Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-003
Revision Number: 00.1
Issue Date: 03/30/2016
Incorporating Change 1, 12/14/2018
Approved by Philip S. Kaplan, Chief Privacy Officer

PRIVACY POLICY FOR DHS MOBILE APPLICATIONS

I. Purpose

This Instruction implements the Department of Homeland Security (DHS or the Department) Directive 047-01, "Privacy Policy and Compliance," concerning DHS mobile applications intended for use by DHS employees and/or the public.

II. Scope

This Instruction applies throughout DHS for mobile applications that are developed by, on behalf of, or in coordination with the Department.

III. References

A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 United States Code (U.S.C.) § 3501 note]

B. Title 5, U.S.C., Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]

C. Title 6, U.S.C., Section 142, "Privacy Officer"

D. Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014 (FISMA)]

E. Title 15 U.S.C., Chapter 91, "Children's Online Privacy Protection Act"

F. Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information"

G. DHS Directive 047-01, "Privacy Policy and Compliance"

H. DHS Sensitive Systems Policy Directive 4300A

I. DHS Instruction 047-01-007, "Handbook for Safeguarding Sensitive Personally Identifiable Information"

J. Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including:

1. Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments (December 30, 2008)

2. Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (December 29, 2008)

~~3. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (March 2012)~~

IV. Definitions

A. ***AppVet*™ ~~DHS Carwash~~** is the service sponsored by DHS Office of the Chief Information Officer (OCIO), which provides development teams with a continuous integration, build, test, source code management, and issue tracking environment for building DHS mobile apps. The shared platform provides application lifecycle management and support for mobile apps built on development frameworks. The *AppVet*™ ~~DHS Carwash~~ also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility.

B. ***DHS Mobile Application (DHS Mobile App)*** means a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or tablet) by DHS employees and/or the public.

C. ***Fair Information Practice Principles*** means the policy framework adopted by the Department in Directive 047-01, Privacy Policy and Compliance, regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information.

D. ***Location Information*** means the ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.

E. ***Metadata*** means the information stored as the description of a unique piece of data and all the properties associated with it. For example, mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

F. ***Mobile Device ID*** means a unique serial number that is specific to a mobile device. These numbers vary in permanence, but typically a device has at least one permanent number. These numbers are used for various purposes, such as for security and fraud detection and remembering user preferences. Combining a unique device identifier with other information, such as location data, can allow the phone to be used as a tracking device.

G. ***Personally Identifiable Information (PII)*** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information may include a name, Social Security number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, biometric identifier (e.g., facial recognition, photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

H. ***Privacy Compliance Documentation*** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

I. ***Privacy Compliance Review (PCR)*** means both the DHS Privacy Office process to be followed and the document designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing Privacy Compliance Documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

J. ***Privacy Impact Assessment (PIA)*** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information are used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long it is retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may, in coordination with the affected Component and the Office of the General Counsel, modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

K. ***Privacy Threshold Analysis (PTA)*** means both the DHS Privacy Office process to be followed and the document used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the proposed use, identifies the legal authorities for the proposed use, and describes what PII, if any, is collected (and from whom) and how that information is used. PTAs are adjudicated by the Chief Privacy Officer.

L. ***Program Manager*** means the responsible agency representative, who, with significant discretionary authority, is uniquely empowered to make final scope-of-work, capital investment, and performance acceptability decisions.

M. ***Sensitive Content*** means information that may not be PII, but raises privacy concerns because it may be related to the use of PII (e.g., location information, mobile device ID, or metadata).

N. ***Sensitive Personally Identifiable Information (SPII)*** means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are SPII if DHS maintains them in conjunction with other identifying information about the individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be SPII, but could be if it is a list of employees who received poor performance ratings.

O. ***System Manager*** means the individual identified in a System of Records Notice who is responsible for the operation and management of the system of records to which the System of Records Notice pertains.

P. ***System of Records Notice (SORN)*** means the statement providing the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system are included.

Q. ***User*** means a person using a DHS mobile app.

V. Responsibilities

A. The ***Chief Privacy Officer*** is responsible for:

1. Working with Component Privacy Officers and Privacy Points of Contact (PPOCs) to provide guidance and ensure that DHS mobile apps are in compliance with DHS privacy policies;

2. Reviewing and approving Privacy Compliance Documentation for DHS mobile apps, as appropriate; and

3. Performing periodic PCRs of DHS mobile apps to ascertain compliance with DHS privacy policy.

B. The ***Chief Information Officer*** is responsible for:

1. Providing web technology services, security, and technical assistance for the development of DHS mobile apps;

2. Ensuring that DHS mobile apps comply with FISMA and DHS Sensitive Systems Policy Directive 4300A; and

3. Performing iterative scans and tests on the source code of DHS mobile apps through the *AppVet*™ ~~DHS Carwash~~ process in order to provide insight on code security, quality, and accessibility.

