Federal Trade Commission
Privacy Impact Assessment

Bureau of Consumer Protection (BCP)
Tech Lab

October 2016

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission's ("FTC's") Bureau of Consumer Protection ("BCP") strives to protect consumers from fraudulent, deceptive, and unfair practices in the marketplace. To accomplish this mission, the FTC conducts investigations, takes law enforcement action against those breaking the law, develops rules to maintain a fair marketplace, conducts research and issues reports to shed light on important issues, and educates consumers and businesses about their rights and responsibilities. The FTC monitors changes in the marketplace, evaluates emerging practices, and identifies consumer protection issues associated with the use of technology.

The BCP Tech Lab ("Lab") provides FTC staff with Internet access, devices, software, and other technological tools to conduct investigations and research in support of the FTC's consumer protection mission. On occasion, FTC staff use the Lab to conduct investigations and research in support of the FTC's mission to promote competition.

BCP's Division of Litigation Technology & Analysis ("DLTA") owns and manages the Lab. The Lab is composed of a main facility and network in Washington, DC, as well as eight satellite locations in each of the FTC's regional offices. The Lab consists of networking hardware and software; various types of consumer technology including computers, mobile devices (e.g., smartphones, tablets, and other wi-fi capable devices), and Internet of Things devices; peripherals including monitors, printers, and scanners; cameras and recording equipment; and various types of software and applications.

The Lab is primarily used by BCP staff (i.e., investigators, technologists, attorneys, and paralegals), but also may be used occasionally by FTC staff in other Bureaus and Offices, authorized law enforcement partners, and FTC-retained experts and contractors. BCP staff use the Lab to investigate unfair, deceptive, or fraudulent practices and to conduct research into consumer protection issues associated with technology. To accomplish these tasks effectively, staff must be able to access the Internet and interact with technology in the same manner as typical consumers. To enable this, the Lab's network in Washington, DC, is physically isolated from the FTC's production network (which has extensive security and other restrictions) and the regional office Lab connections are logically segregated from the FTC's production network. The Lab has computers and other devices dedicated to investigatory and research use.

In conducting investigations and research, Lab users access content that is already available to the public either for free or payment (e.g., a paid mobile app or paywalled database). The tools available in the Lab allow users to analyze and collect digital content (including images, recordings, and code), Internet protocol, network traffic, tracking technologies, data flows between devices, website information, usage data, viruses, spyware, malware, and other threats. Lab users must initiate the collection of information, though a Lab user could configure a device to scan or collect data on an automated basis. The Lab also provides users with the tools and ability to create email addresses, mobile accounts to purchase apps, social media profiles, mock websites, and computer code for use in investigations and research.

The information accessed above may include personally identifiable information ("PII"), such as names, physical and email addresses, phone numbers, IP addresses, financial information, and audio recordings. Individuals are not given notice of the collection. In most instances, the

information collected is already available to the public (e.g., posted on a website). In other situations, Lab users may obtain information from targets of undercover investigations or through research into unfair, deceptive, or fraudulent practices.

The Lab provides tools to help staff organize data as well as limited access file storage to temporarily preserve digital content for investigations and research. Information that must be retained for investigative or research purposes is removed from the Lab and either preserved on physical media (pursuant to the FTC's data protection and privacy policies) or copied into a limited access folder on the FTC's production network. The length of time data will be preserved depends on the length of the investigation and any subsequent law enforcement action, and the length of time to complete research projects.

Lab users occasionally utilize stand-alone equipment located in the Lab to access and scan electronic media for viruses or malware. This electronic media (e.g., DVDs, hard drives, etc.) is provided to the FTC either voluntarily or pursuant to compulsory process, subpoenas, or court orders.

The FTC also collects and maintains information about individual staff access to and usage of the Lab for security and auditing purposes.

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

The Lab is used to collect and maintain information pursuant to the FTC's investigatory, law enforcement, and research authority set forth in the Federal Trade Commission Act, 15 U.S.C. §§ 41 – 58.

