from a device owned or controlled by the CA or Delegated Third Party, (ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by Multi-Factor Authentication, and (iii) the remote connection is made to a designated intermediary device (a) located within the CA’s network, (b) secured in accordance with these Requirements, and (c) that mediates the remote connection to the Issuing System.

3. LOGGING, MONITORING, & ALERTING

Certification Authorities and Delegated Third Parties SHALL:

   a. Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems;

   b. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity;

   c. Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events;

   d. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events;

   e. Conduct a human review of the logging processes for application and system logs at least once a month to validate the integrity of logging processes through continuous automated and ensure that monitoring, and logging, alerting or through a human review to ensure that logging, and log-integrity-verification, functions are effective operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool). Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days and

   f. Maintain the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with disclosed business practices and applicable legislation.

   fg. If continuous automated monitoring and alerting is utilized to satisfy sections 1.h. or 3.e. of these Requirements, respond to the alert and initiate a plan of action within at most twenty-four (24) hours.

4. VULNERABILITY DETECTION AND PATCH MANAGEMENT

Certification Authorities and Delegated Third Parties SHALL:

   a. Implement intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against common network and system threats;