Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, technologies, rulemakings, programs, information sharing arrangement, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If a compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office will send you a copy of the relevant compliance template to complete and return.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application:	**Hotel Hijinks Mobile Gaming Application**		
DHS Component:	**Cybersecurity and Infrastructure Security Agency (CISA)**	Office or Program:	**Cybersecurity Division/ Cyber Defense Education and Training**
Launch date:	**September 25, 2021**	Project or program status:	Choose an item.
Date of last PTA (if applicable):	**Click here to enter a date.**		

MOBILE APP DEVELOPMENT PROGRAM MANAGER/BUSINESS OWNER

Name:	**Latasha McCord**		
Office:	Cyber Defense Education and Training (CDET)	Title:	Education Section Chief
Phone:	202-853-4799	Email:	Latasha.McCord@cisa.dhs.gov

MOBILE APP DEVELOPMENT LEAD/INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	**Matthew Shadwick**		
Office:	CISA/OCISO	Title:	PTS Contracor
Phone:	318-751-9071	Email:	Matthew.shadwick@associates.cisa.gov

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

Describe the DHS mobile application[1]. *Please provide a general description of the mobile app and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal PTA, please state whether or not there were any changes to the mobile app since the last version.*

Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Defense Education & Training Sub-Division (CDET) is conducting this Privacy Threshold Analysis (PTA) for the Hotel Hijinks mobile application.

CDET has partnered with Pacific Northwest National Laboratory (PNNL) to develop a mobile game called Hotel Hijinks focused on providing cybersecurity content for next generation cybersecurity workforce youth. The application is designed to run on iPhone and Android smartphones and will be available via the Apple AppStore and Google Play store for free. The application has a primary audience of high school level students and while this is our intended audience, the application will be publicly available for anyone to download and use. The application is designed to deliver learning material on cybersecurity topics related to Internet of Things and cyber career pathways in a fun and interactive way.

The application will run locally on the user's smartphone. It does not require the user to log in to an account for use and does not collect data on its users.

2. Subjects and Users[2] of the Mobile Application Information

a. Who will SUBMIT information into this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☐ Members of the public ☐ DHS personnel ☐ Other federal employees
Not Applicable. No information is collected from users of the application or players during the game.	
b. Who will USE the information submitted to DHS from this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☐ Members of the public ☐ DHS personnel ☐ Other federal employees
Not Applicable. No information is collected from users of the application or players during the game.	

[1] DHS defines DHS Mobile Application (DHS Mobile App) as 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 table) by DHS employees and/or the public. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

[2] User means a DHS person using a DHS Mobile App.

3) Data to be collected	
a) What information will be submitted through the mobile application? *Please list all data elements.*	
Not Applicable. No information will be submitted through the mobile application. The mobile application is a game intended to deliver learning materials on cybersecurity topics.	
b) Does the mobile application collect Sensitive Personally Identifiable Information (SPII)?[3] Check all that apply.	☐ Social Security number ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☐ Passport Number ☐ Bank Account, Credit Card, or other financial account number ☐ DHS Electronic Data Interchange Personal Identifier (EDIPI) ☐ Social Media Handle/ID ☐ Known Traveler Number/Other Traveler ID Number ☐ Driver's License Number ☐ Biometrics (e.g., fingerprints, facial images/photographs) ☐ Other. Please list:
c) List the *specific authority* to collect SSN or these other SPII elements. *Note*: even if the program is properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking/truncating the SSN, or blocking the display of SSNs within the mobile application.[4]	
Not applicable.	
d) Describe *why* this collection of SPII is necessary and the minimum amount of information required to accomplish the purpose of the program.	
Not applicable.	

[3] DHS defines Sensitive Personally Identifiable Information (SPII) as 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.
[4] Please see DHS Instruction Number: 047-01-009 (Social Security Number Collection and Use Reduction).

e) Does the mobile application collect other types of sensitive content information?[5] Check all that apply.	☐ Location Information[6] ☐ Photos/Videos[7] ☐ Mobile Device ID ☐ Metadata[8] ☐ Other. Please list:
f) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	
Not Applicable. No sensitive content is collected by this app.	
g) How and where is the information stored? *Please describe below.*	☒ Locally on the mobile device ☐ In a back-end DHS system _____ ☐ With a third-party vendor ☐ Other. Describe_____
Information on game state is stored locally on the mobile device so the game can so the player can later return to the where they left off.	
h) How long is information stored or retained? If the data is stored in multiple places, please provide the information for all locations. *Please describe below and indicate retention schedules if applicable.*	
Game state information is stored until the app is deleted.	
i) How do you ensure that information is disposed of or deleted in accordance with the retention schedule?	
App related data is deleted by the operating system when the game is removed by the user.	
j) Does the project, program, or system retrieve information by personal identifier?	☐ Yes. Please list personal identifiers below. ☒ No.

4. Notices

a) Are individuals provided a Privacy Act Statement, Privacy Notice, or some, other type of notice[9] at the time of collection by	☐ Yes. Please describe. ☒ No.

[5] 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).

[6] 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.

[7] Photos/videos meaning the mobile app access the device's camera or photo library.

[8] 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.

[9] Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app.

DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	

5. Disclosures

a) Does the mobile application provide "just-in-time"[10] disclosures to obtain user's 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)?	☐ Yes. Please describe. ☒ No.
No privacy sensitive services or content is accessed by the app.	
b) Does the mobile application provide any information to other DHS Components or systems?	☐ Yes. Please describe. ☒ No.
c) Does the mobile application provide any information to third parties (any organization outside of DHS)?	☐ Yes. Please describe. ☒ No.

