

## **Introduction**

Multiple federal regulations exist today requiring government organizations to implement effective controls that ensure the security of their information systems. Additional legislation exists to provide for the protection of information managed by private companies. The goal of these regulations is to establish a set of policies and controls that reduces the risk of unauthorized access to information or systems, and to improve detection and containment of security breaches to reduce their effect. This paper provides an overview of some of the more important regulations, in particular how they impact the security issues relating to remote support, and how SecureLink can help businesses and agencies meet security requirements.

## **Executive Summary**

A typical government entity or public company may have 50 to 100 vendors requiring access to the network in order to provide support. CIO's are faced with the conflicting goals of maintaining security by restricting access and controlling costs by reducing the number of on-site visits needed for system support. The problem is compounded by the fact that vendors do not use the same type of connectivity. Managing multiple VPNs, desktop sharing, point-to-point networks and modems creates a security nightmare. SecureLink offers a single secure platform for managing remote support connections. SecureLink acts as a gatekeeper for all vendors needing access to the network, providing authentication, encrypted networking, and detailed auditing. In order to better understand where SecureLink helps organizations meet security obligations, let's first take a look at some of the more important compliance requirements.

## **General Federal Regulations and Oversight Agencies**

**Federal Information Security Management Act of 2002** – FISMA imposes a mandatory set of processes for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency. These processes are detailed through a combination of Federal Information Processing standards (FIPS) and the special publications issued by NIST.

**NIST** – The National Institute for Standards and Technology is the source of guidelines for implementing security for Federal information systems. NIST is a non-regulatory agency inside the Department of Commerce whose mission is to “promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.” NIST issues FIPS and additional publications that help define Federal government security standards. NIST Special Publications (SP) includes a series of documents with specific recommendations for applying security controls, such as SP 800-53 – Recommended Security Controls for Federal Information Systems.

**Federal Information Processing Standards (FIPS)** – FIPS are developed by National Institute of Standards and Technology (NIST) and cover a very wide range of information technology standards. The key standards include:

- FIPS 200 – Outlines the minimum security requirements for Federal information and information systems
- FIPS 199 – Provides the standards for security categorization of Federal information and information Systems

## **Agency or Industry Specific Regulations**

**HIPAA** – Title II of the Health Insurance Privacy and Portability Act was passed in 1996 to regulate the use and disclosure of protected health information. HIPAA applies to any agency or “covered entity” in the business of creating, managing, or using protected health information, including firms providing support to covered entities.

**Sarbanes-Oxley** – Also known as the Public Accounting Reform and Investor Protection Act of 2002, the legislation was passed in the wake of the Enron scandal to clearly define the financial accounting reporting obligations of public companies. Of key interest to IT professionals is the requirement that the CEO and CFO attest to their companies having “proper internal controls”. Because most companies’ financial reporting integrity is tightly linked to the security of the IT system in general, and the financial application in particular, IT security is a key component of Sarbanes Oxley compliance.

**Gramm-Leach-Bliley Act** – GLB was Passed in 1999 to open up competition between banks and other financial institutions. With respect to Security, GLBA defined requirements for these institutions to protect customer information. GLBA compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

**PCI DSS** – The Payment Card Industry Data Security Standard was developed by the major credit card companies to help organizations that process credit cards reduce credit card fraud, cracking and other security vulnerabilities. The standard includes twelve requirements for compliance, organized into six logical groups called “control objectives”. Companies processing, storing, or transmitting payment card data must be PCI compliant or risk losing their ability to process credit card payments.

**CJIS** – The Criminal Justice Information Services division of the FBI serves as the focal point and central repository for criminal justice services in the FBI. Programs initially consolidated under the CJIS Division include the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), and Fingerprint Identification. CJIS Security Policy defines the measures law enforcement agencies, municipalities, and contractors must meet to be able to connect with the FBI’s systems.

