

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.....4

A.1. CIRCUMSTANCES MAKING THE COLLECTION OF INFORMATION NECESSARY
4

A.2. PURPOSE AND USE OF THE INFORMATION COLLECTION.....4

A.4. EFFORTS TO IDENTIFY DUPLICATION AND USE OF SIMILAR INFORMATION 5

A.5. IMPACT ON SMALL BUSINESSES OR OTHER SMALL ENTITIES.....5

A.6. CONSEQUENCES OF COLLECTING THE INFORMATION LESS FREQUENTLY 5

A.7. SPECIAL CIRCUMSTANCES RELATING TO THE GUIDELINES OF 5 C.F.R 1320.5 5

A.9. EXPLANATION OF ANY PAYMENT OR GIFT TO RESPONDENTS.....6

A.10. ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS.....6

A.12. ESTIMATES OF ANNUALIZED BURDEN HOURS AND COSTS.....6

A.13. ESTIMATES OF OTHER TOTAL ANNUAL COST BURDEN TO RESPONDENTS AND
RECORD KEEPERS..... 7

A.14. ANNUALIZED COST TO THE FEDERAL GOVERNMENT.....7

A.17. REASON DISPLAY OF OMB EXPIRATION DATE IS INAPPROPRIATE.....7

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

The form in this collection must be used by IHS staff (including 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. 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. The collection does not request the PII/PHI, but PII/PHI is sometimes provided voluntarily by those reporting a breach. Only authorized Incident Response Team (IRT) member is required 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.

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.

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 only 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. A notice was published in the Federal Register on November 11, 2017 and no public comments were received.

B. IHS attempted to have this collection under the Fast Track Collection for IHS. OMB rejected the request therefore, IHS prepared this collection under a regular information collection.

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.

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 |

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

\$58K – Hardware, Software, Federal / Contractors, and License renewal. (Initial software purchase + Annual renewal + Hardware to setup the system + Federal / contractor staff)

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

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.

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

There are no exceptions to the certification.