Indian Health Service Security Ticketing and Incident Reporting

March 29, 2018

Supporting Statement A

Justification

OMB Control No. 0917- NEW

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 a new three-year approval for an information collection request (ICR) entitled "Indian Health Service Information Security Ticketing and Incident Reporting System."

This ICR is authorized by Section 301 of the Public Health Service Act (42 U.S.C. § 241). The 60-day FRN was published on November 11, 2017 and is further discussed in Section A.8. 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 incidence on an electronic form (F07-02b) that goes to the IT and Privacy staff. This form is necessary to meet the requirements of Section 301 of the Public Health Service Act and to mitigate incidents regarding security and privacy. The previous system was unable to generate the required reports for FISMA and other Audits. The previous system utilized an inefficient workflow where users could not open the tickets directly by sending email to IR group. The previous system was unable to provide any useful metrics to manage the level of efforts required to resolve the issues in a timely manner. The previous system was unable to provide a robust knowledge base for user and security engineers to take immediate actions. Given the shortcomings of the system, this necessitates the need for the new collection to address these issues. The new system generates the required reports for FISMA reporting and other audits, provides metrics, and reduces the workload and level of efforts to provide swift response and immediate action to identify and resolve the issue to protect agency systems, data and user community from any vulnerabilities or cyber threats.

The program designed this collection to ameliorate those issues referenced above by incorporating the information on a form to meet the Agency IRT functional requirements. The inherited legacy system was unable to meet the functional requirements needed for FISMA and was hampered by an inefficient workflow.

Section 301 of the Public Health Service Act is the authorizing law for this survey collection. Additionally, these laws also support the collection. 5 CFR 552(a), 5 CFR 293.311 and 45 CFR 164.530.

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' 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 allow us to process privacy incidents/breaches within the IHS in keeping with internal external requirements.

IHS staff (including federal employees, Tribal employees, and contractors and other non-federal employees) must use the form in this collection to report IHS IT security and privacy incidents. This form has three purposes:

1. To notify the CSIRT of an incident
2. Provide respondents updates about an open incident
3. Indicate resolution of an existing incident

The main objective is to address and report IT Security and privacy incidents, including, but not limited to, logging and addressing any PII and PHI breaches that may arise.

This information is intended to track and resolve individual tickets, rather than harness on a broad scale, at this time. IHS does monitor ticket trends, allowing the privacy and security staff to update training based on frequency and severity of the ticket types we receive. For example, depending on the upswing of ticket types we may update the training provided in the ISSA annually, or we may individually update trainings on particular topics (e.g. phishing, spear phishing, insider threats).

Potential users of this collection will be made aware of its existence and user training will be provided during 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. This form is not voluntary when a reportable incident has occurred, and additionally, it is not a form for the general public to use.

The process by which the IT security will respond to submissions and interact with respondents will be:

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, Cyber Security incidents are reviewed by DIS IR personnel and privacy incidents are reviewed by privacy group.
4) Privacy or Security will determine next steps for investigation, mitigation, prevention and closure, (e.g. change of password, install new firewall software, etc.). Investigation, mitigation, prevention and closure are the natural progression of the system to respond to Cyber security or privacy incidents.
5) Ticket will be assigned to the Area office Privacy or Security staff,
6) Area privacy or security staff work with the facility and reporter when necessary, and;
7) Notify the reporter when incident is closed.

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 IT in an effort to reduce the burden to all respondents.

Data and information collected will be stored electronically. Only the Privacy group, Division of Information Security IR staff and HQ ISSOs will have access to the collection of information stored in this system and 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 and does not use similar information from any other systems. This is because each security incident is unique. While other agencies may utilize IT security forms or information similar to this one, this one is unique to IHS' specific needs and requirements because it only will collect the information when a security or privacy incident occurs.

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

The collection of this information does not directly impact small businesses or small entities. Tribes are sovereign governments and not considered "small business or small entities" for the purposes provided for this collection.

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. It is imperative that every occurrence of a breach is reported to IT Security and privacy using this form in order to mitigate IHS breaches. Collecting this information less frequently would endanger the agency and those we serve, and does not align with best security practices.

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. A 60 day notice was published in the Federal Register on November 30, 2017 (82 FR 56832) and a 30 day notice was published on February 14, 2018 (83 FR 6600). No public comments were received.

B. IHS previously attempted to submit this collection under the Fast Track Collection for IHS. OMB did not feel that the Generic was an appropriate forum for the request therefore, IHS prepared this collection as a new collection under a standard information collection request.

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 conforms with the requirements of HIPAA and 45 CFR part 164 and 42 CFR part 2 with regard 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 is considered "identifiable private information" as defined by the Privacy Act 5 CFR 552(a). Access to the data will protected under NIST 800-53 r4 Access Control AC6. IHS DIS staff with least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Software encryption is used to secure data at rest on the file system. The software is FIP 140-2 certified.

While this form does not explicitly request PII/PHI from respondents, PII/PHI is sometimes provided voluntarily by those reporting a breach. 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. Only an authorized Incident Response Team (IRT) member is able to access all tickets that contain PII/PHI. Ticket containing PII/PHI are reviewed by authorized Incident Response Team (IRT) member and transferred over to the privacy officer.
A PIA has been completed and can be found here:
>https://www.ihs.gov/privacyact/includes/themes/responsive2017/display_objects/documents/pia/InformationSecurityTicketing.pdf<

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	.25	425
Total	**-**	**1700**	**-**	**-**	**425**

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. This is also an average over three years, obtained by reviewing the previous reporting number of employees.

Table A-4 lists the estimated annualized burden costs.

Table A-4. Estimated Annualized Burden Costs

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 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 a new collection.

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

This information is intended to track and resolve individual tickets, rather than tabulate trends on a broad scale. IHS has no current plans to tabulate or publish any findings or results.

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

Display of the OMB expiration date is appropriate and will be displayed on all forms.

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

There are no exceptions to the certification.