C. ***Component Privacy Officers*** are responsible for:

1. Coordinating with Program Managers or System Managers, as appropriate, together with the Chief Privacy Officer and counsel to complete Privacy Compliance Documentation, as necessary, for all proposed DHS mobile apps; and

2. Collaborating with the Chief Privacy Officer in conducting Privacy Compliance Reviews.

D. ***Privacy Points of Contact (PPOCs)*** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

E. ***Program Managers, or System Managers***, as appropriate, are responsible for:

1. Coordinating with the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any DHS mobile apps;

2. Engaging and coordinating with the OCIO Carwash team to ensure that DHS mobile apps are sent through *AppVet*™ ~~DHS Carwash~~ process when proposing, developing, implementing or changing any DHS mobile apps;

3. Coordinating with the Component Privacy Officer or PPOC and counsel to prepare drafts of all Privacy Compliance Documentation, as necessary, when proposing, developing, implementing, or changing any DHS mobile apps;

4. Monitoring the design, deployment, operation, and retirement of DHS mobile apps to ensure that the collection and use of PII and sensitive content, if any, is limited to what is described in the Privacy Compliance Documentation; and

5. Coordinating with the Component Privacy Officer or PPOC and the DHS Office for Civil Rights and Civil Liberties to establish administrative, technical, and physical controls for storing and safeguarding PII and sensitive content consistent with DHS privacy, security, and records management requirements to ensure the protection of PII and sensitive content from unauthorized access, disclosure, or destruction as it relates to DHS mobile apps.

VI. Content and Procedures

A. ***Minimum Privacy Requirements for DHS Mobile Apps***: The policies detailed below provide the baseline privacy requirements for DHS mobile apps. Additional privacy protections may be necessary depending on the purpose and capabilities of each individual mobile app.

1. Provide Notice

a. App-Specific Privacy Policy (see Appendix A): DHS mobile apps have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy.

The Privacy Policy should briefly describe the app's information practices to include the collection, use, sharing, disclosure, and retention of PII, SPII, and sensitive content. The Privacy Policy should also address: redress procedures, app security, and the Children's Online Privacy Protection Act (if applicable).

b. Privacy Statement: If a DHS mobile app is collecting PII from users, then a Privacy Statement is provided at the point of collection. This Privacy Statement may be provided through a pop-up notification on the DHS mobile app screens where PII is collected or via another mechanism approved by the Chief Privacy Officer.

c. Contextual Notice: DHS mobile apps deliver direct, contextual, self-contained notice about the uses of information through the mobile platform. Therefore, these notices should be:

(1) Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;

(2) Provided as "just-in-time" disclosures and obtain users' affirmative express consent before a DHS mobile app accesses sensitive content or other tools and applications on the mobile device for the first time (e.g., location services); and

(3) Provided with independent opt-out features so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.

2. Limit the Collection and/or Use of Sensitive Content

a. DHS mobile app features cannot collect and/or use PII, SPII, or sensitive content, unless directly needed to achieve a DHS mission purpose; and

b. If the collection and/or use of PII, SPII, or sensitive content is directly necessary to achieve a DHS mission purpose, then the collection and/or use of the information is documented and justified in the mobile app's Privacy Compliance Documentation.

3. Establish Guidelines for User Submitted Information

a. Where feasible, use forms and check boxes to limit data collection and minimize data entry errors;

b. Before allowing a user to submit information to DHS, provide a "review before sending" function that allows users to correct or opt-out of sending their information to the Department; and

c. Unless necessary to achieve a DHS mission purpose, limit the ability of users to post information within the app that other users may access or view. This limits the potential for users to share PII, SPII, or sensitive content unnecessarily.

4. Ensure Mobile App Security and Privacy

a. Engage with the *AppVet*™ ~~DHS Carwash~~ throughout development to ensure the security and privacy of the mobile app;

b. If users submit information through a DHS mobile app, that information is encrypted in transit and immediately transferred to a protected internal DHS system that is compliant with existing DHS IT security policy;

c. Sensitive content that a DHS mobile app accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This information should not be transmitted to or shared with DHS.

