Division of Information Security

IHS Information Security Policy/Standard Waiver Request Form
F06-11i

Instructions: This form is to be used by Indian Health Service/Tribal/Urban (I/T/U) employees or facilities requesting a temporary waiver of a specific IHS security policy or standard. Waivers may not be granted for a period of more than one year. Please complete Sections 1 and 2 below and submit the waiver request to the IHS Division of Information Security (DIS) at Cybersecurity@ihs.gov.

Section 1

Date of Request:

Requested Expiration Date:

Name:

Title:

Federal/Non-Federal Facility: Make Selection

Area/Facility:

Information System Name:

Policy/Standard to be Waived:

Section 2

1. **Description of Affected Data or Device(s).** In the space below describe the specific data or device(s) affected by this waiver request. For any hardware affected include the make, model, software, firmware, serial number, and system host name. Please note, if this waiver involves a medical device or PHI/PII describe the type of service the device supports and any replacement or mitigation costs if known. Attach the Access Control List (ACL) configuration if the device is on a VLAN.

IP Address: Hostname:

2. **Waiver Justification for Noncompliance or Deviation.** In the space below, explain why compliance with the above policy/standard is not possible due to technical limitations, conflicts with mission requirements, and/or other circumstances. Attach additional documentation if necessary.

3. **Compensating Controls.** Describe any alternative mechanisms or controls in place that reduce the risk to the data or devices described in question #1.

4. **Plan to Exit Waived State.** Describe the plan to bring the system into compliance with IHS/HHS policies and/or standards. Please include any milestones with associated dates.

5. **How Will the Plan be Funded:** Make Selection

5a. **If hours, what are the estimated number of hours needed to complete the plan:**

5b. **If dollars, how will the plan be funded:** Make Selection

5c. **If dollars, what is the estimated cost:**

Area Information System Security Officer

◯ Approve ◯ Disapprove

Area Information System Coordinator or Area Chief Information Officer (as applicable)

◯ Approve ◯ Disapprove

Submit a signed copy of this waiver to the IHS Division of Information Security at Cybersecurity@ihs.gov. The approver(s) shall retain the original.

Section 3

Instructions: This portion of the form is used by DIS officials to analyze the risk inherit to this request and to approve or deny authorization for the requested security waiver. The Waiver Review Board will complete Section 3.

DIS Risk Analysis and Recommendation. In the spaces below, DIS will describe the potential level of risk to the affected system(s) and the IHS enterprise. A recommendation from the Waiver Review Board will be included.

Risk Analysis:

Recommendation:

Condition:

Waiver effective until:

IHS Chief Information Security Officer

○ Approve — I acknowledge that I have reviewed this request for a policy/standard waiver and find the resultant risk to be acceptable.

○ Disapprove — I acknowledge that I have reviewed this request for a policy/standard waiver and find the resultant risk to be unacceptable.