Indian Health Service Security Ticketing and Incident Reporting

Supporting Statement A

Justification

OMB Control No. 0917- 0041

ABSTRACT

The Indian Health Service (IHS) uses secure information technology (IT) to improve health care quality, enhance access to specialty care, reduce medical errors, and modernize administrative functions consistent with the Department of Health and Human Services (HHS) enterprise initiatives.

IHS is responsible for maintaining an information security program that provides protection for information collected or maintained by or on behalf of the Agency, and protection for information systems used or operated by the Agency or by another organization on behalf of the Agency.

The form IHS uses is for federal employees, Tribal employees, and contractors and other non-federal employees to report IHS IT security and privacy incidents. This form has three purposes: to notify the CSIRT of an incident, provide updates about an open incident, and indicate resolution of an existing incident.

Table of Contents

A. Justification

The Indian Health Service (IHS) requests an extension with no changes for this information collection request (ICR) entitled “Indian Health Service Information Security Ticketing and Incident Reporting System.”

This collection uses a form to log and address personally identifiable information (PII) and protected health information (PHI) breaches that take place.

A.1. Circumstances Making the Collection of Information Necessary

Current IT protocol is to report any breach or IT incident on a form that goes to the IT and Privacy staff. This form is necessary to mitigate incidents regarding security and privacy. The program designed this collection to ameliorate those issues by incorporating the information on a form to meet the Agency IRT functional requirements.

This information is not harnessed on a broad scale (vis-a-vis tracking and resolving individual tickets). IHS does monitor tickets by type, which allows the privacy and security staff to update training based on the ticket types we see. For example, depending on the upswing of ticket types we will update the training provided in the ISSA annually, or we may individually update training.

Potential users of this collection will be made aware of its existence and user training is provided. This is covered in the Annual Information Systems Security Awareness training as well as Privacy Training. IHS also has posted this information on the IHS.gov employee resources page.

IHS does protect PII that is inadvertently or voluntarily given to the system. Security controls are in place to protect against unauthorized access. The system utilizes least privilege and role-based access controls. Access is granted to a limited number of authorized administrators, developers, direct contractors, and federal employees. Standard users do not have access to PII. A Privacy Impact Assessment (PIA) has been completed.

In order to estimate anticipated number of respondents, the IHS compared an average of potential respondents over a three-year period, which is 1700 anticipated respondents, annually.

The process on the IT security end for responding to submissions and how will respondents be made aware of remedies is:

1) Individual submits a ticket and receives the acknowledgement of submission,
2) Privacy and Security are notified of the ticket,
3) Privacy or Security (depending on ticket type) review the ticket,
4) provide next steps for investigation, mitigation, prevention and closure,
5) assign the ticket to the Area office Privacy or Security staff,
6) the Area privacy or security staff work with the facility and reporter when necessary, and;

7) Notify the reporter when incident is closed.

Federal employees, Tribal employees, and contractors and other non-federal employees who report IHS IT security and privacy incidents must use the form in this collection. This form has three purposes: to notify the CSIRT of an incident, provide updates about an open incident, and indicate resolution of an existing incident. This form is also used to log and address PII and PHI breaches that take place. The form does not request PII/PHI, but PII/PHI is sometimes provided voluntarily by those reporting a breach.

The form is not voluntary when there is an incident that must be reported, and additionally, it is not a form for the public to use. Only an authorized Incident Response Team (IRT) member is able to access all tickets that contain PII/PHI. Tickets containing PII/PHI are reviewed by an authorized Incident Response Team (IRT) member and transferred over to the privacy officer.

A.2. Purpose and Use of the Information Collection

This form enables IHS to capture the incident notification, update or resolution of the IT security or privacy breaches. This form will further the IHS's ability to use secure information technology (IT) to enhance response time to IT security and privacy incidents and increase the healthcare information security posture at IHS. This form also allows us to process privacy incidents/breaches within the IHS in keeping with internal and external requirements.

The main objective is to address and report IT security and privacy incidents.

