PRA) and contain an Office of Management and Budget (OMB) document control number. The Privacy Act statement explains the authority, purpose, and routine uses of the information to be collected, whether it is voluntary or mandatory for the claimant to provide the information, and any consequences if the information is not collected (e.g., the FTC may be unable to pay the individual his or her redress claim).

Those claimants who submit consumer complaints to the FTC via the FTC online complaint form – as described in the Sentinel Network Services PIA – or via the FTC telephone complaint system (1-877-FTC-HELP), receive a similar Privacy Act statement at the time they submit their complaint. Their relevant consumer complaint information is then forwarded to ECA for processing. All claimants who receive a Privacy Act statement also are provided a physical mailing address and telephone number to update and provide additional information about themselves, their eligibility to file a claim, and their claimant status.

In some cases, the FTC may receive claimant information from a defendant's customer list, and redress may be provided without the claimant having to take any action. In those instances, claimants are not provided with a Privacy Act statement; such claimants can learn about the FTC's collection, use, and disclosure of their information through the FTC's privacy policy, as noted below. In addition, all redress checks include a mailing address and/or telephone number for consumers to contact ECA should they have any questions or concerns about their information.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain):

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

When the FTC uses information provided by a defendant to mail a check to an injured consumer, the individual does not have the opportunity to decline the FTC's use of their information. In those cases, redress distributions are mailed directly to the consumer – using customer information provided by the defendant – without the consumer having to take any action. This use of personal information poses minimal risks to privacy and allows the FTC to provide refunds efficiently and effectively to as many injured consumers as possible.

In cases where there is a claims process, individuals can decline to provide their information. Consumers who choose to submit a claim do not have the right to limit their consent to particular uses of their information. They consent to their information being used as described in the applicable SORN (see Section 8.3) and Privacy Act statement. The consumer exercises this consent by choosing to complete, sign, and submit a claim form.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Claimants can submit their claim through the ECA web portal, but they cannot access, view, or edit their claim online once it has been submitted. Instead, ECA initially enters the claimant data verbatim from hard copy and online forms submitted by the claimant; alternatively, ECA may create a claim record from information submitted to them by the RAO. If a claimant's information is incomplete, ECA mails a letter to the claimant informing the individual that their claim is incomplete due to missing or incorrect information; the claimant is sent a new blank copy of the claim form to update their information and complete the claims process.

Claimants can access their claim record by contacting ECA via telephone or hardcopy mail. Before making requested changes to a claimant's information, ECA will confirm the claimant's identity by asking a series of questions, including the claim record tracking number, name, mailing address on file, or phone number, and instructing the claimant to forward their change request in writing along with supporting documentation if needed. ECA accepts written documentation via fax, mail, or email. Finally, claimants can obtain access to their own information through a Privacy Act request filed with the FTC's Freedom of Information Act (FOIA) Office.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated above in Section 4.3, claimants can request corrections to any inaccurate information by contacting ECA, validating their identity, and forwarding the change request in writing along with any supporting documentation as necessary. Claimants also can file a Privacy Act request through

the FTC's FOIA Office to obtain access to their own information. The FTC FOIA Office will work with the claimant to respond to any complaints, concerns, or questions.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to the contractor mailing a claim form, a redress check, or consumer education material, claimant addresses are standardized and cross-checked against data sources, such as the U.S. Postal Service (USPS) National Change of Address Database and USPS records regarding street names and address ranges. All resulting additions, deletions, and address changes to the data set are approved by the RAO and reconciled against the original source data.

In many instances, claimant data obtained from defendants' files can be used to mail redress checks directly to injured consumers and businesses. In other cases, individuals are contacted to provide or verify their information. For example, claim forms may be mailed to a known set of claimants requesting that they validate their address, loss amount, and entitlement to redress. In other cases, claim forms will be made available to previously unknown claimants via case-specific redress notification and outreach. Claimants provide claim information, including their address, injury amount, and entitlement to redress, under penalty of perjury.

The redress contractor reviews claimant names, check distributions, and claim form responses to confirm that the loss amounts claimed are consistent with the established case-specific claim parameters. Outreach material, redress checks, and claim forms always include an FTC website address for additional information, and a telephone number and mailing address for consumers to contact the redress contractor to have their questions answered and/or to update their information.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Data in the system will be accessed only by authorized RAO and ECA staff to review and determine claimant eligibility for redress. The data will be accessed via secure login, and access will only be made available to authorized staff on a need-to-know basis. Data usage is in accordance with the uses described in the executed contract between the FTC and ECA to support the FTC's redress activities.

