Federal Trade Commission
Privacy Impact Assessment

FTC Emergency Notification System

February 2016

1 System Overview

The Federal Trade Commission (FTC) Emergency Notification System (ENS) uses Send Word Now (SWN) to inform FTC staff and on-site contractors (hereafter FTC staff) of emergency closings, severe weather, major traffic disruptions, and other urgent matters affecting the FTC workplace. SWN is a cloud-based service maintained and operated by a third-party vendor, and allows 24/7 system access for the sending of the above-described notifications (and for other purposes as described below) via any internet connection. Using a third-party contractor allows notifications to be sent at any time, even during a disruption of the FTC network. ENS is administered and maintained principally by the agency's Occupational Health and Safety Manager, who is also the Master Administrator for the system.

The ENS Master Administrator, or a designated and approved FTC system administrator, creates system accounts in the ENS for all FTC staff that contain the following types of FTC Contact Points (CPs): (1) FTC staff name, (2) user type (government or contractor employee), (3) office location, (4) organization code, (5) FTC email address, (6) office phone number, and (7) FTC-issued mobile device number for each FTC staff. Only the ENS system administrator may affect changes to FTC CPs associated with an FTC account. FTC staff also can choose to have notifications sent to their personal email addresses, home telephone numbers, and personal mobile devices (collectively, personal CPs) to ensure the timely delivery of the information during non-business hours. Personal CPs are provided voluntarily by FTC staff via a secure Web-based self-enrollment portal. Only FTC staff with established accounts are able to log on to FTC ENS through this portal and add or modify their personal CPs. Up to seven (7) additional CPs can be added for each system user. SWN notifications will ordinarily be sent to FTC CPs (e.g., an email to the user's FTC email address, and/or text message to his/her FTC-issued mobile device).

As noted above, SWN notifications can be sent to FTC email addresses, office phones, FTC-issued mobile devices, and personal CPs. The FTC ENS system administrator sending the notification selects the specific method of FTC CP used for each notification (e.g., the FTC email address, office phone number, or FTC-issued mobile device). Further, FTC notifications are transmitted to their personal CP(s) as provided via the Web-based self-enrollment portal. ENS also includes a feature that allows the recipient to respond to the notification. In the event of an emergency, this feature typically would be used to confirm that FTC staff are safe or to determine if assistance is needed.

Because this system maintains information relating to FTC staff only and not members of the general public, a Privacy Impact Assessment (PIA) is not legally required by the E-Government Act.[1] However, as a best practice, the FTC is conducting this PIA to help ensure that agency staff and on-site contractor personal contact information (i.e., home

[1] The E-Government Act of 2002 (Pub.L. 107-347, 44 U.S.C. § 101), Section 208 requires that all federal agencies conduct Privacy Impact Assessments (PIAs) for all new or substantially modified information technology systems that collect maintain, or disseminate personally identifiable information (PII).

address, personal telephone number) that is entered and maintained in the ENS database is protected from unauthorized access or use.

2 Information Collected and Stored within the System

1. What information is to be collected, used, disseminated, or maintained by the system?

ENS maintains a database of accounts for FTC staff, and each account includes the following FTC CPs: (1) FTC staff name, (2) user type (government or contract employee), (3) office location, (4) organization code, (5) FTC email address, (6) office phone number, and (7) FTC-issued mobile device number for each FTC staff. This information is entered into the database by the authorized ENS system administrator. The FTC organization code is included to facilitate sending notification to a targeted group of individuals; for example, an event impacting all Washington, D.C.-based users would result in notifications being delivered to that regional group. FTC staff also can choose to have notifications sent to personal CPs, including personal email addresses, home telephones, and personal mobile devices.

To support the system's principal function of sending notifications to FTC staff, ENS maintains login credentials (username and password) for: (1) FTC staff who choose to enter additional personal CPs or edit their personal notification preferences, and (2) FTC ENS system administrators. ENS also generates logs of system access (both user and system administrator), notifications sent, and responses received from recipients. The system also provides tracking of email notifications via the Alert Tracer. This feature indicates if an email has been transmitted successfully or if it has encountered errors during delivery. Alert Tracer does not track if the email has been opened or reviewed. A separate SWN polling and response feature, Get Word Back, can be used by the FTC system administrator to ensure that recipients have opened and read the email alerts. The recipient is provided a multiple-choice response and can reply via email or text message.

