



IPSWITCH FILE TRANSFER WHITE PAPER

# Supporting FISMA and NIST SP 800-53 with Secure Managed File Transfer

Adherence to United States government security standards can be complex to plan and implement. There are a number of standards that the implementer must become familiar with. Many of them are subjective and open to interpretation, further complicating matters. Most U.S. federal government agencies and departments are required by law to adhere to these standards and are audited regularly for compliance.

The Federal Information Security Management Act of 2002 (FISMA) is the principal law that defines federal security requirements. FISMA was enacted as Title III of the E-Government Act of 2002. It acts as an “umbrella” law that enforces a number of processes and standards which assess, categorize, secure, and audit information systems. An important component of understanding FISMA is the *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 describes how to categorize information systems and calculate the resulting level of security applied to them. That calculation uses the following formula:

$$SC_{\text{information system}} = \{(confidentiality, impact), (integrity, impact), (availability, impact)\}$$

The resultant security category (SC) defines the security controls that must be implemented. The possible values for impact are labeled as low, moderate, and high, and they indicate *potential impact*. FIPS 199 labels confidentiality, integrity, and availability as *security objectives* which are important constructs to be discussed later in this paper. Note that the value for SC is the highest value of any component, and as such is commonly called the high water mark. In other words, the highest security objective rating defines the security category regardless of the other ratings.

Because this formula uses relative and subjective values to classify information systems, planning is truly the key to doing it correctly. Planning allows appropriate time for all participants to come to agreement on the security category of an information system. Once agreement is in place, specific standards then define the minimum security controls necessary for the information system. Those standards are based on seventeen security-related areas, which are chiefly contained in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems*.

Implementing the appropriate security controls as defined in NIST SP 800-53 can be daunting. File transfer solutions are particularly complex, as files used within such systems often retain their classification both during and after the transfer.

That means that the transfer itself must also adhere to the NIST SP 800-53 requirements. This paper explores the details around securing and managing file transfer while maintaining the appropriate level of FISMA compliance.



# Securing and Managing File Transfer

File transfer has a set of unique considerations. When the files move between systems they must be properly managed to ensure compliance with all systems involved. For example, imagine a cross-department working group. They collaborate by working on a shared set of files. Each member of the working group must access the files from their computer. This means that the file transfer must adhere to the SC for the data and all participating systems, while maintaining the high water mark level of compliance.

There are a number of factors that play into the security considerations of file transfer. Depending on the SC level these may include:

## Data Encryption Type and Strength

The files must be protected during transfer. The type of encryption will vary, including algorithm, key size, and key type, depending on the data classification of the file. Again, the high water mark principle applies here, so when a single file transfer contains files with multiple classifications, the transfer must adhere to the highest standard.

## Accessibility to Intended Users

Files being transferred must be accessible to all intended users and systems. The transfer could take place between disparate systems such as from a Unix source to a Linux or Windows client. This complexity in interconnected systems requires the authentication and authorization techniques to be NIST compliant. At the same time they must be flexible enough to support federated or non-native user credentials.

## Enforcement of Data Containment Policy

Any file transfer solution in an agency must enforce the data containment policy of that agency. These vary widely based on variables including the agency, the file transfer needs, and so on. While technical controls can be applied to specific file sets and communication channels, it is the overall data containment policy that requires adherence and is audited for conformity to FISMA.

## Creation of Audit Records

Regular audits are a core component of federal regulation requirements that help verify compliance to laws and policies. In most cases the applicable data classification requires a thorough auditing of all file transfer operations. Although not required at all levels, providing an audit trail for file transfers assists in a number of ways. For example, when a data leak occurs, the audit records can be examined by an investigator to determine where and when the file was transferred, what level of authentication was provided, when the file was accessed, and so on. Audit records and resulting processes directly help in identifying the culprit and in resolving any core security problems that led to the leak.



Beyond the specific regulatory requirements, there are administrative options to consider whenever an administrator is considering a new IT implementation. These include:

### Ease of Administration for Servers and Clients

There's a maxim that "the enemy of security is complexity". This is very applicable to information systems which comply with a myriad of regulations and laws. File transfer has the potential to make the system even more complex as files move between computers, between agencies, and ultimately between security controls. To ensure that the information system remains manageable the solutions and controls should be easy to use and easy to administer. That means implementing solutions that provide tools and techniques that both implement the required level of security while also doing it in an unobtrusive manner.