Prior to maintaining and disseminating claimant data, RAO staff removes all unnecessary information from the claimant data file and encrypts all data transmitted to ECA via email. ECA encrypts claimant data at rest. In addition, the FTC instructs ECA to collect the least amount of claimant information necessary.

If personal information is collected through a web site, page, or online form accessible through the Internet, appropriate Transport Layer Security (TLS) encryption algorithm is used to protect all external communications.

ECA employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access to consumer data. These controls include, but are not limited to the following:

- ECA websites are hosted within a FISMA accredited boundary;
- ECA websites are maintained on a separate network segment from the consumers' specific claims data;
- When appropriate, claimants are provided a unique claim identifier and PIN to verify that they are a member of the redress pool;
- Consumer data is encrypted when transmitting between the web server and client based computing device;
- Administrative controls include lockout after a number of failed attempts, server event logging, and standard web logging, including collection of IP addresses for security and performance troubleshooting.

The ECA ClaimsMatrix system uses a defense-in-depth strategy to protect system resources against attacks by utilizing security technologies and services that maintain the Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation requirements outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53.

Audit trails maintain a record of authorized and unauthorized system events both by system and application processes and by user activity of systems and applications. Audit logging is continuous, and logs are archived to provide access for review. In conjunction with other processes and controls, such as incident response capabilities and user identification and authentication, audit trails can assist in detecting security violations, network performance problems, and flaws in applications. Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis. The ECA systems are periodically reviewed by FTC staff as well.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes, ECA has undergone the appropriate security risk assessment and received authority to operate. ECA employs both information security and physical security for the privacy-related information it collects. ECA is categorized as a moderate system using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems. The claims administration contractor has received an Authorization to Operate (ATO), which was issued in accordance with FISMA following guidance provided by NIST. Contractor systems are routinely reviewed by the FTC to ensure compliance with FISMA.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Development and User Acceptance Testing (UAT) environments are physically and logically separate from that of production, and UAT mirrors production as closely as possible at both the hardware and software levels. This structure allows performance testing and valid user acceptance testing to be performed without the risk of disruption to production or client environments. FTC data is not used in lower environments except in cases of a data specific issue. In such cases, FTC approval is be obtained prior to use, to minimize and protect PII during such use, and data would be deleted immediately upon remediation of the data specific issue.

☐ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

All data is stored within ECA's secure, layered environment; in order to mitigate potential risks, all communication in and out of ECA's systems is encrypted and signed using Federal Information Processing Standard (FIPS) 140-2 approved libraries. Full backups of all production data are routinely conducted. Encrypted backups are replicated to an off-site datacenter through a dedicated, secure connection, for business continuity purposes.

All records and documentation, including any notes, recordings, and audit logs pertaining to FTC claim matters, will be maintained by ECA for the duration of the claims process in accordance with General Records Schedules 3.1 and 4.2. At the end of the claim closure period, ECA shall transfer a trustworthy electronic copy of the records and documentation to RAO. After review and approval of RAO, ECA shall then destroy all records and documentation in its possession associated with the matter, in accordance with NARA, OMB, and NIST regulations and guidelines. RAO maintains records in accordance with the FTC's NARA-approved records retention schedule, N1-122-09-1.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

☐ Not Applicable

ECA does not host any permanent websites on behalf of the FTC. However, ECA may host a temporary website in a particular redress matter when the FTC determines it is appropriate and necessary to support online electronic claim submission. Persistent tracking technologies will not be used on these temporary, matter-specific redress sites. Temporary session cookies will be used for user session verification and will be terminated at the end of the visit. These cookies do not store any

PII, and the information they obtain cannot be directly correlated to an individual claimant. See the FTC's Cookie Page for more information. ECA staff reviews each temporary website for compliance with the privacy requirements.

In compliance with the Privacy Act of 1974, the E-Government Act of 2002, guidance issued by OMB, and the FTC's own Privacy Policy, the FTC mandates that ECA limit the collection of information from website visitors to the information necessary to assess and improve user experience, respond to consumer concerns, and administer redress.