Hierarchy Diagram:

- 1) FISMA – overriding legislation
  - a. Specified NIST as developer of standards
- 2) NIST – developed minimum standards (FIPS 200), categorization (FIPS 199), specific details (e.g. FIPS 197, FIPS 140-2) and guidelines for implementation SP-800
  - a. FIPS 200 – minimum security requirements
  - b. FIPS - 199 – categorization
  - c. SP 800-53 – guidelines for applying security controls (in particular see page 20 – sec 2.4 – security controls in external environments)
- 3) Additional specific security requirements in areas governed by other agencies
  - a. HIPAA
  - b. Sarbanes-Oxley
  - c. Gramm-Leach-Bliley

These statutes and organizations cover a tremendous range of security and privacy topics but they all have some key elements in common: categorizing data, systems, and processes that are covered by the legislation (or in the purview of the agencies), defining standards to make federal

and federally regulated information systems more secure, and defining metrics to determine ongoing compliance. The following table summarizes the relevant components of each piece of legislation. (Note: The table is focused on security issues related to the use of remote support and how that affects information systems security. It does not attempt to cover all of the security legislation or the details covered in the documents in the table.)

<b>FISMA</b>	
<b>Sec 301 and 302 – Information Security and Management of Information Technology</b>	
Sec 3541 - Purposes	<ol style="list-style-type: none"> <li>1) Provide comprehensive security framework</li> <li>2) Recognize highly networked nature of Federal computing environment</li> <li>3) Provide for development and maintenance of minimum security controls</li> </ol>
Sec 3542 – Definitions	Information Security – protecting information and information systems from unauthorized access, use, disclosure, disruption in order to provide: <ol style="list-style-type: none"> <li>a) Integrity</li> <li>b) Confidentiality</li> <li>c) Timely and reliable access</li> </ol>
Sec 3544 – Agency Responsibilities	Provide information security commensurate with the risk and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction.
Sec 11331 - Responsibilities for Federal information systems standards	Prescribe mandatory standards and guidelines on the basis of standards and guidelines developed by NIST
<b>Sec 303 - NIST</b>	
	<ol style="list-style-type: none"> <li>1) Develop standards, guidelines, an associated methods and techniques for information systems</li> <li>2) Categorize information and information systems for providing appropriate levels of security according to a range of risk levels</li> <li>3) Define minimum security requirements for each category</li> </ol>
<b>FIPS</b>	
FIPS 200	Mandatory minimum security requirements for Federal information and information systems including: <ol style="list-style-type: none"> <li>1) Access control</li> <li>2) Audit and accountability</li> <li>3) Identification and authentication</li> <li>4) System and communications protection</li> <li>5) System and information integrity</li> </ol>
FIPS 199	Standards for security categorization of Federal information and information systems: Low, Moderate, High
<b>NIST SP-800</b>	Recommended Security Controls for Federal Information Systems The guidance document and recommendations for picking security controls to meet FIPS 200.

	IA – 2 Identification and Authentication - The information system uniquely identifies and authenticates users (or processes acting on behalf of users).
	AU-2 Auditable Events - The information system generates audit records for the organization defined events. Compile audit records from multiple components throughout the system into a system wide, time-correlated audit trail.
	AU-3 Content of Audit Records - The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
	AC-17 Remote Access - The organization authorizes, monitors, and controls all methods of remote access to the information system. Automated mechanisms, cryptography, limited access points, privileged functions only.
	MA-4 Remote Maintenance - The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed. Audit all remote maintenance sessions, requires maintenance provider to have security at least the level of agency being supported.