### Process Automation

Another frequent compliance concern relates to process implementation. Simply put, people are fallible and mistakes are often the result of human error. When considered in the light of the last section's complexity maxim, the likelihood of human mistakes causing a breach of compliance are greatly increased. In fact, many of today's data security breaches are a direct or indirect result of human missteps. The recommendation to automate processes is repeated throughout both FIPS and NIST content as a best practice in reducing exactly this human risk.

Fully automating file transfer operations can be challenging due to their diverse nature. This type of automation usually requires robust tools that integrate with the security controls already in place. The tools can help simplify the process and ensure compliance, often identifying and mitigating risks that humans might not identify. Although file transfer automation can be involved during setup, the resultant level of reliability is often well worth the investment.

### Training and Support Costs

In line with the previous two considerations are the costs of training staff on a new managed file transfer solution while also supporting it once implemented. Numerous studies indicate that users who do not understand or agree with a security control either ignore or work around it. Such behavior defeats the purpose of the solution and often causes a breach of compliance. When considered in the light of FISMA, it also means legal liability for the violator and his agency.

Training and support costs can vary depending on the staff but are usually significant. Realistically, they are also often the most difficult cost to justify in a security solution. One way to mitigate the risk of not training staff is to use the simplest, most transparent, and most robust solution possible. Most engineers don't consider simplicity when identifying solutions, but it is a core contributor to the success of the solution.



# Creating a Secure and Managed File Transfer Solution

Specific tasks must be completed to create a file transfer solution that complies with FISMA and NIST SP 800-53. The tasks can be summarized as, in order:

1. Classify the security requirements of the information system using the process described in FIPS 199 and supporting standards.
2. Select a solution that meets the defined functionality and provides adequate security controls as described by NIST SP 800-53.
3. Implement the solution.
4. Verify the solution's compliance with functionality and security requirements.
5. Ongoing auditing of the solution's operation.

Navigating through these steps can consume a substantial amount of effort, matching regulation requirements to solution features. Alternatively, working with solutions which have been designed with compliance in mind can significantly streamline fulfilling these tasks. NIST 800-53 defines a number of control families that can and should be enforced by your selected solutions. Each of these families contains a set of controls along with three levels of security (low, medium, high) that further restrict or relax the security requirements of the control.

Solutions like those from Ipswitch include capabilities which map to these 800-53 control families. A few feature highlights that most organizations need in their compliance efforts include:

- Auditing of file transfer operations
- Data protection during the transfer process
- Server and client file transfer protection

The most thorough way to examine the benefits of your chosen solution is by looking at each control group within the context of your secure and managed file transfer requirements. For each control family below you'll see a few key controls whose implementation is greatly simplified by Ipswitch's file transfer solutions.



## Access Control

This family addresses the enforcement of access to specific data. Some key controls include:

- **Account Management** - Integrate with existing access control mechanisms and support access auditing
- **Access Enforcement** - Enforce approved authorizations for access to the files
- **Information Flow Enforcement** - Enforce policy adherence of data flow between systems
- **Least Privilege** - Limit user access to the minimum necessary to accomplish assigned tasks
- **Remote Access** - Enforces remote connection requirements to limit data access
- **User-Based Collaboration and Information Sharing** - Ensures that peer-based file sharing continues to meet data security requirements

## Awareness and Training

Information system managers must ensure that administrators and users are properly trained.

- **Security Training** - Provide security training. Simpler and well-managed systems require less training.

## Audit and Accountability

All information systems that implement NIST SP 800-53 must provably maintain security with regular and continuous auditing.

- **Auditable Events** - Creating appropriate audit entries when actions of interest (e.g. a file is transferred or accessed) occur
- **Content of Audit Records** - Record enough details of each auditable transaction to satisfy the requirement of each control
- **Audit Review, Analysis, and Reporting** - Review audit information periodically and report actions. This task is simpler in automated systems with centralized auditing
- **Non-Repudiation** - Protects audit information to ensure that an individual cannot deny performing an audited action
- **Audit Generation** - Allows audits to compile data across system-wide sources to correlate events

## Security Assessment and Authorization

Systems must be analyzed before they carry secure information.