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)*: Credentials such as API keys used in authentication for various web services such as Twitter, Google, and Amazon.
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☒ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

Note: Because the function of the Lab is open-ended and designed to respond to emerging consumer protection threats, this list may not be exhaustive.

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 Lab is used to view, collect, and where appropriate, preserve information that is available through the Internet and mobile applications. Lab users may collect and preserve static or dynamic digital images and recordings as well as raw digital content (e.g., code). Lab users also can analyze and capture Internet protocol,[2] network traffic, tracking technologies, data flows between devices, website information, usage data as well as viruses, spyware, malware, and other threats.

[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.

[2] Internet protocol refers to the communications protocol or principal set of digital message formats and rules for exchanging data across network boundaries.

In addition, access and event log data about internal Lab user activities, including the Lab user's name, phone number, organization code, date and time of entry and exit, mobile device usage, and network traffic are collected and maintained for management, security, and auditing purposes.

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

Information is collected in the Lab to conduct investigations and research that support primarily the FTC's consumer protection mission (and on occasion, the FTC's competition mission). When investigating whether targets are engaged in unfair or deceptive practices, staff must obtain evidence of the target's practices. For example, the Lab may be used to collect and preserve websites or mobile application content posted by the targets of an FTC investigation. These websites and mobile app content may contain statements or features that are likely to mislead consumers. The FTC must collect and preserve this content to prove in court that the target's website or app contained a statement and appeared in a particular manner on a particular day.

Lab users also collect information as part of their research into consumer's use of technology and the consumer protection issues associated with technology. For example, the Lab may be used to view, collect, and preserve the data transmitted between devices (e.g., from an IOT device to an app on a mobile device), and to third parties. Lab users also may examine the manner in which the data is transmitted, such as whether data is encrypted; the use and prevalence of various security practices; the nature and operation of scams; and the nature and use of malware, among other things. Lab users must collect information in order to effectively analyze the data and to have evidence from which users may draw conclusions. Research findings may be used to inform internal FTC policy and/or to provide information and guidance to consumers, businesses, and policymakers.

Lab activity and usage information is collected and maintained for administrative and security purposes, and to ensure Lab usage is appropriate.

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*
Publicly-available internet services	The FTC collects information primarily from the web or through mobile applications. This information is collected by capturing content, data, network protocols, and communications. In addition to collecting information offered for free, the FTC collects information through paid services.
Individual members of the public	The FTC collects information from individual members of the public who are targets of law enforcement investigations or who engage in activities that are the subject of FTC research. This information is collected by capturing content, data, network protocols, and communications.
Public records	The FTC may collect information from public records to support its

	investigations and research, such as corporate record information and real property ownership.
Lab users	Lab activity and usage information is collected through system event and device usage logs. In addition, the FTC's Administrative Services Office collects physical access information by logging key card access to the Washington, DC, Lab.

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.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC Staff	FTC staff have access to the Lab to conduct investigations and research in support of the agency's consumer protection mission. All BCP employees have physical access to the Lab; other FTC staff must request access based on business need and obtain approval from the DLTA Assistant Director. To obtain access to the Lab network, staff must sign a Rules of Behavior form and select a User ID and password. A User ID and password is required to obtain access to the Lab network. Lab users are granted the fewest folder and file access rights needed to perform their duties. Therefore, only those staff assigned to work on a specific investigation or research project may have access to the information collected in the Lab pertaining to that matter. FTC staff may share information collected in the Lab with external entities that do not have direct Lab access, including, for example, courts, opposing counsel, defendants, expert witnesses, or other individuals as otherwise authorized by the law. See, e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.
FTC Contractors	If an FTC contractor or expert is assigned to work or consult on a specific matter, they may have access to information collected in the Lab pertaining to that matter. If a contractor is assigned to assist Lab Administrators with maintenance and support, the contractor would have access to all information in the Lab.
Authorized Law Enforcement Personnel	Authorized non-FTC law enforcement staff may have approval to use the Lab, pursuant to the procedures discussed above for FTC staff, and may have access to the information related to the matter to which they are assigned.
Authorized Lab Administrators	FTC staff who are assigned to manage the Lab network have administrative privileges and access to all information in the Lab.

