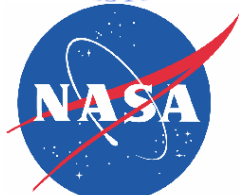




## Government & Military

### Selected Clients



## Securing Remote Management for the World's Most Critical Information & Communication Assets

### The Challenge

As agencies and employees become more geographically disparate, remote management of IT and voice systems becomes a necessity. Every day internal technicians, contractors, and outside vendors remotely access all types of equipment, including PBX and VoIP systems, IT devices, and storage systems. Remote access and management systems have changed from simple terminal emulation programs to web, remote desktop, and proprietary tools. Operations departments are overwhelmed by new and ever-changing security and compliance requirements, burdened with repurposing and managing legacy remote access technology ill-equipped to meet today's remote management requirements.

### What We Do

ION Networks manufacturers purpose-built security appliances, modems, and access gateways used for the remote management of IT and voice systems.

### Value to Government Agencies

- **Satisfies All Government Requirements for Secure Access** to PBXs, routers, servers, etc. for device administration (service, updates, changes) by all technicians, consultants, and vendors.
- **Centrally Managed and Easy-to-Deploy Solution.** ION products require little to no customization. Products are designed to snap into your network and work with existing tools.
- **Supports Virtually Any Device, Application, and Connectivity.** Unlike traditional VPN and modem solutions, ION's solution is vendor agnostic and multi-purpose.
- **Meets Department of Defense Requirements to Secure Administrative Interfaces,** which eliminates the cost for expensive upgrades and switch replacements.
- **Reduces Network Downtime and Equipment Costs.** Built-in features, including alarm management, water monitoring, and temperature monitoring notify your team members of potential problems and provide the access they need to diagnose and fix problems remotely. This significantly reduces downtime, eliminates the need for costly site visits and decreases the risk of damage to equipment.
- **Secure Department of Defense (DoD) Access:** Use ION's DoD-approved, highly secure portal to simplify access to devices located deep within the DoD network.

## Selected Products



### Secure Modem

Remote dial-up access with built-in multi-factor authentication and audit trail.



### Secure Appliances

Highly secure remote IP and dial-up access to virtually any IT or voice system. All-in-one solution for access, management and compliance.



### Secure Access Gateway

Simple, secure, and centralized remote management via the Internet.

## Selected Use Cases

### US Department of Defense (US Air Force & US Marine Corps)

The US DoD required that all systems installed on IP or voice networks pass a system interoperability and information assurance test. [The ION solution was one of the first systems that passed both sets of tests and received APL approval ([http://jitc.fhu.disa.mil/tssi/apl/apl\\_ion.html](http://jitc.fhu.disa.mil/tssi/apl/apl_ion.html)).] The ION system was used to secure Class 4 & 5 Nortel switches and voice adjunct devices that failed a DoD Field Security Office security audit. Use of the ION system was then expanded to secure all system administrative interfaces of critical communication systems located at US Marine Corps bases across the globe.

### NASA

NASA needed a secure out-of-band (dial-up) access system to Cisco routers and switches that met their requirement for strong authentication. Since two-factor authentication and SSH encryption is embedded in ION solution NASA choose the SA5600 Secure Appliance for this application.

### White House Communications Office

The White House Communications Office is responsible for managing and monitoring critical voice systems used by the President of the United States. Whether the President is in the White House or traveling in Air Force One his communications go through a special Avaya voice system. The White House Communications Team uses the ASG Guard II (Avaya OEM of ION's ION Secure 5500 appliance) to remotely access these Avaya switch and voice adjunct systems for remote diagnostics and management.

### United States Postal Service

Sprint is the primary voice provider for the United States Postal Services. Sprint needs to remotely access the Nortel voice devices installed at US Post Office locations across the country. The US Post Office has a stringent security requirement that Sprint could only meet with the ION SA5600 Secure Appliance. With the SA5600 Secure Appliance, Sprint can now securely monitor voice systems installed at post office locations throughout the country.

## About ION Networks

Now part of Cryptek, Inc., ION Networks is the most trusted name in remote administrative management and secure access technology. Founded in 1982, ION has an over twenty year history solving the problems associated with remote access. One of the first solutions certified by DoD JITC, ION has a significant install base of government customers in both the United States and abroad, using both the ION and ASG (Avaya OEM) suites of products. Additionally, Fortune 500® firms and more than half the world's largest service providers rely on ION's products for remote technician access. For more information, visit [www.ion-networks.com](http://www.ion-networks.com) or call +1 908.546.3900.