

## Regulatory Compliance in Provisioning for Secure Networks

*Regulations simply standardize sensible practices for securely storing, retrieving and transporting electronic information.*

### CONTENTS

Abstract	2
Meeting basic operational needs	2
Best practices	3
Mandatory compliance	3
The blended threat landscape	4
Assessing security needs	6
The letter of the law	8
Constant compliance	8
SonicWALL solutions for compliance	9
Summary	10

**Abstract:** *Network security compliance suggests a sea of regulations and paperwork. But the fact is regulations simply standardize sensible practices for securing, storing, retrieving and transporting electronic information.*

*The easiest way to understand regulatory compliance is to first understand the common elements of compliance and their origins in self-regulation and best practices. Compliance is not an end-state: the last checkmark on the final punch list. Rather, it is a process that will continue to shape how organizations operate and how they specify and provision information security solutions.*

*Regulations regarding information security actually date back to the very beginnings of the information age. These earliest regulations represent the organizing principles of information security. The objectives contained in those original regulations remain as a foundation and continue to guide today's policies.*

*With electronic information now occupying a central role in all administrative operations, it is inevitable that clear policy guidance in its management is required. It's this same central role that has also attracted the attention of malicious and criminal elements. Information managers can sometimes feel they are in the middle of a shadow battlefield, buffeted and sniped at by forces outside their view and beyond their control. Under these conditions, regulations can sometimes, mistakenly, be regarded purely as "orders" and compliance can be seen as "following orders".*

*But, perhaps a better perspective is to think of security regulations as a user's manual for information system managers to be applied in the course of action. This perspective frees managers to act on the unique specifics of their needs and circumstances, apply their good judgment in fashioning solutions, and use regulations to help guide execution.*

*Compliance can actually simplify the network provisioning process. Driven by economics and increased attention to service levels, the profile of networks and information systems has become more uniform across the public and private sectors. The explicit mandating of some criteria has clarified the evaluation process. In fact, the evaluation process itself related to security solutions has become more uniform to assure broader compatibility and to accelerate the process of compliance.*

*Understanding the broad forces at work—even before filling in the details—can enable anyone concerned with the security of information to more quickly and effectively achieve their ultimate goals for delivering excellence in service including maintaining public trust. These forces include: the context in which an institution operates, the nature of the threats they face, the applicability of various regulations in the course of addressing these threat, and principles for action moving forward.*

## Meeting Basic Operational Needs

Operational enterprises—private corporations and government—are organized in very similar ways: created by an enabling act and subject to the terms of a charter, bylaws and rules. Once established there is a day-to-day set of standard operating procedures or business practices, whether written down or not, which define how business is done and which include the processes for managing:

- Financial controls
- Physical facilities
- Contract obligations
- Assignment and delegation of authority
- Protection of intellectual property
- Procurements
- Employees and contractors
- Internal databases
- Voice and data networks

Collecting these standard operating procedures, business practices and methods of achieving business needs constitute self-regulation. They originate from necessity, even if subsequently proscribed by law or regulated by voluntary standards (such as ISO 9000) or by contract obligations (such as lending ratios or service level agreements).

## Best Practices

Within government and across every industry there arise some business practices which come to be generally appreciated as especially effective or prudent. An example is the custom of nurses taking written notes on the care of patients. At one time this concept was novel. Today it is customary everywhere. Practices such as this, which become common sense in a market and generally accepted, are referred to as “best practices.”

The significance of best practices is that they are often a source of substantive law attempting to set minimum standards. The policy community will often look to what people are already doing as a matter of common practice in defining what comes to be proscribed by law.

Examples of best practices may include generally accepted:

- Auditing standards
- Standards of corporate governance
- Standards of patient care
- Methods of contract compliance
- Methods of risk management
- Methods of quality assurance and process control

Most importantly, the ultimate mission of any organization is to serve a larger population. As information systems have brought new efficiencies to workflow, expectations for service levels have also increased. These expectations generally fall into two categories: increased speed and quality, and increased availability and “self-service” for the public being served. The drive to put business online has collided with the need for sound information security practices. Essentially, the issue is privacy.

Privacy is a central tenet in most transactions between individuals (including entities such as corporations that, under law, are treated as individuals). This principle applies even when the transactions are being conducted via electronic systems. Law and public policy affirm the right to have communication systems and content free from unauthorized access, interruption, delay or modification. This principle is at the root of all information security regulation.

## Mandatory Compliance

Mandatory compliance seeks to satisfy the various rules and regulations which are required by law. These include sources of international law, various state laws and law mandated by national government.