B. ***DHS Mobile App Development***:

1. Program Managers and System Managers notify their Component Privacy Officers or PPOCs and the OCIO Carwash team before engaging in the development of a DHS mobile app.

2. Component Privacy Officers or PPOCs engage with Program Managers and System Managers to ensure privacy protections outlined in Section IV. A. of this document are integrated into the development of the DHS mobile app.

3. Before deployment, the DHS mobile app goes through the *AppVet*™ ~~DHS Carwash~~.

4. The OCIO Carwash team provides the iterative scan results of the *AppVet*™ ~~DHS Carwash~~ to the Program Managers and System Managers.

5. Before deployment, Program Managers and System Managers in consultation with Component Privacy Officers or PPOCs complete a PTA, an App-Specific Privacy Policy, and a Privacy Statement (if necessary) for the DHS mobile app. The PTA documents a general description of the proposed use, identify the legal authorities for the proposed use, and describe what PII, if any is collected (and from whom) and how that information is used. Component Privacy Officers or PPOCs compare this PTA to the *AppVet*™ ~~DHS Carwash~~ iterative scan results to ensure the PTA accurately describes the DHS mobile app's collection, use, maintenance, retention, disclosure, deletion and destruction of PII, SPII, and sensitive content.

6. Before deployment, the DHS mobile app's PTA, App-Specific Privacy Policy, Privacy Statement (if necessary), and results of the *AppVet*™ ~~DHS Carwash~~ iterative scans are submitted to the Chief Privacy Officer for a prompt review and evaluation to determine whether the DHS mobile app contains appropriate privacy protections and whether a new or updated PIA, SORN, or other Privacy Compliance Documentation is required.

7. Once it is determined that all necessary Privacy Compliance Documentation is complete and that the DHS mobile app contains appropriate privacy protections , the Chief Privacy Officer provides approval for the release of the DHS mobile app.

8. DHS mobile apps go through the *AppVet*™ ~~DHS Carwash~~ any time there is a change made to the DHS mobile app that affects or potentially affects the collection and use of PII, SPII, or sensitive content and consistent with the PTA review cycle. Existing DHS mobile apps, which were developed before the implementation of this policy, go through the *AppVet*™ ~~DHS Carwash~~ within 6 months of this policy's issue date. Program Managers and System Managers provide the *AppVet*™ ~~DHS Carwash~~ results, pertaining to their particular DHS mobile app, to the Chief Privacy Officer for a prompt review and evaluation to ensure that the DHS mobile app continues to contain appropriate privacy protections.

C. ***Retention of PII***: Component Program Managers or System Managers, where appropriate, maintain PII collected through DHS mobile apps in accordance with approved records retention schedules.

D. ***Privacy Compliance Reviews (PCR)***: The Chief Privacy Officer, in collaboration with Component Privacy Officers or PPOCs, may conduct PCRs of DHS mobile apps periodically, at the sole discretion of the Chief Privacy Officer, to ascertain compliance with DHS privacy policy.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.

Karen L. Neuman
Chief Privacy Officer

March 30, 2016
Date

Privacy Policy
For the
[INSERT NAME] Mobile Application

Overview
The overview should be a single paragraph that is used to describe the DHS mobile application ("mobile app"). It should include the name of the DHS component that developed the app as well as the name of the DHS mobile app, itself. This overview should also provide a brief description of the DHS mobile app's purpose and function.

Information Collected
Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and sensitive content that is collected by the DHS mobile app. Details regarding the retention of information collected by the DHS mobile app should also be addressed in this section.

Uses of Information
List each use (internal and external to the Department) of the information collected or maintained by the DHS mobile app. Provide a detailed response that states how and why the different data elements is used.

Information Sharing
Discuss the external Departmental sharing of information (e.g., DHS to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security
Discuss the technical safeguards and security controls, specific to the particular DHS mobile app, in place to protect information that is collected and/or maintained by the DHS mobile app.

How to Access or Correct your Information
Provide information about the processes in place for users of the DHS mobile app to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

Analytics Tools
Discuss any analytics tools that the DHS mobile app may use. This should include a description of any information collected through these analytic capabilities.

Privacy Policy Contact Information
Provide component privacy office contact information so that users may provide feedback and/or ask questions in regards to this DHS mobile app Privacy Policy. This contact information may include the component privacy office's phone number, email, and mailing address.