2. What are the sources of the information in the system?

FTC CPs are imported into SWN from an existing FTC database. Specifically, the initial FTC CP data will be compiled into an Excel spreadsheet and uploaded to ENS by the FTC ENS Master Administrator. This initial data load includes FTC CPs only as described in Section 1 above; no personal CPs are imported/input by the FTC ENS Master Administrator. On a monthly basis, an FTC ENS Master Administrator will add additional FTC CPs for new FTC staff. (See sections 2.4 and 2.5 below for further details about CP updates and modifications.)

Personal CPs are provided voluntarily by FTC staff via a secure self-enrollment portal that requires a unique user ID and a password of the user's choosing. Only FTC staff having an established account are able to log on to FTC ENS and add or change their personal CPs. (See section 5.5 regarding establishment of accounts.)

FTC staff have the option of responding to an emergency notification via the Get Word Back feature. This information is limited to a multiple-choice response and is provided by email or text message.

3. Why is the information being collected, used, disseminated, or maintained?

CP information is collected to notify FTC staff in the event of an emergency or other urgent situation (e.g., earthquake, office closings, etc.).

Certain CPs, including office location, organization code, etc., are collected to allow system administrators to tailor messages depending on the circumstances (e.g., to send an alert to the Northeast regional office only).

Login credentials are collected and stored to provide a secure environment for administration of the system. The SWN generates system logs to support continuous monitoring activities performed by SWN administrators for specific parameters to include system administrator activity, data access/deletion/changes, and permission changes.

Alert Tracer data are compiled to help determine and ensure that email notifications have been successfully delivered. FTC staff responses provided via the Get Word Back feature are collected to allow FTC's emergency command to confirm individual receipt of a notification and to target assistance to that individual, if appropriate or necessary.

4. How is the information collected?

As stated in section 2.2, the FTC CPs are derived from an existing FTC database and compiled into an Excel spreadsheet. The FTC ENS Master Administrator completes the initial import of information via the SWN Administration Portal. The FTC ENS Master Administrator or a designated and approved FTC system administrator will complete subsequent additions, modifications, and deletions to user information via the Administration Portal. Personal CPs are voluntarily provided by FTC staff via a secure self-enrollment portal.

Login IDs and passwords are created, collected, and maintained in the system as described in section 6.7 below. These login credentials are requested and collected from users by the SWN system for verification against the user credentials maintained in the system database each time FTC staff logs into the system.

5. How will the information be checked for accuracy and timeliness (currency)?

The FTC ENS system administrator will routinely update (at least monthly) the FTC CPs in the database to reflect new hires, departures, organizational moves, and changes to FTC CPs. The system relies on FTC staff to confirm and update personal CPs in their online accounts. FTC staff are sent periodic reminders to check the accuracy of personal CPs and to update accordingly. The FTC system administrator will delete all data of

former FTC staff in accordance with approved retention schedules. When FTC staff leave the agency, their FTC accounts along with the corresponding personal accounts are deleted from the ENS via the secure SWN administration portal.

6. Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

No. The SWN system replaces the FTC Alert system that operates in a similar manner and contains similar data.

7. What law or regulation permits the collection of this information?

Collection of this information is permitted by and consistent with the FTC Act, 15 U.S.C. § 41 *et seq.*, the Federal Information Security Modernization Act, 44 U.S.C. 3551 *et seq.*(FISMA), and other Federal laws and regulations.

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

Risks:

(1) Inadvertent or unauthorized disclosure of, or unauthorized access to, FTC staff CPs (FTC and personal) and account login credentials.
(2) Unauthorized use of FTC and personal CP data for unsolicited communications to FTC staff and contractors.
(3) Malicious alteration or deletion of FTC user account data.

Mitigations:

Administration of the FTC's account is strictly limited to the ENS Master Administrator and/or other authorized individuals who need to manage the system and send notifications. In addition, the SWN platform contains a number of security and access controls, including: (1) administrative access limited to ENS system administrator or his designee, (2) access to ENS limited to those FTC staff who have an account, (3) FTC staff only able to access their own account (4) use of website page timeouts, (5) use of HTTPS protocol, (6) requirement for account passwords and security questions for password reset requests, and (7) use of data encryption in transit and at rest.