- **Information System Connections** - Authorizes, monitors, and documents connections between information systems to assure security requirement adherence



## Configuration Management

Once a system is assessed as meeting other secure requirements, any change can alter that security. Configuration Management controls help avoid lowering security by managing changes.

- **Baseline Configuration** - Defines the components of an information system and their configuration, including a deny-all, permit-by-exception authorization policy
- **Access Restrictions for Change** - Automated enforcement of access restrictions and identification of changes to restrictions
- **Least Functionality** - The information system and components provide the least functionality necessary to meet defined requirements

## Contingency Planning

Data loss and compromise incidents are possible in all systems, and plans must be in place to recover from such incidents.

- **Information System Backup** - Backs up and tests data in a separate facility
- **Information System Recovery and Reconstitution** - Ensures that files can be recovered and reconstituted after a disruption, compromise, or failure

## Identification and Authorization

In all access controlled systems, users must provide their identity before being permitted to access secured assets.

- **Identification and Authorization (Organizational Users)** - Uniquely identify users and assign access to files based on the authentication. Note that this requirement is very broad and is covered by a number of supplemental standards including FIPS 201 and NIST SP 800-73, 800-76, and 800-78.
- **Device Identification and Authorization** - Uniquely identify devices (e.g. computers) and assign access to files based on the authentication.

## System and Services Acquisition

Organizational changes often include acquiring assets that may not adhere to mandatory security requirements.

- **Acquisitions** - Requires documented security requirements for acquired data
- **Information Systems Documentation** - Documents security requirements for acquired data
- **Developer Configuration Management** - Requires documentation of configuration management process during software development and that developers provide information to facilitate security verification
- **Developer Security Testing** - Requires software developers to verify software compliance with established security controls including authentication and authorization
- **Supply Chain Protection** - Requires a secure acquisition and validation process when purchasing system components



## System and Communications Protection

Data security must be implemented consistently when data is both transmitted and stored.

- **Security Function Isolation** - Security functions remain separate from non-security functions and ensures boundaries between all functions
- **Information in Shared Resources** - Stops unauthorized data access that can occur when reusing shared system resources
- **Boundary Protection** - Connects to other systems consistent with security requirements
- **Transmission Integrity** - Maintains file integrity during transfer
- **Transmission Confidentiality** - Protects file contents against unauthorized disclosure during transmission
- **Use of Cryptography** - Implements required standard cryptographic modules
- **Confidentiality of Information at Rest** - Protect confidentiality of data while stored locally

## Finding the Right File Transfer Solution Means Finding a Compliant File Transfer Solution

All U.S. federal agencies are impacted by FISMA to some degree. It can be a daunting task to implement and ensure compliance. There are numerous benefits, most notably a provably secure state based on accepted standards. Plus, ensuring compliance keeps you and your agency leadership compliant and defensible when subjected to audits and regulatory inspections.

The most effective way to implement FISMA compliance requirements for file transfers is by using solutions that meet the needs outlined in this paper. One that helps with these requirements is the Ipswitch suite of managed and secure file transfer products. Because the Ipswitch line helps provide and maintain compliance with FISMA through NIST SP 800-53, and uses FIPS 140-2 compliant cryptography, it can greatly simplify any agency's compliance efforts.

Ipswitch File Transfer provides solutions that move, govern and secure business information between employees, business partners and customers. The company's proven solutions lead the industry in terms of ease of use, allowing companies of all sizes to take control of their sensitive and vital information and improve the speed of information flow. Ipswitch lets business and IT managers govern data transfers and file sharing with confidence and enable compliance by balancing the need for end user simplicity with the visibility and control required by IT. Ipswitch File Transfer solutions are trusted by thousands of organizations worldwide, including more than 90% of the Fortune 1000, government agencies, and millions of prosumers. For more information on Ipswitch File Transfer and its products, go to [www.IpswitchFT.com](http://www.IpswitchFT.com).