Examples from the U.S. experience include:

- The Federal Information Processing Standards (FIPS) which date back to the mid-1960's. Specific components of these standards have been added, revised or withdrawn repeatedly in the years since.
- The Privacy Act of 1974 which was enacted during a period of rapid increase in the amounts of private information stored in electronic systems.
- The Computer Security Act of 1987 which reaffirmed the role of the National Institute of Standards and Technology (NIST) as defining the security standards for protecting non-classified federal data. It established security baselines, required security planning by system owners and security awareness training for the operators of systems containing “sensitive information.”
- The E-Government Act (Public Law 107-347) of 2002 formally recognized the importance of information security to the national security interests of the United States. Title III of the E-Government Act—the Federal Information Security Management Act (FISMA)—requires each federal agency to develop a comprehensive program to secure the information and information systems that support their operations. FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security.

In addition, much regulation of corporate governance and private sector business affairs has information security ramifications. Well-known laws like Sarbanes-Oxley, Gramm-Leach-Bliley, the Electronic Signatures in Global and National Commerce (E-Sign) Act and HIPAA each have clear requirements regarding the secure handling of information which, inevitably, is in electronic form.

While government regulation is not the only factor in the particulars of compliance, it is a good compass for what is proper, adequate and justifiable. The regulations detail what information must be secured and what criteria need to be applied in evaluating prospective solutions. But they do not detail what threats need to be countered. To do that, you need to know the landscape of the threats.

## The Blended Threat Landscape

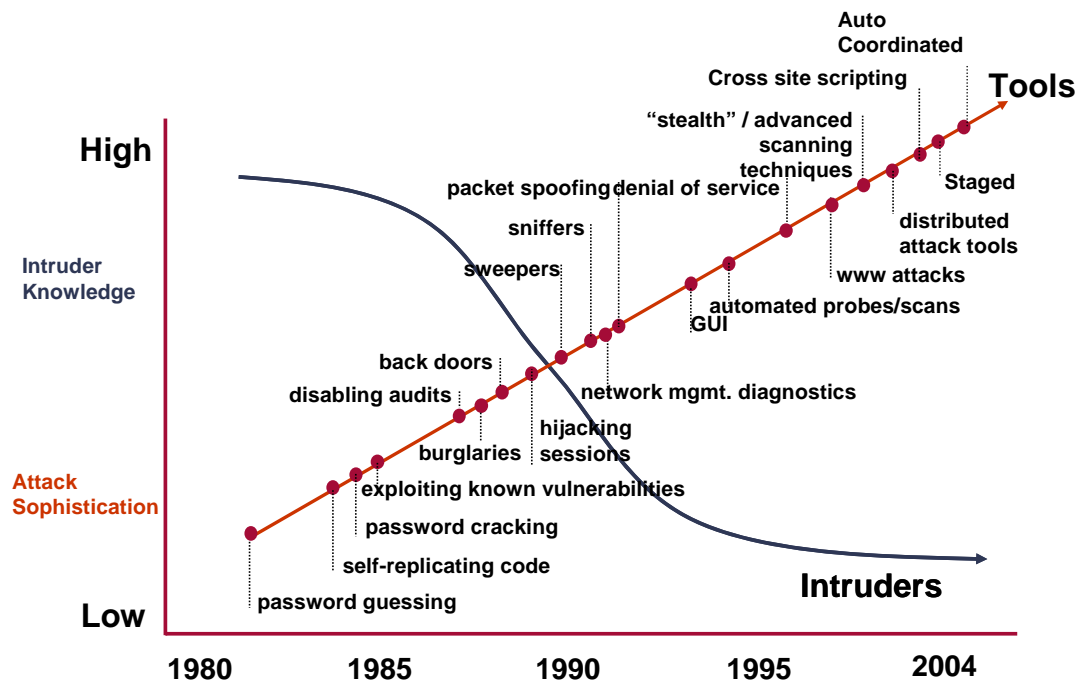
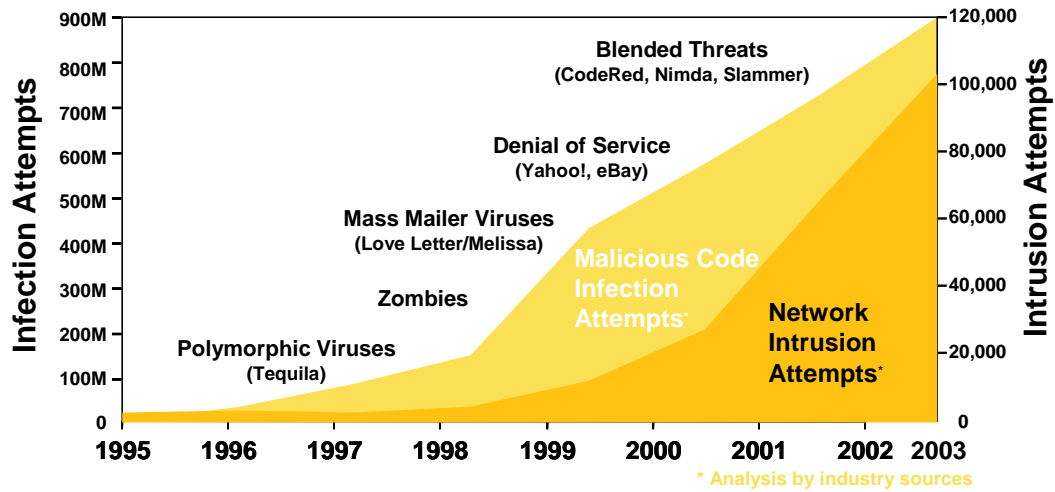
Attacks on internet systems have been on the rise, and continue to accelerate. Attacks are becoming automated as their frequency increases. Pranksters have been replaced by professionals who use the sophisticated attacks to engage in various forms of theft or fraud.