SWN has a policy requiring that all of its employees certify at least annually that they have received and read a copy of the SWN Information Security Policy (ISP) and will comply with all requirements in the ISP applicable to their job functions. New SWN employees will receive a copy of the ISP upon commencement of their employment and will be required to provide the certification at that time. SWN has certifications in place from all current employees. The ISP covers a broad range of privacy and security topics. Additionally, SWN employees receive additional specialized, in-depth training relative to

their job responsibilities. SWN outside consultants, contractors, and temporary employees are subject to the same information security requirements and have the same information security responsibilities as SWN work force members. All agreements dealing with the handling of SWN information by third parties must include a special clause, which allows SWN to audit the controls used for its information handling activities, and to specify the ways in which SWN information will be protected.

Once availability of the system is announced by the Occupational Health and Safety Manager, FTC staff may initiate access by entering their user ID (their FTC email address) and their non-public assigned Management Information Systems number (Misno) as their PIN.[2] The PIN is one-time use only. Once the user accesses the system, they are required to create a unique password that they will use login going forward.

Use of the FTC staff Misno for the one-time, initial PIN sufficiently reduces the risk of unauthorized access to an FTC staff's ENS account while significantly reducing the overhead in issuing the initial account access. The Misno is not externally discoverable, making unlawful access by non-FTC staff unlikely. The Misno is sufficiently complex that a brute force attack would not work.

The Misno is available within the FTC via the employee locator on FTC's intranet, and any FTC staff could improperly use the Misno of any other employee, creating the risk of employees accessing fellow employee accounts. However, since the Misno is used only for the initial login, the FTC staff personal CPs would not yet be in the system. The only personal information available in the account at initial login is the FTC CPs, which – except for FTC mobile device numbers – are readily available to all employees via the FTC Global Address List. By forcing users to create a permanent password once the valid user has entered their personal CP, the risk of FTC staff accessing a fellow employee's FTC ENS information is mitigated. Using the Misno as a one-time PIN significantly reduces the complexity of distributing access to the ENS accounts while maintaining adequate security.

A risk exists in the inadvertent exposure of or unauthorized access to PII, including name, work phone numbers, personal phone numbers and email addresses. To mitigate this risk in the Administration Portal, system administrator accounts: (1) can only be created upon approval of FTC ENS Master Administrator, (2) can only be created by the FTC ENS Master Administrator, and (3) can only be created for employees having an "ftc.gov" email address. System administrator accounts are granted to a limited number of approved staff; those individuals can only view the information needed to complete their role. Only system administrators can create an FTC user account. Additionally, password authentication is required to access the portal; the portal utilizes HTTPS, all data is encrypted in transit and at rest, and the portal has an automatic time out set at 15

[2] The SWN system is not able to generate random passwords and email them to FTC staff. Likewise, creating random passwords and emailing them to each individual would be time consuming and prone to human error. In any event, the privacy risk of using the non-public Misno as an initial PIN is low, because the information in the system at the time it is first used to access the account is limited to FTC CP, much of which is public elsewhere (e.g., names of FTC staff), and the user can change the non-public PIN to ensure greater security for any subsequently entered personal CP, as explained above.

minutes of inactivity. Requests to reset passwords require that the user answer a security question; reset passwords are sent to the user's ftc.gov email address.

To mitigate this risk of exposure of PII in the Self-Enrollment Portal, account holders can only view their own information. Password authentication is required to access the portal and passwords are required to follow FTC policy; the portal utilizes HTTPS; all data is encrypted in transit and at rest; and, the portal has an automatic time out at 15 minutes of inactivity.

The impact level of this data is low because the unauthorized disclosure, modification, and access, use or loss of confidentiality, availability, and integrity of the information would have limited adverse effects on the FTC and its employees and contractors.

The SWN system and network administrators are employed directly by SWN. SWN employees and subcontractors must execute both confidentiality/non-disclosure agreements and acknowledgements of familiarity/compliance with SWN information security policies. Third-party communications partners do not store or process customer data, and are not permitted to access customer data.

In using the system, the FTC maintains the minimum amount of information necessary for efficiently and effectively notifying its workforce. (For example, the system does not collect Sensitive PII such as Social Security numbers or financial account numbers.) Likewise, FTC staff are able to control and limit what personal CPs the system maintains. Further discussion of security measures is set forth in Section 5.5 of this document.

