JUDICIAL INFORMATION SYSTEMS
9.4 POLICY ON RESTRICTIONS TO INTERNET SITES

(a) Introduction

To enhance Judiciary network security and performance, it is necessary to restrict access to Internet web sites that host content that has been deemed objectionable, presents a security risk, or has been found to downgrade network performance. As a result, this policy is established for such a purpose and is intended to comport with the Judiciary's Security Policy and Standards.

(b) Policy

(1) A web-filtering appliance is installed on the Judiciary Private Network to restrict access to web sites that host the following categories which includes:

(A) Adult/Pornographic
(B) Dating
(C) Gambling
(D) Peer-to-Peer or Web-Based File Sharing (unless otherwise approved)
(E) Personal Web-Based Email
(F) Streaming Media (unless otherwise approved)
(G) Illegal/Questionable Activity

(2) In addition to blocking access to the above categories, the web-filtering appliance records by source IP address and user name, all access to the Internet from within the Judiciary Network. Depending on the volume of Internet activity on the network, the appliance has the capacity to store the most recent thirty days of Internet access history.

(3) In recognition of the need to access personal web-based email during the business day, the Public Wireless Network has been configured to allow access to personal email accounts.

(c) Procedure for Requesting Internet Activity

(1) In support of an investigation, requests for Internet activity must be submitted to AOC Human Resources or Internal Affairs.

(d) Procedure for Requesting a Blocked Internet Site

(1) To request access to a blocked Internet site, an Administrative Official must submit the request to JIS Information Security and include the business justification for allowing the site and the names of the individuals who require access to the site.