

Jim Gibbons  
Governor



Jearld L. Hafen  
Director

Captain PK O'Neill  
Division Chief

Livescan Customers:

The following are hardware and service requirements that are required for establishing a connection to Nevada Department of Public Safety for the purposes of submitting fingerprints electronically:

- **Agencies connected to or through SilverNet** (government agencies only) should supply their DoIT-routable address. (10.0.0.1 – 10.255.255.254)
- **Agencies using an Internet connection** need to supply a static IP address that is routable on the Internet. Of the IP address range from 0.0.0.0 to 223.255.255.255, the following address ranges are NOT routable on the Internet:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- **A firewall capable of creating an IPSEC VPN tunnel that also meets Federal Information Processing Standard (FIPS) 140-2** for the encryption engine. DPS strongly recommends using the Cisco ASA 5505 or another Cisco product in the ASA series. Using this product will enhance the ability for “canned” configurations. If you want to see if your device meets the FIPS 140-2 standard, check the list at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>. At this site, the products are listed by date of approval and not by manufacturer or model so you may need to hunt around for your specific product. If you find your product, there should be text that says “Validated to FIPS 140-2”. If your product is not in the list or the entry for your product lacks this endorsement, you may not use that product to connect to Nevada DPS.
- **If you are planning to use a mobile livescan unit**, and/or you are thinking of connecting your livescan wirelessly, or your livescan unit might possibly be stored in a non-secure location, please call first so we can discuss the requirements with you before you purchase your livescan unit.

## **Nevada Specification Requirements**

All livescans must be configured to the current Nevada Specifications prior to connection and be able to transmit SMTP. Your livescan must also have the ability to retrieve messages using a POP3 account. You and/or your vendor may obtain these specifications from one of the Livescan Coordinators listed on the Livescan Connection Cover Letter.

## **Site Security Inspection**

Before DPS can allow your site to connect to the DPS network as well as indirectly via L-1 ESD (hereafter known as L-1 ESE), the Information Security Officer (ISO) or the ISO's designee may evaluate the security assessment in lieu of performing physical site security inspection or as otherwise prescribed by the Division. You must already have your Internet service established and your firewall in place. If you are selecting or preparing the site for the livescan unit, keep the following pointers in mind:

- The livescan unit should be in a location that is physically accessible only by those who are authorized to use the device, plus those who have passed fingerprint-based background investigations. All others must be continuously escorted while in the livescan area. This includes custodians and maintenance workers of all kinds.
- The definition of a secure area is one in which unauthorized access can only be gained by the use of special tools and access would show obvious signs of damage. Some common items to check are:
  - If an access door to the secure area has the hinges outside the secure space, the hinges should be the type where the hinge pin can't be removed.
  - If there is a drop ceiling, verify that all the walls go to the top of the structure and not just to the drop ceiling. If someone could get into the room just by removing ceiling tiles and climbing over the wall, the room is not secure.
- You may not connect any other computers or install any wireless access points behind the firewall that protects the livescan unit.

The livescan unit and all wiring and hardware up to and including the firewall must be secured from unauthorized access. The most obvious way to do this is to keep the livescan and its firewall in a locked office. Using a wireless connection for connecting the livescan unit is discouraged.

Any hard drive or non-volatile memory must be sanitized before the livescan can be stored in a non-secure location or transported by a person who is not authorized to access the livescan unit.

### **Turning Up Service**

All activities, the administrative provisioning for livescan system settings, site security checks, establishing connectivity, and turning service on or off, are all initiated with a call to the DPS Fingerprint Examiner Unit. The primary contact is Stan Shafer, (775) 684-6227, or Erica Souza, (775) 684-6235. The Fingerprint Examiner Unit will coordinate all the activities with the other DPS units and will be a central point of contact for you.

All security issues discovered during the site security inspection must be addressed before submitting fingerprints electronically.

Please understand that the administrative setup, the security inspections, coordinating test submissions, and the network connectivity are all separate functions of DPS and may require different individuals for each task.

### **Compliance Auditing**

Your site may be checked at any time to ensure compliance with current policies affecting livescan use, and we use the opportunity to provide education about any changes to policy. If any security issues are brought up during these visits, please act and respond promptly. This will keep you securely connected for fingerprint submission.

Thanks!