3 Use and Access to Data in the System

1. Describe how information in the system will or may be used.

CP information will be used to notify either all or a subset of FTC staff in emergencies. These situations may include office closures, natural disasters, major traffic disruptions, or other crises. Notification will consist of text and/or voice messages delivered to e-mail addresses and/or phones with notice of the incident. In some cases, the notification may also solicit a response from the recipient, such as confirming the FTC staff member's safety or the need for assistance. Login credentials and system logs and similar system data are collected or generated for security and audit purposes.

2. Which internal entities will have access to the information?

The authorized FTC ENS Master Administrator and system administrators will have access to maintain and administer the system. FTC staff with ENS system accounts will only have access to their personal CP information via the online web portal and will not be able to view any other FTC staff member data or change an FTC CP established by the FTC ENS Master Administrator or system administrator.

3. Which external entities will have access to the information?

External access to the FTC ENS data is limited to SWN authorized personnel. SWN system and network administrators are employed directly by SWN. SWN employees and third-party contractors must execute both confidentiality/non-disclosure agreements and acknowledgements of familiarity/compliance with SWN information security policies. Third-party communications partners do not store or process customer data and are not permitted to access customer data. The FTC ENS is not available to the public.

4 Notice and Access for Individuals

1. How will individuals be informed about what information is collected, and how this information is used and disclosed?

The FTC notifies its FTC staff of the purposes for which the data is collected and how the data may be used, including emergency notification, at the time of data collection and via periodic reminders to staff to review and update their personal CPs. All users, both FTC system administrators and FTC staff who use the FTC ENS, can view, print and retain both the FTC Privacy Act Statement and the SWN privacy policy via separate web-links available at the bottom of each page of the SWN user interface for FTC users.

2. Do individuals have the opportunity and/or right to decline to provide information?

FTC staff do not have the opportunity to decline to provide their FTC CPs, which are automatically entered for all FTC staff into ENS. This includes the user's name, whether the user is a government or contractor employee, office location, organization code, FTC email address, office phone number, and FTC-issued mobile device number.

FTC staff do have the right and opportunity to decline to provide personal CPs, which may include their personal email address, home phone number, and mobile personal devices. Personal CPs will be included only if FTC staff voluntarily provide this information via the self-enrollment portal. This portal will allow FTC staff to delete their personal CPs at any time if they do not want to be notified through the system at their personal CPs and/or do not want their personal CPs maintained in the system.

Login credentials are required for FTC ENS system administrators and FTC staff to ensure secure system administration and self-enrollment activities. FTC staff are not required to respond to alerts, and not all alerts will have the option to respond. FTC staff cannot opt-out of Alert Tracer if that feature is used by the Master Administrator to determine whether a notification has been successfully delivered to the user. Likewise, individuals are not able to opt-out of system access logs or any other automated data that may be generated by the system about their system access, such as notifications sent and responses received from recipients, discussed in Section 2.1 above.

3. Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals do not have the right to consent to only particular uses of the information. FTC CPs pertaining to FTC staff are entered into the system by an FTC ENS system administrator for the purpose of emergency notifications.

FTC staff consent to the use of personal CPs for the purpose of emergency notification by voluntarily entering the information into the FTC ENS. The personal CP can be changed or deleted at any time by the user. FTC and personal CPs are used only for the purpose of emergency notifications by the FTC. Login credentials are not voluntary for the FTC ENS system administrator or FTC staff who wish to access the system, and there is no procedure for obtaining the individual's consent for the use of such data for this purpose. Likewise, FTC staff do not have any consent rights as to the use, if any, of Alert Tracer or the collection of any system log or other automated system data about their access to the system.

4. What are the procedures that allow individuals to gain access to their own information?

FTC staff will use the FTC ENS self-enrollment portal to access the system. In this portal, they may view their FTC CPs and view, edit, or delete their personal CPs and change their login password and associated password reset security question. If a user forgets his or her login password, they may click on the "Forgot your password?" link at the self-enrollment portal to generate a new password. FTC staff may delete his or her personal CPs but not their FTC CPs.

5. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The FTC ENS requires unique user IDs and passwords to access, modify and/or delete personal CPs. System administrative and user password requirements will follow the FTC approved policy to ensure: (1) minimum length, (2) complexity, (3) expiration, and (4) prevent reuse. Auto-lockout will be enabled after five (5) of invalid login attempts. When a user forgets their password, they will click on the "Forgot your password?" link at the self-enrollment portal, which will send an email to the user's FTC.gov email address. The email will contain a URL that will allow the reset of the user's password. The FTC ENS Master Administrator will require the user set up and use a security question during the password reset process.