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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?	☐ Yes. Please describe. ☒ No.
No privacy sensitive services or content is accessed by the app.	
b) Before allowing a user to submit information to DHS, does the mobile application provide a "review before sending" function that allows users to correct or opt-out of sending their information to the Department?	☐ Yes. Please describe. ☒ No.
No information is submitted via the app.	

7. Mobile App-Specific Privacy Policy

[10] DHS mobile apps are to be developed so as to 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).

[11] DHS Mobile apps are to provide users 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.

a) Does the mobile application have an App-Specific Privacy Policy[12] that is available to users through the commercial app store as well as within the app? If yes, please include a copy of the App-Specific Privacy Policy with this PTA upon submission.	☒ Yes. Please describe. ☐ No.
Once approved, the Privacy Policy can be found here: Cyber Games Privacy Policy | CISA	

8. DHS AppVet process?	
a) Has this mobile application been through the DHS AppVet[13] process?	☐ Yes. **Please provide the results of the AppVet with this PTA.** ☒ No.
AppVet scan results are attached.	

PRIVACY THRESHOLD REVIEW
(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Shannon Riley
Date submitted to Component Privacy Office:	**September 15, 2021**
Date submitted to DHS Privacy Office:	September 17, 2021
Concurrence from other Components involved (if applicable):	Click here to enter text.
Component Privacy Office Recommendation: *Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.*	
The CISA Office of the Chief Privacy Officer recommends the Hotel Hijinks Mobile Application is not privacy sensitive. The Hotel Hijinks mobile application game provides cybersecurity learning material tailored to high school students in a game environment, however, the application will be available to all members of the public via the Apple AppStore and Google Play store for free.	

[12] All DHS Mobile apps are required to 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. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

[13] DHS AppVet is the service sponsored by DHS Office of the Chief Technology Officer (OCTO) that 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 DHS AppVet also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility. DHS AppVet replaced the DHS Carwash. This is a requirement of DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

There is no collection of PII or sensitive information by CISA or the application developer Pacific Northwest National Laboratory. The game is downloaded and stored locally on the user's phone from the respective app stores and does not require a username or password for use.

The Privacy Policy is provided below and will be made available to users. Additionally, the application has completed the DHS AppVet process and has been determined to be low risk.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Kattina Do**
DHS Privacy Office Approver (if applicable):	Riley Dean
PCTS Workflow Number:	**0020183**
Date approved by DHS Privacy Office:	September 17, 2021
PTA Expiration Date	September 17, 2024

DESIGNATION

Privacy Sensitive Application?	**No If "no" PTA adjudication is complete.**
Determination:	☒ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement/Privacy Notice required. ☐ Privacy Policy required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
e(3)/ Privacy Notice	Choose an item.
Privacy Policy	Choose an item.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	
CISA is submitting this PTA to discuss the Hotel Hijinks Mobile Gaming Application. Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Defense Education & Training Sub-Division (CDET) has partnered with Pacific Northwest National Laboratory (PNNL) to develop a mobile game called Hotel Hijinks focused on providing cybersecurity content for next generation cybersecurity workforce youth. The application	

is designed to run on iPhone and Android smartphones and will be available via the Apple AppStore and Google Play store for free. The application has a primary audience of high school level students and while this is our intended audience, the application will be publicly available for anyone to download and use. The application is designed to deliver learning material on cybersecurity topics related to Internet of Things and cyber career pathways in a fun and interactive way.

The mobile application does not access sensitive content or other tools and applications on mobile devices, and does not collect sensitive content, generate, or retain individual information. A privacy policy is available through the mobile application informing the user of this.

The DHS Privacy Office (PRIV) agrees with CISA Privacy that the Hotel Hijinks Mobile Gaming Application is non-privacy sensitive. No PIA or SORN coverage is required.

Privacy Policy
For the
Defend the Crown, Network Collapse, and Hotel Hijinks Mobile Applications

Overview

Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Defense Education & Training Sub-Division (CDET) has partnered with Pacific Northwest National Laboratory (PNNL) to develop three mobile games: Defend the Crown focused on providing cybersecurity educational content for CISA and other federal employees or individuals new to cybersecurity concepts; Network Collapse focused on providing cybersecurity content to middle school students or individuals new to cybersecurity concepts; and Hotel Hijinks focused on providing content to high school students related to the Internet of Things and cyber career pathways. The applications are designed to deliver learning material on cybersecurity topics such as cyber-attacks and defenses, internet of things security, computer networking, and cyber safety in a fun and interactive way.

Information Collected

No information is collected from users of the Defend the Crown, Network Collapse, or Hotel Hijinks mobile applications and retained by CISA or PNNL.

Uses of Information

No information is collected or retained from users of the Defend the Crown, Network Collapse, or Hotel Hijinks mobile applications and used by CISA or PNNL.

Information Sharing

No information is collected from users of the Defend the Crown, Network Collapse, or Hotel Hijinks mobile applications and shared by CISA or PNNL with other federal, state, and local governments or private sector entities.

Application Security

The Defend the Crown, Network Collapse, or Hotel Hijinks mobile applications were scanned for vulnerabilities and malware using DHS AppVet which combines multiple commercial and open source scanners provide enhanced vulnerability and malware detection coverage.

How to Access or Correct your Information

No information is collected from users of the Defend the Crown, Network Collapse, or Hotel Hijinks mobile applications to provide access to or correction of information.

Analytics Tools

The mobile platforms offer App Analytics which provides data on aggregate user engagement with metrics such as App Store Impressions, Product Page Views, Sessions, Deletions, and more. To protect user privacy, it only shows data in App Analytics after a certain number of data points are available. This data is not linked to a user.

Privacy Policy Contact Information

For more information please reach out to the CISA Privacy Office at privacy@cisa.dhs.gov.