In May of 2005, the United States Government Accounting Office issued its assessment of emerging cybersecurity threats facing U.S. Federal government systems. Chief among these were spyware, spam and phishing. Of course, these threats are not unique to the U.S. Federal government.

- Spyware is a hybrid of viruses and hacking. In effect, it automates hacking—gaining surreptitious access to a computer to steal or corrupt information. At the same time it is related to adware, some of which has become an industry of its own for unscrupulous advertising companies. The result is a population of developers and an inventory of code that can produce new spyware at a furious rate.
- Spam represents two kinds of threats to information systems. The sheer volume of nuisance communications can be a drain on resources. And spam is a vehicle for a new category of threat: social engineering.
- While nuisance spam e-mail generally is trying to sell something, social engineering e-mail operates entirely on false pretenses, i.e. unsolicited letters pleading for help transferring money and requesting bank account information. More devious are phishing e-mails— fraudulently appearing to come from and link to a trusted source like a bank—which trick people into divulging passwords, personally identifiable or financially valuable information. These attacks are called “social engineering” because they depend on unsuspecting people behaving in a particular way in response to the message.

All these menaces have now come together in what is called blended threats. These are attacks using spam e-mail to deliver automated threats—viruses, spyware, bots (that secretly take control of infected machines), and more—under cleverly constructed false pretenses.

Figure 1 shows the emergence and convergence of these threats. Figure 2 shows how technology is increasingly being applied in their execution.



What all these facts together make clear is the threat landscape is increasingly complex, fluid and active. The good news is that by addressing these threats sensibly and vigorously, you will likely be coming into compliance with all the regulations relevant to your particular situation.

## Assessing Security Needs

A fair starting assumption is that all the information for which an organization is responsible is valuable. It is not to be corrupted, stolen, or misused. The foundational principles of network security then are relatively straightforward:

- 1) Policy management – Ensure that the permissions and rights for access and use are defined, documented and managed accordingly.
- 2) Access control – Ensure that access to records, facilities and systems are in accordance with policy and that identity is authenticated when accessing sensitive information
- 3) Integrity of communications – Ensure that systems are reliable and not subject to alteration, or their content is not subject to unauthorized intrusion, monitoring or modification.
- 4) Integrity of records – Ensure that records are reliable, can be authenticated as genuine and are maintained without alteration in any records management systems
- 5) Audit Trails – Ensure that access to archival and sensitive records and systems can be accounted for and that any attempts to monitor, alter, erase or tamper with them can be detected promptly to prevent loss and can be traced to the actual person or persons responsible

Here are the how these issues can be addressed:

Issue	Method of Compliance
Policy Management	Automatic policy enforcement for clients and networks
Access Control	Secure remote access with authentication over SSL-VPN and IPSec VPN
Integrity of Traffic	Wired / Wireless: content filtering and unified threat management
Integrity of Records	Continuous data protection of records
Audit Trails	Live and historical event reporting and monitoring

The process of actually coming into compliance impacts every aspect of network architecture and operations. Regardless of the applicable regulations—federal, state, local or industry self-regulation—by securing the networks in a way that assures the integrity of your organization’s mission, you will likely satisfy the relevant regulations.