The FTC ENS Master Administrator, or his designee, are the only authorized users who may change an FTC CP. Per FTC policy, employees and contractors may not share user IDs or passwords for any FTC system or application with anyone.

The SWN system maintains a fully implemented program of continuous monitoring on specific parameters including all administrator activity, data access, data deletions, data changes, and permission changes. If this monitoring detects any suspicious activity, an

alert is generated and forwarded to the SWN Network Operations Center (NOC) for review. The NOC is staffed 24/7.

5 Web Site Privacy Issues

1. Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).

The SWN system uses a temporary session ID cookie on the system administration and self-enrollment portals.

2. If a persistent tracking technology is used, ensure that the proper issues are addressed.

Not applicable. In accordance with FTC policy, persistent tracking technology is not used by ENS.

3. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

The SWN system uses HTTPS to provide authentication of the website, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. Additionally, the SWN system uses 128-bit Secure Sockets Layer (SSL) encryption.

4. Explain how the public will be notified of the Privacy Policy.

Not applicable. ENS is does not contain personal information from the general public; it houses FTC staff data and is only accessible to FTC employees and contractors.

5. Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

Users may access FTC ENS by logging into the system via the internet. See Section 2.8 above for discussion of privacy risks and mitigations.

6. **If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).**

Not applicable.

6 Security of Information in the System

1. Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

Yes. The FTC follows all applicable Federal Information Security Modernization Act (FISMA) requirements, ensuring the data are appropriately secured by the third-party service on the FTC's behalf. The data are categorized as low using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

2. Has an Assessment and Authorization been completed for the system or systems supporting the program?

Yes. SWN has received an Authority to Operate (ATO) from the US Army following an Information Assurance Assessment and Authorization conducted in June 2014. FTC's Office of the Chief Information Officer (OCIO) has reviewed the information provided by the US Army and will be issuing an Authority to Operate prior to allowing the entry of personal CPs.

3. Has a risk assessment been conducted on the system?

Yes. The OCIO has reviewed the information provided by the US Army and finds the risk assessment acceptable.

4. Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

Yes. The FTC has addressed risks and vulnerabilities as described elsewhere in this document. See, e.g., Section 2.8.

5. What procedures are in place to determine which users may access the system and are they documented?

System administrator access to the FTC ENS is limited to a small number of users both at the FTC and at SWN. Other FTC staff can only access their own accounts, which may contain their personal CPs, and cannot see any other user information. All FTC IT-related policy and procedures are documented. SWN staff are required to sign a confidentiality agreement and ethics agreement upon hire. The SWN system and network administrators are employed directly by SWN. SWN employees and third-party contractors must execute both confidentiality/non-disclosure agreements and acknowledgements of familiarity/compliance with SWN information security policies. Third-party communications partners do not store or process customer data, and are not permitted to access customer data. See also Section 5.5 above.

6. Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff are required to complete information security and privacy awareness training annually. Interactive online training covers topics such as how to handle sensitive PII and other data, online threats, social engineering, and the physical security of documents.

As part of the requirements for an SSAE16 Type II audit, SWN adopted a policy requiring all SWN employees to certify at least annually that they have received and read a copy of the SWN Information Security Policy (ISP) and will comply with all requirements in the ISP that are applicable to their job functions. New SWN employees receive a copy of the ISP upon commencement of their employment and are required to provide the certification at that time. SWN has certifications in place from all current employees. The ISP covers a broad range of privacy and security topics. Additionally, SWN employees receive additional specialized, in-depth training relative to their job responsibilities.

Outside consultants, contractors, and temporary employees of SWN are subject to the same information security requirements, and have the same information security responsibilities, as SWN employees. All agreements dealing with the handling of SWN information by third parties include a special clause. This clause allows SWN to audit the controls used for these information-handling activities, and to specify the ways in which SWN information will be protected.

7. What auditing measures and technical safeguards are in place to prevent the misuse of data?

SWN maintains a fully implemented program of continuous monitoring on specific parameters including all administrator activity, data access, data deletions, data changes, and permission changes. If this monitoring detects any suspicious activity, an alert is generated and forwarded to the SWN Network Operations Center (NOC) for review. The NOC is staffed 24/7.