To the extent that ECA's web hosting provider collects standard web log data, such as IP address, date and time of visit, and other required information, for cyber security and management reporting, such collection is needed to ensure compliance with FISMA, 44 U.S.C. § 3541 et seq.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Personally identifiable information is maintained by both RAO and ECA.	In order to minimize privacy risks, in the vast majority of redress matters, the information stored by RAO and ECA is limited to name, contact information, and claim information, possibly coupled with validation under penalty of perjury. Comprehensive data security plans have been implemented to protect all data, including frequent, automated scans of information systems as well as policies and procedures to limit access to sensitive data and to ensure compliance with data privacy standards. To ensure the security of the data, the systems use TLS encryption between the server and each ECA user. Each FTC or ECA user must use a secure password to gain access to the system as a whole, and then only users authorized to work on a particular redress matter have access to that matter's data.
Individuals are provided with access to their own information.	Various steps are taken to ensure that individuals only are able to access their own information. Individuals can only submit their information through the ECA-hosted website for a specific redress matter. They cannot access or alter previously entered information. Alternatively, if an individual seeks access to their information through the FTC's FOIA office, the risk of unauthorized disclosure is mitigated by procedures for asking the individual to verify his or her identity in writing, or, if the individual has authorized a representative to have access, to provide proof of such authorization in writing.
Individuals may provide unnecessary PII or data	When submitting a claim form, a claimant may inadvertently provide PII, including sensitive PII or health information, that is not

that is inaccurate or incomplete.	be required or requested for claims processing or verification. To mitigate this, claims forms do not include open-text comments fields. Furthermore, fields are limited to the minimum information necessary to process a claim to reduce the risks of a user accidentally providing unnecessary information. SSNs are not collected on claim forms. As to the risk that data provided might not be accurate, complete, or timely, it is important to note that individuals voluntarily provide claim information on the website so that they may receive redress. The process of filing claims is made as easy as possible for individuals. Claims have the ability to validate and verify claimant information and to update any inaccurate information. To the extent claimant information is provided via defendant's records, ECA and the FTC make every effort to confirm the information received is accurate, such as cross-checking with U.S. Postal Service address lists.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

ECA's architecture prevents direct access to the data sets. ECA employees wishing to access the systems must use two-factor authentication. Technical management communications for all systems within the Client Data Environment (CDE) are firewalled to a specified Virtual Local Area Network (VLAN). Individual drives on the Storage Area Network (SAN) are self-encrypting, ensuring physical possession of the hard drive will not endanger customer data.

All remote access occur over Virtual Private Network (VPN) connections, require use of two-factor authentication with a physical or soft token for management approved users, and is authenticated over a secure VPN.

ECA's login policy is configured to enforce sessions and workstations to automatically lock after a period of inactivity. The user's password is required to unlock the workstation and two-factor authentication is required to reconnect to the secure environment. System lockout occurs after five invalid login attempts.

Additionally, PII can be masked to end users depending on the level of classification.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Consumers are assigned a unique ID for identification, tracking, and reporting purposes. As such, the redress contractor databases are covered by existing Privacy Act SORNs for nonpublic FTC program records, FTC-I-1, and for computer system user and identification access records, FTC-VII-3.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

ECA has account management policies and controls in place to manage ClaimsMatrix system accounts, including the establishment, activation, modification, and termination of system accounts. ECA account management activities include:

- Identification of account types;
- Conditions for group membership;
- Identification of authorized users specifying access privileges;
- Requirement of appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring use of the guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when users are terminated, transferred, or access requirements change;
- Deactivating temporary accounts and accounts of terminated users as required;
- Granting access to the system based on valid access authorization; intended system usage, and other attributes as required by the organization;
- Reviewing accounts quarterly, at a minimum.

The collection, use, and disclosure of information from the ECA claims administration system has been reviewed to ensure consistency with the FTC's Privacy Policy.

9 Approval and Signature Page

Prepared By:

_____ **Date:** _____
Nicole V. Fleming
Bureau of Consumer Protection (BCP)

Reviewed By:

_____ **Date:** _____
Katherine Race Brin
Chief Privacy Officer (CPO)

_____ **Date:** _____
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date:** _____
Jeffrey M. Smith
Chief Information Security Officer (CISO)

_____ **Date:** _____
Jeffrey D. Nakrin
Director, Records and Filing Office

Approved By:

_____ **Date:** _____
Raghav Vajjhala
Chief Information Officer (CIO)