DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

Indian Health Service
Rockville MD 20852

SEP 14 2009

Dear Tribal Leader:

As part of our ongoing effort to secure information resources, the Indian Health Service (IHS) is required to establish formal agreements with all non-Agency users that access IHS information technology (IT) systems through system interconnections. Your cooperation is needed to assure that your health program complies with this requirement.

Over the past nine months, the IHS information technology infrastructure has experienced a myriad of attacks. These incidents include major breaches emanating from foreign hosts, four separate virus and Trojan horse outbreaks, and a significant Denial of Service attack. Undocumented and unapproved system interconnections contributed to these attacks and will continue to pose a security risk to IHS information resources in the future. Currently, only sixty percent of Tribal system interconnections are operating with an approved Tribal Interconnection Security Agreement (Tribal ISA). In addition, there are a significant number of organizations connecting to IHS IT systems through tribal networks without a Business Partner Interconnection Security Agreement (BPISA).

Federal mandates require federal agencies to establish interconnection agreements. The National Institute of Standards and Technology (NIST) Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems," recommends completion of an ISA to document the technical requirements of an interconnection and a Memorandum of Understanding to document roles and operational responsibilities for interconnection access. These actions must occur prior to accessing IHS IT systems and will apply to all new and existing interconnections.

Due to the recent attacks on IHS information resources, all system interconnections must have approved ISAs in place no later than Thursday, December 31, 2009. Any system interconnection found operating without an approved ISA after that date will be subject to an immediate disconnect from the IHS network. A disconnect from IHS network resources could adversely affect a site's ability to provide patient care.

Please contact your IHS Area Office for additional information and assistance. Mr. Brandon Begaye of the IHS Division of Information Security is assisting Area Office staff with this effort. Mr. Begaye can be reached by phone at (505) 248-4356 or by e-mail at brandon.begaye@ihs.gov. The ISA and MOU templates can be downloaded from the DIS website at http://security.ihs.gov/ISA.cfm.

I appreciate your involvement and forbearance as we work together to address these vital security concerns.

Sincerely yours,

/Yvette Roubideaux/

Yvette Roubideaux, M.D., M.P.H.
Director

I also plan to convene a tribal consultation meeting to discuss the results of this request and to plan our next steps together as we work to reform the IHS. If you would like to recommend a location or specific date to hold the tribal consultation meeting, please include this information in the e-mail with your three priorities.

As we go forward, communicating with you on the status of ongoing initiatives becomes ever more vital to our long-term success. One of my priorities is to develop strategies to be more transparent about our work. Last month, the IHS rolled out a new tool to help us keep track of our progress on internal IHS reform. The Web site, **www.ihs.gov/reforms**, will feature updates and related information on internal IHS reform.

I look forward to working with you to bring change and improvement to the IHS.

Sincerely yours,

/Yvette Roubideaux/

Yvette Roubideaux, M.D., M.P.H.
Director