<b>HIPAA - Health Insurance Portability and Accountability Act</b>	
	Access Control - § 164.312(a)(1) – Unique User Identification, emergency access procedure, automatic logoff, encryption and decryption
	Audit Controls - § 164.312(b) - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information
	Data Integrity - § 164.312(c)- Implement policies and procedures to protect electronic protected health information from improper alteration and destruction
	Transmission Security - § 164.312(e)(1) - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

<b>Sarbanes-Oxley – Public Company Accounting Reform and Investor Protection Act</b>	
	Section 302: Corporate Responsibility for Financial Reports- To ensure accurate financial disclosure, signing officers must certify that they are “responsible for internal controls” and “have evaluated the effectiveness of the internal controls as of a date within 90 days prior to the report” and “have presented in the report their conclusions about the effectiveness of their internal controls.
	Section 404 – Management Assessment of Internal Control - Requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting
	Section 409 – Real Time Issuer Disclosures - Requires publicly traded companies to promptly report any changes in financial condition or reporting that might be material to investors

<b>Gramm-Leach-Bliley – Financial Services Modernization Act</b>	
	Financial Privacy Rule - Provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer’s personal nonpublic information.  Safeguards Rule – Requires financial institutions to develop a written information security plan that describes how the company will protect clients’ nonpublic personal information.
12 CFR Part	Identification and Authentication – Financial institutions must have access controls on customer information systems, including controls to authenticate and permit access

208, Appendix D-2, II C(1)(a); 16 CFR Part 314	only to authorized individuals.  Overseeing Service Provider Arrangements – GLB requires financial institutions to oversee its service provider arrangements to (a) require its service providers to meet the objectives of GLB, and (b) monitor its service providers to confirm that they have satisfied their obligations.
--	---

<b>PCI DSS – Payment Card Industry Data Security Standard</b>	
2: Passwords	Do not use vendor supplied defaults for system passwords and other security parameters Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access
4: Transmission of Customer Data	Encrypt all transmissions of customer data over a public network Use strong cryptography and security protocols
7: Restrict Access	Restrict access by business need-to-know Limit access only to those individuals whose job requires such access Establish a mechanism for systems with multiple users that restricts access based on need-to-know and is set to deny all access unless specifically allowed
8: Unique ID	Assign a unique ID to each person with computer access Implement two-factor authentication for remote access Ensure proper user authentication for non-consumer users
10: Monitor Network Access	Track and monitor all access to network resources Establish a process for linking all access to system components to each individual user Implement automated assessment trails to reconstruct events Retain assessment trail history for at least one year, with a minimum of three months online availability

<b>CJIS – Criminal Justice Information Services</b>	
	VPN's <ol style="list-style-type: none"> <li>1) Implement VPN mechanisms using cryptography, key management, access control, authentication, and data integrity.</li> <li>2) Implement an authentication method using pre-shared keys or digital signature.</li> <li>3) At a minimum, a user shall be restricted from establishing a VPN session without first being authenticated by no less than a userid and password.</li> </ol> Encryption <ol style="list-style-type: none"> <li>1) All transmitted CJIS data shall be protected with a minimum of 128-bit encryption.</li> <li>2) After 2005, must meet FIPS 140-2</li> </ol>

### **Maintaining Security in a Remote Support Environment**

The economics of remote support are well understood. It is far less expensive and far timelier to remotely access a customer system over a network to provide support than it is to send technicians to the customer site. While deciding between on-site and remote support is simple for most businesses, those who have legislated security requirements must manage an additional set of issues. Specifically – a) Authentication – how to make sure the remote vendor accessing the system is who they claim to be, b) Restriction – limiting access to only those systems and activities required to perform support, and c) Audit – tracking, logging, and reporting the details of remote support sessions to be able to prove ongoing compliance with security policy. NIST SP

800-53 covers each of these issues in its guidelines and additionally identifies multiple levels of protection for remote access and support.

**Sidebar: NIST SP 800-53 – Recommended Security Controls for Federal Information Systems**

**Remote Access:**

The organization authorizes, monitors, and controls all methods of remote access to the information system. Additional levels of security (from low to moderate to high) require the following enhancements to the general guideline:

- 1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
- 2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.
- 3) The organization controls all remote accesses through a limited number of managed access control points.
- 4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

**Remote Support:**

The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

The general guideline is enhanced by the following additional controls:

- 1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.
- 2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.
- 3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement a level of security at least as high as that implemented on the system being serviced.