Specifying that security solution can be achieved with a simple four-step process:

### Process Audit

Compare the organization’s priorities to current security policies. Talk to managers to identify which systems they feel are essential to support operations and if they have any concerns about those systems. Review the policies and procedures already in place for those systems and data. This will help you isolate the relevant regulations in crafting a solution.

### Infrastructure Audit

Locate all the devices and systems on the network, including mobile devices and the systems of “outside” entities that may have access to the network via an intranet or VPN. Prioritize them according to which assets are most vital to the agency.

## **Risk Assessment**

The extent of compliance is almost always gauged by the security measures taken relative to the degree of risk. This involves the likelihood of a particular kind of attack or exploitation factored by its impact on the agency's fulfillment of its mission.

For a useful reference, the "20 Most Critical Internet Security Vulnerabilities" has been produced by the SANS Institute ([www.sans.org](http://www.sans.org)) and the FBI. The majority of successful security breaches target one or more of the vulnerabilities on this list. "The 10 Most Critical Web Application Security Vulnerabilities" has been produced by the Open Web Application Security Project ([www.owasp.org](http://www.owasp.org)). It describes common vulnerabilities for Web applications and databases and the most effective ways to address them.

## **Solution Review**

In crafting a solution, you can begin to address particulars of compliance: the policies and goals that are to be addressed. Again, the technical aspects of compliance tend to be common-sensical:

- Identity management for authenticating and auditing access
- VPNs and firewalls securing every location on the network
- VLANs to secure groups and isolating attacks
- Monitoring and reporting tools to identify attacks, respond to them and perform forensics on the incident

For purposes of this document, we've focused on Internet Protocol (IP) networks. To assess the defensibility of an IP network, consider its component layers:

- The Application Layer sends and receives data for particular applications, such as Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). Defending this layer provides protection at the most fundamental level.
- The Transport Layer provides services for transporting application layer services between networks utilizing Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Controls at this layer can be used to protect the data in each active session.
- The Network Layer routes packets across networks. In addition to IP, this network layer might employ Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). Controls at this layer apply to all applications. Network layer controls give network administrators a way to execute and enforce security policies. And, since IP addresses are added at this layer, the controls can protect both the data within the packets and the IP information for each packet.
- The Data Link Layer handles communications on the physical network components, frequently via the Ethernet protocol. An Internet-based connection will usually represent several physical links chained together. This is the last possible line of defense.

These layers represent the "membrane" that allows administrators to intercept network activity, inspect it and evaluate the compliance of that activity with policy. By focusing on the primary points at which information can be secured, you can quickly make major strides toward securing that data and doing so in a way that complies with all relevant regulations.

## The Letter of the Law

Regulations have been promulgated to guide provisioning for three main categories of information security: Procurement (equipment must meet certain levels and kinds of capability to harden the network infrastructure), Data Security (the data itself must be safely stored and transported) and Document Retention (information must be preserved intact for purposes of audit).

There are currently over 10,000 U.S. federal, state, and local laws and regulations addressing what, how, when and why records must be created, stored, accessed, maintained and retained over increasingly longer periods of time. This doesn't include the regulations of private sector organizations such as the National Association of Securities Dealers or the New York Stock Exchange. These criteria can impose themselves in unexpected ways. For instance, law enforcement officials dealing with a matter of public health are bound by HIPAA regulations regarding record-keeping. Public utilities may be required to comply with FERC security standards in managing some of their information.

While FISMA lays out the required elements of security programs, it doesn't set the benchmarks. The National Institute of Standards and Technology (NIST) supports FISMA by providing guidance and best security practices to government agencies at all levels. Security accreditation for federal implementations, which is required under OMB Circular A-130, provides a form of quality control in execution of NIST recommendations. This accreditation reflects an evaluation of the most effective security controls and techniques possible, given technical constraints, operational constraints, cost and schedule constraints and mission requirements.

While the operational needs of the Federal government are unique to it in many ways, as has been pointed out earlier there is much that makes them the same as those for private business. Regulatory compliance can therefore be a useful surrogate for a whole series of selecting practices that produce a short-list of viable solutions.

## Constant Compliance

Once an information system has been brought into compliance, it needs to be kept there. Changes in compliance requirements tend to come from plugging holes or from the changing nature of threats. Regardless of the legal details, no network administrator wants to fall victim to vulnerability beyond their control.

Many network technology managers are keeping pace with threat signatures and system configuration changes to thwart threats of all kinds by the practice of vulnerability management. This involves a mix of security tools, policies and procedures. NIST will soon publish a draft of a new document that will mandate a set of no fewer than 17 controls that each government agency will have to apply to each of their major applications and general support systems. These controls are based on how critical different systems are to an agency's mission. This same value equation can be applied to systems of all kinds.

