US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

April 12, 2019

OPDIV:

OS

Name:

SynAck

TPWA Unique Identifier:

T-6821486-576574

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

No

If SORN is not yet published, identify plans to put one in place.

Not Applicable

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 1/1/01 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: Not Applicable

Does the third-party Website or application contain Federal Records?

No

Describe the specific purpose for the OPDIV use of the third-party Website or application:

Synack provides crowd sourced proactive application security penetration testing from an adversarial perspective. The service can assess vulnerabilities within web and mobile applications, host infrastructure and networks, and connected IoT devices. The Synack portal serves as a single location to control assessment traffic, manage cybersecurity assessment activities, and report and remediate findings.

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

The public does not access this website.

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

No

How does the public navigate to the third party Website or application from the OPIDIV?

The public does not access this website.

Please describe how the public navigate to the thirdparty website or application:

Synack solution uses role based access control (RBAC) to limit access to HHS content per assessment. The public does not have access to HHS information. Additionally, only designated persons from each operating divisions (OpDiv) have access to their penetration testing results.

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to anongovernmental Website?

No

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

No

Provide a hyperlink to the OPDIV Privacy Policy:

Not applicable

Is an OPDIV Privacy Notice posted on the third-part website or application?

No

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

Synack is a service to provide management, assessment, and closure of IT cybersecurity vulnerabilities. While infrequent, it is possible the submissions received by the third-party, which will be provided to OPDIV, may contain personally identifiable Information (PII). It is not the intent of the third-party to process any specific sensitive PII as any collection of PII is incidental to the management of the assessments. In these infrequent cases PII can include user account names, real names, and in some cases images of exposed PII in assessed systems which could include PII such as Social Security numbers (SSN), clearance status, etc. PII is only shared through the Synack portal, is protected in transit using Transport Layer Security (TLS) 1.2 and leverages advanced encryption standard (AES) 256 bit encryption at rest.

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

All content is provided to Office of the Chief Information Officer (OCIO) and the designated Operating Division (OpDiv) management and staff on a per assessment basis via the Synack portal. Access to this information is secured using RBAC and 2-factor authentication for all accounts.

If PII is shared, how are the risks of sharing PII mitigated?

Content on the portal is protected by RBAC and 2-factor authentication, limited to specific

Will the PII from the third-party website or application be maintained by the OPDIV?

No

Describe how PII that is used or maintained will be secured:

Any collection of PII, while infrequent, will be secured by encrypting data in transit using TLS 1.2, encrypting data at rest using AES256, and restricting access to authorized users via RBAC configuration and mandatory 2-factor authentication.

What other privacy risks exist and how will they be mitigated?

Not applicable