Authorized Lab Administrators and OCIO staff	These staff have access to the information collected from Lab usage records.

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.

☐ Not Applicable

There are two general types of contractors who may have access to data in the Lab. First, contractors who provide assistance to FTC staff on a particular investigation or research project would have access to data in the Lab that is related to that matter. Second, contractors who provide assistance to Lab Administrators in Lab maintenance and support would have access to all information. Lab Administrators would give assignments and instructions to the contractor and oversee their work. These contractors must adhere to the same rules and security procedures as Lab Administrators. In addition, all access to and actions taken in the Lab infrastructure are logged.

In both scenarios, contractors would sign a rules of behavior form to obtain access to the Lab. In addition, all FTC contractors are required to complete computer security and privacy awareness training annually. Finally, all FTC contractors are subject to a non-disclosure agreement.

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.

Contractors who assist Lab Administrators perform all of their work within the FTC-owned Tech Lab. These contractors are not permitted to remove data from the Lab. Therefore, the contractor's privacy incident response plan is not applicable. Instead, the contractor is subject to the FTC's Breach Notification Response Plan.

☒ 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.

☐ 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): _____

Individuals are not given notice of the collection. In most instances, the information collected is already available to the public (e.g., posted on a website). In other situations, Lab users may obtain information from targets of undercover investigations or through research into unfair, deceptive, or fraudulent practices. Lab users therefore do not provide notice to these individuals about what information is collected or how it is used. This PIA, however, provides such individuals with general notice as to the nature and scope of information that the FTC may collect from them, if any, and the purposes for such information collection and maintenance.

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)?

No. In most instances, the information collected is already available to the public (e.g., posted on a website). In other situations, Lab users obtain information from targets of undercover investigations or through research into unfair, deceptive, or fraudulent practices. Lab users therefore do not provide notice to these individuals about what information is collected or how it is used, other than this PIA, as explained above.

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

Individuals may make a request for access to FTC records under the Privacy Act and the Freedom of Information Act (FOIA). The rules and procedures for making these requests are published in the Code of Federal Regulations, 16 C.F.R. 4.13, and on the FTC's website. Because the primary Lab use is for law enforcement, records about certain individuals (e.g., targets and defendants) may be exempt from mandatory access by such individuals. See 16 C.F.R. 4.13(m) (exemptions applicable to certain FTC Privacy Act system of records); 16 C.F.R. 4.10 (FTC nonpublic records, including those exempt from FOIA disclosure).

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 discussed in 4.3 above, because the primary Lab use is for law enforcement, records about certain individuals (e.g., targets and defendants) may be exempt from mandatory access or correction by such individuals. Individuals may file requests with the FTC under the FOIA and the Privacy Act of 1974 for access to any agency records that may be about them and are not exempt from disclosure to them under those laws.[3] Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly.

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?

Not applicable. The information collected by Lab users is not systematically checked for accuracy and timeliness in light of the purposes for which the information is collected and used, (i.e., law enforcement and research). Information available on the Internet and mobile marketplace is subject to frequent and continuous change. Therefore, information that is collected by users is considered an accurate representation of the content as of the time it was collected.

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.

All BCP staff are granted *physical* access to the Lab as part of the employee check-in process. Other FTC staff, FTC contractors, and law enforcement partners may request access to the Lab based on business need, and these requests must be approved by the DLTA Associate Director.

Administrative information about Lab usage is monitored by Lab Administrators and is subject to review and audits by OCIO. Lab activity and usage details are collected through system event and device usage logs and may be reviewed periodically to ensure Lab users are utilizing the system for legitimate business needs and authorized job-related purposes.

To obtain access to the Lab *network*, all users must sign a Rules of Behavior form and create a user account. Lab Administrators utilize Active Directory to provide logical access to Lab users. (The Lab uses an independent instance of Active Directory, which is controlled by Lab Administrators.) Users must select a User ID and password, which are then used to obtain access to the Lab network. The ID and password are different from the users' login and password for the FTC production network. Users are required to have a password length and complexity that is compliant with OCIO policies, and passwords are required to be changed every 60 days. If there are five consecutive invalid attempts to access the Lab during a 30-minute period, the Lab will lock the user's account for one hour.