**SecureLink – Security for Remote Support**

SecureLink’s remote support network is the first system designed specifically to address the issues involved in managing remote support connections for security conscious agencies and enterprises. SecureLink includes a dedicated server for hosting the remote connection management platform and client software called a Gatekeeper for establishing and defining a secure remote connection from vendor sites. SecureLink server provides all the tools needed by the support technician to create and maintain remote support connections including:

- Support vendor lists
- Gatekeepers associated with each vendor
- Session history for each vendor

By consolidating connection types, application management and remote access from vendor systems onto a single platform, SecureLink greatly reduces the problem of tracking, auditing and reporting on remote support activities– all of the remote connection session data is in one place. Let’s review the specific ways SecureLink handles Authentication and Identification, Restriction, and Audit.

**Authentication and Identification**

SecureLink identifies and authenticates users in multiple ways. First, both sides of the remote access connection (the support technician and the agency) use a unique username and password

when establishing and accessing a connection for remote service. In addition, restrictive password requirements are enforced on the SecureLink server for all users.

### **Restriction and Access Control**

User authentication does not enable remote support connections to any system in the agency's environment however. With SecureLink, agency IT staff defines individual (or group) access to a specific server (or IP address), application, and capabilities that are enabled for support (read, write, file access, FTP, chat). Any remote support connection coming through the SecureLink server must be approved first by the agency (through the enabling of the Gatekeeper). Agencies have a great deal of flexibility and control to define Gatekeeper access:

Connectivity Settings - Access is either enabled or disabled. A remote connection can be made to the agency system only when the Gatekeeper access is enabled. Gatekeeper connection status can be managed in three ways: 1) on a defined schedule (day, date, hour), 2) disabled after an elapsed time access (within n hours), or 3) manually.

Encryption - Users can choose between several encryption options to secure the communications between SecureLink server and support vendor: 1) AES in 128, 192, and 256 bit modes – required to meet FIPS 140-2, 2) Triple-DES – required to meet FIPS 197, and 3) Blowfish.

Vendor Privileges - The services used by the support technician to diagnose and resolve software issues (FTP, shared desktop, command prompt) are included in the Gatekeeper and enabled (or disabled) by the agency. When configuring the Gatekeeper, agencies build an access list that contains hosts or IP addresses and ports the vendor is allowed to access. Using the Gatekeeper access list, the agency controls a) the host and ports accessible to the software vendor and b) the services available on those hosts.

One of the key security features in the SecureLink design is that the entity whose systems are accessed (and who has the obligation of protecting the data) defines and enforces the rules of remote access. Remote support connections are managed through the SecureLink server, but are enabled and defined by the Gatekeeper. The agency sets levels of security on the Gatekeeper, defines which systems can be accessed and what services are available to the support technician, and sets the schedule for remote access. The SecureLink Gatekeeper enables the establishment of a de facto security policy for remote support with minimal agency overhead (no code to write, no additional applications to integrate).

### **Audit**

SecureLink creates historical audit reports of each remote support session including detailed log files. The reports detail who accessed the system, when it was accessed, what parts were accessed, what was done (at the command level), and what tools were used.

Information recorded for each session includes:

- Session information and status
- Owner
- Registration code
- Creation date, completion date, session duration
- Which support technicians participated during the session
- What services the support technician accessed, what happened, and how long it took:
  - Start and end time of each activity
  - Telnet logs
  - Files transferred

- Bytes sent and received during desktop sharing
- Chat history

SecureLink makes the history of each remote connection session available to both the agency and the software vendor. Both the agency and the vendor have the detail they need to prove compliance.