The threat dynamic requires more than hardware or software of a certain specification. As the characteristics of attacks change, the systems and procedures to counter them will change as well. At a certain point, these procedures may be codified in a policy or a mandate with which IT management must comply. In this light, security provisioning can be seen as building a compliance platform. It must be adaptable and upgradeable. It may not even be a purchase at all, but a service offering that can change and evolve as required.

## SonicWALL Solutions for Compliance

As a market leader in Internet security solutions, SonicWALL is dedicated to serving the security needs of organizations of all kinds. Offering both appliance-based products and value-added security subscriptions, SonicWALL can deliver the kind of protection needed to counter multiple security threats including blended threats. Subscriptions include Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Complete Anti-Virus, Content Filtering Service and an award winning management and reporting software.

Understanding the importance of compliancy issues, SonicWALL works closely with the U.S. National Institute of Standards and Technologies (NIST). In fact, a number of its firewall/VPN appliances, including the TZ 170 and PRO 3060, have received Federal Information Processing Standard (FIPS) 140-2 Level 2 certification. Additional products are also under evaluation for certification. FIPS 140-2 is required for cryptography related products in use by federal government agencies.

A heightened sense of security coupled with continuous budgetary constraint is leading many organizations to seek comprehensive multifunction security solutions that are both affordable and easy to implement. SonicWALL offers fully integrated and competitively priced bundles designed especially to meet such needs:

Issue	Solutions from SonicWALL	
	Method	Products
Policy Management	Automatic policy enforcement for clients and networks	Global Security Client Global Management System (GMS)
Access Control	Secure remote access with authentication	IPSec VPN , SSL-VPN
Integrity of Traffic	Wired/Wireless: content filtering and unified threat management	UTM , CSM 2100 Secure Distributed Wireless
Integrity of Records	Continuous data protection of records	Lasso CDP
Audit Trails	Live and historical event reporting and monitoring	GMS / ViewPoint

### Unified Threat Management (UTM)

The SonicWALL complete UTM solution provides intelligent, real-time network protection against sophisticated application-layer and content-based attacks. Comprising Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, its solution flushes out both internal and external threats by addressing multiple threat access points and thoroughly scanning all network layers. Utilizing a high-performance, deep packet inspection engine, SonicWALL delivers threat protection directly on the security gateway by scanning against multiple application types and protocols and by matching files against an extensive signature database.

Many solutions utilize a firewall architecture known as stateful packet inspection, which works primarily at the network layer to determine whether data packets were requested and should be allowed onto the network. This approach permits selective but flexible access from outside the network and relatively unrestricted transmission from within. Given that many viruses originate from within an organization's e-mail service, it's clear that numerous threats will bypass the stateful level of protection.

SonicWALL employs a comprehensive method known as deep packet inspection (DPI), which matches downloaded, e-mailed, and compressed files against an extensive and continuously updated signature database. The SonicALERT team and third party sources develop the database signatures, which scan in real time to detect and block packed executables and macro virus files.

With DPI technology, SonicWALL solutions examine information at the application layer and defend against attacks targeting application vulnerabilities. The SonicWALL DPI engine scans against multiple application types and protocols including SMTP, POP3, IMAP, FTP, HTTP, NetBIOS, dozens of other stream-based protocols, and over 50 application types for IDP. The SonicWALL engine scans all network layers including Link, IP, TCP/UDP, Static Port, Dynamic Port, and Application—so your remote site gateway, internal network, file downloads, server, and desktop are all protected. As an added layer of security, SonicWALL protects the application layer from internal as well as external threats.

## Summary

Complying with the many regulations regarding information security doesn't have to be as daunting as it seems. It's probably the last thing you want to think about. And, in a way, it can be. In fact, the applicable regulations for your particular circumstances can probably be addressed in the course of your normal decision and implementation processes for network provisioning:

- Articulate the mission of your organization
- Identify the information needs that fulfill the mission
- Specify the systems that satisfy your information needs
- Identify the points in your systems where vulnerabilities should be addressed
- Specify the solution for each vulnerability
- Correlate your solutions to the relevant regulations

At this point, you will probably find yourself in compliance. There may be some special requirements—say, for record-keeping or interoperability—that will require additional work. But, if you have applied best practices in addressing the fundamentals, you should have a suitable platform for any industry-specific compliance issues that arise.

Just as important, you will have a platform for ongoing compliance. As the regulations—and the threats they seek to address—continue to evolve, you should have nothing to fear...from the bad guys or the regulators.