The FTC ENS Master System Administrator will have the ability to create, modify, and delete FTC and user provided CPs and user IDs, as well as configure the system and send notifications. Designated FTC system administrators will be granted the appropriate permission by the FTC ENS Master Administrator within the FTC ENS and may have the ability to create, modify, and delete FTC user IDs, as well as FTC CPs and user provided CPs; the Master Administrator also has the ability to send notifications. The FTC ENS Master Administrator can tailor the system administrator permissions to meet the need. Only the FTC ENS Master Administrator and designated system administrators can create an FTC user ID in the FTC ENS.

After the initial import of FTC data, the Master Administrator will: (1) create FTC staff one-time use user IDs (their FTC.gov email account), and (2) assign their corresponding Misno as their PIN. Upon the user's successful initial log in (via the FTC.gov/PIN combination), they will be prompted to create a unique user ID and password.

Password requirements will follow the FTC approved policy to ensure: (1) minimum length, (2) complexity, (3) expiration, and (4) prevent reuse. Auto-lockout will be enabled after five (5) of invalid login attempts. When a user forgets their password, they will click on the "Forgot your password?" link, which will send an email to the user's FTC.gov email address. The email will contain a URL that will allow the reset of the user's password. The FTC ENS Master Administrator can require the user set up and use a security question during the password reset process.

The FTC ENS Master Administrator will announce to Agency personnel via the FTC Daily that this service is available and provide the link to access the site. The user will access the FTC ENS by using their FTC email address as their user ID and MIS number as the PIN. Upon the initial successfully login, the user will be prompted to enter a unique user ID and select a password.

8. To whom should questions regarding the security of the system be addressed?

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7 Data Retention

1. For what period of time will data collected by this system be maintained?

The SWN system performs a daily differential backup to save changes made to the data in the FTC account, with full backups performed weekly. Daily backups are maintained for 30 days and weekly backups are maintained for 52 weeks. The data collected by the SWN system for current and new FTC staff, will be maintained until superseded by current information. When an FTC CP is deleted by the FTC system administrator, the information is immediately removed from the FTC account on the SWN system. When an FTC user ID is deleted, the corresponding FTC CP(s), as well as, the associated personal account and CPs are immediately deleted. The FTC will dispose of all system data for former FTC staff and contractors, as well as other information collected, in accordance with approved retention schedules.

2. What are the plans for destruction or disposal of the information?

All data will be deleted/destroyed in accordance with Office of Management and Budget (OMB), National Archives and Records Administration (NARA), and National Institute of Standards and Technology (NIST) regulations and guidance.

3. Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

When FTC staff leave the agency, their accounts along with the corresponding personal accounts are deleted from the ENS via the secure SWN administration portal. The SWN

system performs a daily differential backup to save changes made to the data in the FTC account, with full backups performed weekly. Daily backups are maintained for 30 days and weekly backups are maintained for 52 weeks. The data collected by the SWN system for current and new FTC staff will be maintained until superseded by current information. When a user ID and/or CP is deleted, information is immediately removed from the FTC account on the SWN server. The FTC will dispose of printouts and electronic information collected in accordance with approved FTC retention schedules.

Encrypting data at rest is a security measure that is commonly used to protect files from being accessed, stolen or altered by an unauthorized party while they are being stored on disk (at rest). It protects data when unauthorized parties gain access to it through means other than over the network. Lost backup media, stolen database files, and discarded hardware have all led to high-profile data breaches. SWN provides full database encryption to its clients.

8 Privacy Act

1. Will the data in the system be retrieved by a personal identifier?

Contact data may be retrieved by individual name, email, or phone number.

2. Is the system covered by an existing Privacy Act System of Records notice (SORN)?

To the extent that the FTC ENS constitutes the maintenance of a system of records under the Privacy Act, the relevant SORN would be Computer Systems User Identification and Access Records (FTC-VII-3) and Unofficial Personnel Records (FTC-II-2) data.

All of the FTC's SORNs are listed and can be downloaded from our public SORN page: http://www.ftc.gov/foia/listofpaysystems.shtm.

9 Privacy Policy

1. Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of the FTC and personal CPs, user ID credentials, password reset security question, system access logs, SWN Alert Tracer and Get Word Back features, as described above is consistent with the FTC's privacy policy.

10 Approval and Signature Page

System Owner:

_____ Date: _____
Russ Roeller
Occupational Health and Safety Manager

Reviewed By:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Katherine Race Brin
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date: _____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____

Raghav Vajjhala
Chief Information Officer