



Introduction to CAO Cybersecurity Services

Reese Weber, MBA, CISSP
Chief Information Security and Privacy Officer
Indian Health Service
California Area Office

Interconnection Security Agreements (ISAs)

- This agreement defines procedures of reciprocal cooperation and coordination between IHS and a tribal-entity. "All Tribal IT or Urban IT systems that will be connected to the IHS network, regardless of the nature of the connection, require... an ISA to be submitted and approved prior to activation of the connection." Indian Health Manual, Part 8 Chapter 15.
- ISAs are implemented at the national, area, or facility level. Partners conducting business with a single facility should have an agreement with the local area and/or facility. Partners with national contracts, or separate contracts operating within many different IHS areas, should have a national agreement with the IHS Office of Information Technology.

Information Technology Access Control

- The Information Technology Access Control (ITAC) system is a web-based system that records access to information systems
- Can be utilized to record access to any system, even tribal/urban/local systems
- Fulfills HIPAA access control record requirements

The screenshot displays the Indian Health Service (IHS) website's Information Technology Access Control (ITAC) system interface. At the top, the IHS logo and name are visible, along with a search bar and navigation links. The main header includes a menu with options like Home, About IHS, Locations, for Patients, for Providers, Community Health, Career Opportunities, and Newsroom. The left sidebar contains a list of links for the Office of Information Technology, including Home, New User, Update Access, Remove User, Drafts, Annual Access Review, Team Management, Alternates, Request Tracking, and Training. The main content area is titled "Information Technology Access Control (ITAC)" and features a "Request Submission Sub-System" section. This section includes a welcome message for Theresa Weber acting for Robert Gemmell, a brief description of the system's purpose, and instructions on how to access the system. A small image of a person at a computer is also present. The footer contains contact information for the Indian Health Service (HQ) and a "STAY CONNECTED" section with social media links.

Indian Health Service
The Federal Health Program for American Indians and Alaska Natives

Search ihs.gov

Home About IHS Locations for Patients for Providers Community Health Career Opportunities Newsroom Your Account

Office Of INFORMATION TECHNOLOGY

Home
New User
Update Access
Remove User
Drafts
Annual Access Review
Team Management
Alternates
Request Tracking
Training

Questions or Comments? Please contact the Content Manager.

Information Technology Access Control (ITAC)

Request Submission Sub-System

(Theresa Weber acting for Robert Gemmell) [\[switch user\]](#)

Welcome!

Welcome to the Information Technology Access Control (ITAC) system, **Request Submission Sub-System**. The purpose of this system is to enable qualified Indian Health Service (IHS) personnel to submit requests for access to computer and network resources.

Appropriate supervisors can submit **new access**, **update access** or **remove access** requests for their team members, as well as perform required **annual access reviews** and **team management** functions.

To access this system, you need:

- 1. An IHS Web Login:**
If you have an IHS Web Systems Login (username and password), you can login by clicking the 'Login' button (left). If you do not have an IHS Web Systems Login, you can register with the system by clicking the 'Register' button (left).
- 2. System Permissions:**
For permissions to access this system, you will need to have your supervisor submit an access request for this system.

Welcome, Robert Gemmell.

Indian Health Service (HQ) - 5600 Fishers Lane, Rockville, MD 20857 - Find a Mail Stop

Accessibility • Disclaimer • FAQs • Website Privacy Policy • Plain Writing Act • Freedom of Information Act • HIPAA • No Fear Act • Contact Information • Download Plug-Ins

STAY CONNECTED
f y in

Malicious Traffic Notifications

- HHS and IHS both have Computers Security Incident Response Teams (CSIRT) that are constantly using software to scan the network for malicious files
- HHS and/or IHS CSIRT notifies ISSO, ISSO works with the site to identify users/systems and mitigate the risks.

RiskVision incident HHS_CSIRC_ID has been created to track this incident.

HHS CSIRC findings:

* Source IP(s): 198.45.3.26

* Destination IP(s): 216.119.115 [REDACTED]

* Destination Host: mail.kimaw[.]org

* Date/Time: 2018-10-17T16:13

* Traffic Type: HTTP GET Request/Malicious .doc file

*MD5: 25b19fcb6d4e793a165a9cdc5834d6a8

Critical Patching Notifications

- HHS regularly scans all systems on the domains for patch compliance, especially during pervasive attacks
- IHS also does the same sort of scans, using resources like Tenable and Nessus scans.
- HQ notifies Each Area ISSOs of affected systems, or vulnerable systems
- ISSOs disseminate to appropriate contacts for remediation, provides instructions and offers assistance in regards to mitigation.



Sample Wanna Cry Area Report

[illegible]

Additional Services by IHS

Services Offered by HQ:

- Firewall management and support
- Network device management
- IHS Web Account Management

Services Offered by Area Office:

- Disaster Recovery Planning
- Backup planning
- Access Control implementation
- Account/access reconciliation
- ISSA tracking

Questions??

Reese Weber, MBA, CISSP

Information Systems Security Officer

Indian Health Service, California Area Office

916.930.3981 x 307

Theresa.weber@ihs.gov