[3] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

Non-BCP staff user accounts must have an expiration date. BCP users who leave the agency must check out with a Lab Administrator; based on this, their account is disabled. Lab Administrators also disable accounts based on their monthly review of agency records listing staff who have transferred to another part of the agency or left the agency. In addition, accounts that have been inactive for more than 90 days will be deactivated.

Lab users must review and sign the Rules of Behavior form annually. Lab Administrators notify users of this requirement, and disable accounts if users fail to do so within 30 days.

Lab users are granted the fewest folder and file access rights needed to perform their function. Each user is provided with limited access storage space on the Lab's storage area network. This space is accessible to only the assigned user (and Lab Administrators). Limited access storage space may be assigned to a particular investigation or research project. In those instances, only those staff working on that matter are provided with access to the storage space. Users may temporarily save information they obtain while using Lab resources to the storage folder. Lab users are instructed not to save data locally to Lab workstations. Any data that is saved locally is deleted on a monthly basis as part of regular Lab maintenance procedures. Similarly, the Lab deletes data and apps saved on mobile devices on a monthly basis as part of regular Lab maintenance.

Any data that must be maintained for investigative or research purposes is removed from the Lab, typically for inclusion in a larger investigative file. This information is subject to FTC data protection and privacy policies, including those pertaining to the safeguarding of PII. (For a discussion of the FTC's system for maintaining non-public investigational or other legal records, see FTC System of Records Notice I-1. This data may be preserved on physical media or copied into a limited access folder on the FTC's production network. This network is part of FTC Data Center General Support System.

The Lab also maintains mobile devices that any user can access for investigative or research purposes. Any data or apps saved on the device are deleted on a monthly basis as part of regular Lab maintenance procedures. If users need to retain mobile evidence for investigative or research purposes, they can request that a device be assigned to their particular investigation and segregated from general use. The user stores the device either in locked cabinet in the Lab or in his or her office.

To provide further safeguards, the Lab network is subdivided into virtual local area networks ("VLANs") within security zones for the purpose of segregating computing resources based on function and purpose. In the Lab, the security zones segments are set aside for specific functionality associated with users performing investigations as a typical consumer or end user, researching Internet and associated technologies, and administrative applications or sensitive servers with elevated privileges. Depending on the rule sets, purpose, and function of the specific zones, data may or may not be transported from one zone to another.

The Lab's firewall helps to prevent sensitive data loss potentially occurring through the Lab. The firewall enables the Lab Administrators to detect critical pieces of PII, such as Social Security or credit card numbers, within application traffic. The rules that are set in the firewall by Lab Administrators are based on defined polices so the firewall can then take automatic action when it finds data that matches the rules – from alerting to blocking – to prevent inadvertent or intentional disclosure of sensitive data. For example, if the firewall detects transmission of credit card numbers or Social Security numbers on the Lab's investigative and research zones of the

network, it alerts Lab Administrators. Because these transmissions frequently occur with undercover purchases, the firewall does not block this activity; it merely detects it. However, if the transmission occurs on the management and server zones of the network, the firewall blocks the transmission to prevent data loss.

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

A risk assessment for the Lab was completed and an Authorization to Operate was granted in April 2016.

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?

☒ Not Applicable

Staff use undercover identities/dummy PII when using the Lab to conduct investigations and research – such as signing up for web-based services, testing apps, or determining what information an IoT device transmits to third parties.

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?

Lab users may retain information collected in the Lab for use in an investigation, law enforcement action, or a research project. The length of time data will be preserved depends on the length of the investigation and any subsequent law enforcement action, and the length of time to complete research projects. The content and context of information collected in the Lab conforms to the definition of "non-record materials" as identified in 44 U.S.C. 3301 and 36 C.F.R. 1222.14. National Archives and Records Administration (NARA) guidance is to destroy or delete non-records when they are no longer needed.