### **Summary**

Legislation and business requirements have created a class of enterprises that must maintain a high level of security. This includes well defined processes for how systems are accessed by vendors providing remote support. When considering large numbers of customers and support technicians, and the variety of connectivity types, application versions, and hosting servers, the problem of managing remote support connections becomes immense and creates significant security risk.

Federal agencies and business that operate under Federal regulations must meet information system security requirements or risk losing accreditation, access to key government systems, or, in the most severe cases, criminal and civil penalties. Remote support is a fact of life for large information systems users, and it's critical that IT professionals find ways to manage remote access by support vendors that does not diminish the overall information security environment.

SecureLink manages complexity and enables security by providing a single platform from which to manage remote support connections. Multiple levels of identification and authentication, agency defined access and control, and detailed audit, reporting and real-time monitoring capability for every remote support session all work together to enable security process definition by the agency and to provide easily verifiable proof of compliance.

SecureLink Solutions Summary

## SecureLink Solution Summary

<b>Legislative Requirement</b>	<b>SecureLink Feature</b>
<b>FIPS 200</b>	
Access Control	Customer configurable Restrict access as to time, scope, function, and file. System or user level access rights Unilateral ability to terminate session at any time
Audit and Accountability	Detailed logging of each support connection session Complete historical reporting
Identification and Authentication	Multi-level authentication Both sides of connection must authenticate Unique username/password combination for all logins Unique randomly generated key for each connection
<b>FIPS 140-2, FIPS 197</b>	
Encrypted Communications	Customer configurable encryption AES in 128, 192, and 256 bit modes Triple DES. Meets FIPS certification #918.
<b>NIST SP-800</b>	
Identification and Authentication	Multi-level authentication Both sides of connection must authenticate Unique username/password combination for all logins Unique randomly generated key for each connection
Auditable Events	Detailed logging of each support connection session Complete historical reporting
Content of Audit Records	Session information and status Owner Registration code Creation date, completion date, session duration Which support technicians participated during the session What services the support technician accessed, what happened, and how long it took
Remote Maintenance	Authorization, monitoring, and control of all remote access for remote maintenance and diagnostic activity.
<b>HIPAA</b>	
Access Control, Unique user identification, automatic logoff	Multi-level authentication Unique username/password combination for all logins Restrict access as to time, scope, function, and file. System or user level access rights Unilateral ability to terminate session at any time Automatic logoff after 10 minutes of inactivity
Audit Controls	Detailed logging of each support connection session Complete historical reporting
Data Integrity	Strict control of remote access to limit support related data corruption Detailed audit to identify changes and enable corrections
Transmission Security	Customer configurable encryption AES in 128, 192, and 256 bit modes Triple DES

<b>Legislative Requirement</b>	<b>SecureLink Feature</b>
<b>Sarbanes-Oxley</b>	
Audit and Accountability, Management Assessment of Internal Controls	Detailed logging of each support connection session Complete historical reporting
<b>Gramm-Leach-Bliley</b>	
Identification and Authentication	Multi-level authentication Both sides of connection must authenticate Unique username/password combination for all logins Unique randomly generated key for each connection
Overseeing Service Provider Arrangements	Authorization, monitoring, and control of all remote access for remote maintenance and diagnostic activity Customer configurable remote access control Restrict access as to time, scope, function, and file. System or user level access rights Unilateral ability to terminate session at any time
<b>PCI DSS</b>	
Password Control	Unique username/password combination for all logins Unique randomly generated key for each connection
Secure Data Transmission	Customer configurable encryption AES in 128, 192, and 256 bit modes Triple DES
Unique ID	Multi-level authentication Both sides of connection must authenticate Unique username/password combination for all logins Unique randomly generated key for each connection
Monitor Network Access	Authorization, monitoring, and control of all remote access for remote maintenance and diagnostic activity Customer configurable remote access control Restrict access as to time, scope, function, and file. System or user level access rights Detailed logging of each support connection session Complete historical reporting