Network Security Policy

XO makes use of a variety of security mechanisms and practices to protect traffic on its IP/MPLS backbone.

Network

The XO IP/MPLS Core Network consists of routers owned and operated by XO, and located in XO-operated facilities, along with peering routers in XO-managed space in collocation hotels and similar facilities. The Core Network uses circuits provided by DWDM and circuit-transport systems likewise owned and operated by XO. It is connected to customer-facing Edge Routers owned and operated by XO, located in both XO facilities, collocation hotels and similar facilities. The Edge Routers use circuits across both XO and third-party managed CWDM/DWDM and circuit-transport systems. Any third-party systems used for circuits are required to meet reliability standards equivalent to those of XO.

Common Carrier

XO is a common carrier engaged in the provisioning and carriage of telecommunications services. The protection of communications carried via a common carrier's network are subject to federal law and regulation, including restrictions and prohibitions regarding access to and or disclosure of voice or data communications carried or stored on its network (e.g. Telecommunications Act, Electronic Communications Privacy Act, Stored Communications Act, Communications Assistance for Law Enforcement Act, etc). XO acting as a common carrier transports voice and data traffic without reference to the nature of the communications, and the direct provision of any Confidential Information, (including; Associate Information, Customer Information, or information subject to privacy laws, collectively known as "Protected Data"), from the customer to XO is neither required by XO, nor necessary for the provisioning of services by a common carrier.

Customers should agree that they will not directly disclose, or provide Protected Data to XO, and that use of common carrier services, does not constitute disclosure. If any customer must reveal "Protected Data" to XO in connection with any telecommunications services, which are, or may be provided, it will inform XO in advance of the necessity, and reasons for such disclosures. Customers would need to prominently mark such information as "Legally Protected Confidential Information."

Release Version 7, August 2012

SSAE 16

SSAE is an international accounting audit standard that discusses the requirements for various types of audits of a service organization's controls.

SSAE 16 replaces SAS 70 which has recently been retired. There are three types of audit reports under SSAE 16, called Service Organization Control (SOC) reports. A SOC 1 report applies to an audit of controls over financial reporting and is often used by an entity's auditors.

SOC 2 and SOC 3 reports apply to audits of operational controls of certain facets within a business (i.e., security, availability, confidentiality / privacy, and processing integrity.

One facet of SSAE 16 certification can involve whether a company has implemented exceptional measures for protecting their datacenters, especially as it relates to protecting their customers' personal or other protected information. Many, potential customers (through RFPs and questionnaires), as well as existing customers, ask XO for reassurance that we are compliant with SSAE 16.

XO is currently evaluating SSAE 16 certification requirements to determine the cost benefit of such certification. The reason XO has not previously conducted an SSAE 16/SAS 70 audit is actually very simple and supported by federal telecommunications laws.

As a carrier, XO has a general obligation to carry any communication regardless of the nature of those communications, and long-standing US federal telecommunications laws provide for the security of all communications, regardless of their nature, traveling over or stored on telecommunications voice and data networks (e.g., Electronic Communications Privacy Act, 18 USC 2510, et seq.; Stored Communications Act, 18 U.S.C. §§ 2701-2712; and Communications Act, 47 USC 222 & 605). These laws operate to protect all voice and data communications against unauthorized interception, surveillance or disclosure by a telecommunications carrier or internet service provider. Accordingly, there is no need for an SSAE 16 audit of such services.

XO understands that some customers need assurance that the XO telecom network itself is secure in keeping with XO's obligations under law. XO appreciates that some customers with sensitive data concerns may need information about network security policy, testing, breach response and notification so that they can be in a position to know whether communications have been compromised and make any necessary assessments about their own response based on the nature of the information the customer transmitted. Customers and prospective customers can be assured that, in keeping with its obligations as a common carrier, XO employs commercially reasonable technical, logical, physical and administrative safeguards aimed at protecting its proprietary network and the communications backbone owned and/or controlled by XO to ensure that a standard set of security procedures are in place for network elements. As a common carrier under US law, XO has taken those steps necessary to secure its own telecom infrastructure to prevent unauthorized access to the network. XO does not have IT datacenters filled with our customers' sensitive information that requires protection, nor does it have responsibility for the potential need to encrypt data moving through the XO network. XO does not encrypt customer data, nor does it process such data, as it does not have access to such data. We merely transport customer data safely between the customer's network and the limits of the XO network. Customers may choose to encrypt sensitive data themselves.

When serving as a collocation service provider of facilities that house customer owned and controlled equipment on which customers may store, transact or transmit data, XO may have some obligations to secure the facilities. However, because XO has no knowledge or investment in the type or quality of customer equipment or data being stored in these facilities, the customer is responsible for securing logical access to their equipment and data. RFPs or questions involving Colocation services that include SSAE 16/SAS 70 compliance questions should be openly answered by acknowledging that XO is not presently SSAE16/SAS70 certified.

For the bulk of RFPs and questions, once potential customers are enlightened to the fact that XO only provides data transport and/or collocation space and does not have access to or responsibility for any customer data which requires protection, it has been our experience that customers generally accept that XO has no SSAE 16/SAS 70 obligation.

Security Demarc

This is relative to the products in question, but typically is defined as the last device that is wholly managed by XO or the Customer. "Managed" is defined by the party that is primarily responsible for the configuration of the device. In the majority of cases (excluding security related services) encryption of data must occur before the Customer side of the demarc point. Security Policies will apply in the following way; XO's security policies; will apply on the Provider side of the Security Demarc while the Customer's security policies will apply before the Customer side of the Security Demarc.

Vulnerability & Penetration Testing

Customers wishing to conduct Vulnerability or Penetration testing across the XO network directed at their own devices and environments should notify XO in advance to avoid false alarms being generated within the network. However, customer's should be aware that

our "Acceptable Use Policy" (AUP) so any activities directed at our network elements will result in either the immediate suspension of services or possible termination of the contract.

Command and Control Network

A logically and/or physically separate telemetry network is used to manage the backbone network elements. This provides a means to manage and repair systems when in-band communications are disrupted.

Denial-of-Service Protection

XO makes use of several strategies to detect and mitigate Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks as well as other malicious traffic within its networks. These include:

- Source address filtering: Singly-homed customers cannot source IP packets with spoofed IP addresses.
- Detection: Near real-time DoS and DDoS attack detection based on packet-per-second threshold alarms on individual router interfaces.
- Router protection: Each backbone router makes use of a local firewall filter to block unwanted traffic. Services that must be allowed are rate-limited to prevent resource exhaustion attacks.
- Coordination with Peer Providers and the Internet Security Community

User Authentication

Interactive logins to network elements are authenticated by a two-factor authentication system based on SecurID tokens. Users must both know a PIN password and possess the token before access is granted. Additionally, management access to network elements is only permitted from a small set of approved locations.

XO's deployment addresses the following standard requirements:

- Periodic password resetting
- Time activated lockouts regarding temporary passwords
- Tracking invalid logon attempts
- Disable accounts following failed attempts
- Real-time account suspension of departing employees
- Tracking successful & unsuccessful administrative access attempts

User Authorization

XO staff members are granted specific access privileges to each type of backbone element they are tasked to manage. The commands and features available to a particular user on a device are limited to those required by their task.

Encrypted Management Access

Where supported, network element management sessions are encrypted using the SSH protocol. This encryption protects the privacy of element configuration data while in transit.