Information in the Lab, including any information that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with applicable schedules issued or approved by NARA.

Disposal of Lab information is conducted in accordance with FTC policies and procedures and in compliance with OMB, NARA, and NIST guidelines. For destruction of removable media and hard drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitization and destruction.

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

The Lab does not host any websites for use by the general public. However, in connection with particular matters, Lab users may set up temporary websites within the Lab for investigative or research purposes. These temporary websites may be accessed by contractors and expert witnesses for investigative or research purposes. In these circumstances, access to the site is limited by IP address, so only those individuals with permission to access the website can do so.

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*
Information contained in the Lab may be exposed through a breach, introduction of malicious code, or other incident.	The Lab has several safeguards to minimize the risk of a breach. The Lab network is subdivided into VLANs within security zones for the purpose of segregating computing resources based on function and purpose. The use of VLANs limits the access of any hacker or malicious code, and therefore increases the level of protection of the information collected in the Lab. In addition, as discussed above, the Lab's firewall also helps to prevent data loss.

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

As discussed in 5.2 above, Lab users must have an account (User ID and password) to obtain access to the Lab network. Users must change their passwords every 60 days. The Lab will lock a user's account for one hour after five consecutive invalid access attempts during a 30-minute period.

Lab users are granted the fewest folder and file access rights needed to perform their function. Each user is provided with limited access storage space on the Lab's storage area network. This space is accessible to only the assigned user (and Lab Administrators). Limited access storage space may be assigned to a particular investigation or research project. In those instances, only those staff working on that matter are provided with access to the storage space.

To provide further safeguards, the Lab network is subdivided into VLANs within security zones for the purpose of segregating computing resources based on function and purpose. In the Lab,

the security zone segments are set aside for specific functionality associated with users performing investigations as a typical consumer or end user, researching Internet and associated technologies, and administrative applications or sensitive servers with elevated privileges. Depending on the rule sets, purpose, and function of the specific zones, data may or may not be transported from one zone to another.

The Lab's firewall helps to prevent sensitive data loss potentially occurring through the Lab. The firewall enables the Lab Administrators to detect critical pieces of PII, such as Social Security or credit card numbers, within application traffic. The rules that are set in the firewall by Lab Administrators are based on defined polices so the firewall can then take automatic action when it finds data that matches the rules – from alerting to blocking – to prevent inadvertent or intentional disclosure of sensitive data. For example, if the firewall detects transmission of credit card numbers or Social Security numbers on the Lab's investigative and research zones of the network, it alerts Lab Administrators. Because these transmissions frequently occur with undercover purchases, the firewall does not block this activity; it merely detects it. However, if the transmission occurs on the management and server zones of the network, the firewall blocks the transmission to prevent data loss. There would be no reason for sensitive PII to be transmitted from those zones, and the automatic blocking supports the privacy of such information from being compromised by the system.

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).

No. The Lab is not a system of records retrieved by individual name or other personal identifier under the Privacy Act. Rather, information removed from the Lab is normally incorporated into FTC nonpublic investigatory files, which are part of the Privacy Act system of records designated as FTC I-1.

The Lab user logs, which control user access to Lab resources and track Lab user activities, are part of a separate FTC system of records, see VII-3, Computer Systems User Identification and Access Records – FTC. Key access logs, which record the use of FTC key cards when users access physical Lab facilities, are part of another FTC system of records, see II-11 – Personnel Security, Identity Management, and Access Control Records System – FTC. See the FTC's SORN page for descriptions of these FTC record systems.

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?

Lab Administrators periodically review access logs, storage logs, and firewall logs to ensure that users are complying with the Lab policies and procedures. Selected security controls are audited on a yearly basis, which results in all the controls being evaluated every three years. In addition, Lab users must review and sign the Rules of Behavior form annually.

Approval and Signature Page

Prepared By:

_____ **Date: _____**
Laura DeMartino
Bureau of Consumer Protection
Division of Litigation Technology & Analysis

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)