

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

January 23, 2026

OPDIV:

IHS

Name:

IHS Service Now

TPWA Unique Identifier:

T-4004039-001509

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.

null

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: null

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

Yes

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

ServiceNow GCC (Government Community Cloud) is a government-authorized version of the ServiceNow platform. It is used to support and manage internal IHS business processes such as ticketing, workflows, customer surveys, and service requests. The system is hosted in U.S.-based data centers and operates in accordance with applicable IHS and federal security and privacy requirements. Access is limited to authorized users, and administrative, technical and physical safeguards are implemented to protect IHS information. ServiceNow GCC supports IHS operations and does not alter the types of information collected; it provides a secure environment for processing information consistent with IHS policies.

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:

This is not a publicly accessible system. This system is restricted to IHS Internet Protocol (IP) addresses only. User must be connected to IHS Virtual Private Network (VPN) to be gain access to the ServiceNow GCC Platform.

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

Yes

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

This is not a publicly accessible system.

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

The public cannot navigate to this system. It is only available to internal IHS customers. Non-internal users will receive a access restricted error message.

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:

<http://www.ihs.gov/privacypolicy>

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?

No

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

No

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:

The PII collected includes Name, email address, phone numbers, device identifiers. Although Protected Health Information (PHI) , Social Security Numbers (SSN), and Dates of Birth (DOB) are not requested, users may inadvertently submit this type of information. In these cases, the information will not be used or shared but merely stored.

All system data is in compliance with FedRAMP certified cloud storage facility in the US. Compliance ServiceNow GCC meets stringent U.S. Federal security requirements for handling sensitive data, including Personally Identifiable Information (PII) and PHI.

This system is designed to handle requests for service internal to IHS and the users may provide IHS issued contact information such as IHS email addresses and IHS phone numbers. The users are not asked to provide personal information such as personal phone numbers, email addresses or home addresses.

A new ticket is created for every service request. The following information may be utilized to create a service desk ticket:

- a. Full name or Active Directory user name.
- b. Business, mobile phone number (if applicable) and e-mail address.

- c. Location of equipment
- d. IT technician Assignment Group
- e. Configuration item (government asset name / computer name)
- f. Service Level due date
- g. Description of service request
- h. Relevant files such as screenshots or error logs are attached
- i. Ticket number for existing service request.

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:

PII collected by this system is not shared with external organizations. The information is stored and used internally within the IHS Office of Information Technology only.

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

Not Applicable

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:

Although Protected Health Information (PHI), Social Security Numbers (SSN), and Dates of Birth (DOB) are not intentionally collected, users may inadvertently submit PII. Any PII maintained in the system is protected through administrative, technical, and physical safeguards.

Access to the system is restricted to authorized users with an IHS D1 account and requires authentication through Single Sign-On (SSO) and multi-factor authentication (MFA). The system is accessible only from the IHS network.

System data is hosted within a Federal Risk and Authorization Management Program (FedRAMP)-authorized ServiceNow Government Community Cloud (GCC) environment located in the United States. All data is encrypted both at rest and in transit using Federal Information Processing Standards (FIPS) 140-validated cryptographic modules. These controls ensure that any PII maintained in the system is secured in accordance with HHS and federal requirements.

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

Not Applicable