Table A-1. Information Collection Summary

Information Type	Purpose
Incident Reporting Form	To capture the incident notification, update or resolution of the IT security or privacy breach.
ISTS Privacy Web Submission	To capture the incident notification, update or resolution of the IT privacy breach.
ISTS CSIRT Web Submission	To capture the incident notification, update or resolution of the IT security or privacy breach.

A.3. Use of Improved Information Technology and Burden Reduction

IHS will use all available information technology in an effort to reduce the burden to all respondents.

Data and information collected will be stored electronically. Only staff from IHS will have access, which requires a user name and password.

A.4. Efforts to Identify Duplication and Use of Similar Information

This survey is not duplicative because each incident is unique.

A.5. Impact on Small Businesses or Other Small Entities

The collection of this information does not directly impact small businesses or small entities.

A.6. Consequences of Collecting the Information Less Frequently

IHS makes every attempt to minimize IT security and privacy breaches. Only one data collection request will be made when a breach occurs. These forms will not assess changes or trends over time, and will only be used during breaches of IT security and privacy.

A.7. Special Circumstances Relating to the Guidelines of 5 C.F.R 1320.5

This request complies with the regulation.

A.8. Comments in Response to the *Federal Register* Notice and Efforts to Consult Outside the Agency

A 60 day notice was published in the Federal Register on February 17, 2022 (87 FR 9071). No public comments were received. A 30 day Federal Register notice was published on April 28, 2022 (87 FR 25284).

A.9. Explanation of Any Payment or Gift to Respondents

There will be no remuneration or gifts to the respondents.

A.10. Assurance of Confidentiality Provided to Respondents

The forms will adhere to the provisions of the U.S. Privacy Act of 1974 and conform to the requirements of HIPAA and 42 CFR part 2 with regard to surveying and questioning individuals for the Federal Government. Each respondent will be informed of the authority of IHS, the purpose and use of the form, and next steps, if any, of not responding. Personal identifiers will not be included during collection of information but may inadvertently be provided by respondents.

Information collected may be considered “identifiable private information.” Access to the data is protected under NIST 800-53 r4 Access Control AC6. IHS DIS staff operate with least privilege access, allowing only authorized accesses for users (or processes acting on behalf of users). Software encryption is used to secure data at rest on the file system. The software is FIP 140-2 certified.

A.11. Justification of Sensitive Questions

The survey collects no private information on individual people, but reports breaches of IT security and privacy. None of the data collection effort requires responses to any sensitive questions.

A.12. Estimates of Annualized Burden Hours and Costs

The total time required to complete the form is about 15 minutes.

Table A-3. Estimated Annualized Burden Hours

Type of Respondent	Form Name	No. of Respondents	No. Responses per Respondent	Average Burden per Response (hours)	Total Burden (hours)
IHS Federal and Non-Federal Staff	Incident Forms	1700	1	15/60	425
Total	**-**	**1700**	**-**	**-**	**425**

Table A-4 lists the estimated annualized burden costs.

Table A-4. Estimated Annualized Burden Costs to the Government

Type of Respondent	Total Burden Hours	Annual Rate	Total Respondent Costs
Contract	425	$25,075.00	$59.00
Total	**425**	**-**	**$59.00**

A.13. Estimates of Other Total Annual Cost Burden to Respondents and Record Keepers

There is no anticipated cost burden to the respondents resulting from the collection of information, except the costs associated with their time. There are no capital/startup costs associated with this collection of information.

A.14. Annualized Cost to the Federal Government

The initial cost for the Hardware, Software, Federal / Contractors, and License renewal equals **$58,000**. (Initial software purchase + Annual renewal + Hardware to setup the system ($32,925) + Federal / contractor staff ($25,075).

A.15. Explanation of Program Changes or Adjustments

There are no program changes or adjustments. This is an existing collection.

A.16. Plan for Tabulation, Publication, and Project Time Schedule

IHS does not plan to tabulate, or publish any results.

A.17. Reason Display of OMB Expiration Date is Inappropriate

Display of the OMB expiration date is appropriate and will be displayed on the forms, and in the online system.

A.18. Exceptions to Certification for Paperwork Reduction Act Submissions

There are no exceptions to the certification.