White Paper

FISMA COMPLIANCE
UNDER MULTIPLE CONTRACTS

Prepared by
BSC Systems Incorporated
14340 Sullyfield Circle, Suite 250
Chantilly, Virginia 20151

10 September 2015

INTRODUCTION

The Federal Information Security Management Act (FISMA) [1] and its associated security control requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [2] were conceived to protect sensitive information within a well-defined, though possibly large and complex, set of computing and communications resources. FISMA is imposed on organizations that store, process and/or transmit information that a Federal Agency designates as sensitive.

However, many organizations hold multiple contracts that require differing levels of FISMA compliance. Often, these contracts specify security requirements over and above NIST SP 800-53 control requirements. This white paper proposes a method to manage an organization's security control infrastructure over a variety of contracts. The goal is to exercise effective control with maximum efficiency.

THE PROBLEM

When an organization is standing up a new FISMA-compliant security program, the first order of business is to determine the level of information sensitivity using the Federal Information Processing Standard (FIPS) 199 [3]. The organization rates the information as low, moderate, or high impact for each of the three tenants of security: Confidentiality, Integrity, and Availability. A single sensitivity level is calculated as the highest ranking for any of the ratings. This single sensitivity level is then used to determine which of the NIST SP 800-53 controls will apply to the application.

> As an aside, many organizations deliberately over-rate the sensitivity of their data thinking that is prudent. However, this can lead to excessive and continuing costs. You can explore this further by checking the BLOGs at www.passfisma.com.

Another critical early task is to determine the "Accreditation Boundary" (AB) which serves to limit the scope of the FISMA effort by excluding elements of the network that will not "touch" the sensitive information.

Here are the challenges for multi-contract organizations.

1. Different contracts will involve information at different sensitivity levels. For example, suppose that Organization A holds 20 contracts that impose FISMA. The FIPS 199 exercises show that 19 are rated "low" sensitivity while only one is rated "moderate'. Organization A is faced with the prospect of raising its entire security program to the moderate level by implementing 44 *additional* 800-53 controls across its operation.

2. When Organization A wins a new contract, it must determine the impact on its existing AB. Ideally, there is no impact as the information for the new contract either already exists at Organization A or can be stored/processed/transmitted using resources that are already accredited under the current FISMA program. Often, however, this is not the case and the organization must decide whether and how it needs to isolate the new information and either

extend the existing AB or draw a non-contiguous AB around it. The latter approach, of course, assumes that the existing resources can be feasibly reconfigured to isolate the new information.

And then there is the ever growing popularity of the "cloud" and the virtualization of hardware, software and data. Although that consideration is beyond the scope of this white paper, suffice it to say that the Cloud Service Provider (CSP) must be compliant under the Federal Risk and Authorization Management Program (FedRAMP).

Sometimes, a contract will impose security control requirements that are either over-and-above the NIST SP 800-53 or just different from them. We will refer to these as "Special Controls" (SC). The challenge is to incorporate these controls into the organization's FISMA program without major disruption and in such a way that they can be validated to meet the contractual requirements and demonstrated as such to auditors.

AN APPROACH

We propose the discipline of Configuration Management (CM) to organize and control the security requirements from multiple contracts. The most important benefit of CM is the precise knowledge of the current state of resources and the ability to control changes to those resources in a rigorous manner. Central to the CM discipline is the concept of "baselines". A baseline is a formally documented state which has been approved by a recognized authority. For our purposes, there are two obvious families of baselines: the Security Program and the contracts. Once established, the Security Program baseline should only be changed by a formal approval process normally defined by a Configuration Management Plan [4]. The contracts baseline is established upon signature of both parties to the contract and can only be changed by a process defined in the contract.

For both baselines, it is important to have a taxonomy of the detail requirements so that contractual requirements can be traced to security artifacts. For a FISMA-compliant Security Program, the overarching artifact is the System Security Plan (SSP) [5]. Each control detailed in the SSP should be tagged with the corresponding control number contained in NIST SP 800-53. For example, the SSP IR-6 would describe how the organization meets the SP 800-53 control requirement IR-6, Incident Reporting. The SSP numbering scheme can be extended where appropriate to include or reference multiple artifacts that, taken together, meet the NIST control. For example, SSP IR-6.1 might describe how incidents are reported within the IT department while SSP IR-6.2 might contain a *reference* to the organization's overall public relations/communications policy rather than repeating that policy in the SSP. The objective would be to eliminate redundancy. We will use the acronym SSPCN to designate a SSP Control Number.

In addition to the SSP, NIST SP 800-53 requires additional artifacts such as the Incident Response Policy, Contingency Plan, etc. However, all of these artifacts can be referenced from the SSP. Thus the SSP should be considered at the top of a "cascade" of security-implementing artifacts that are the separate purview of IT, Human Resources, Training, and other departments.

Another feature of the SSP is a series of annexes. If a particular contract calls for Special Controls over and above NIST SP 800-53 Rev 4, then there should be an SSP annex that defines how these special requirements will be met. There would be one annex for each such contract.

Each contract will have its own baseline. However, a consistent taxonomy should be used for all contracts. If the contract's security-related requirements already have numbers, then those should be used but pre-pended with an alpha numeric that identifies the specific contract.

Now that we have the SSP and contracts baselines, there must be a way to trace between them. This has multiple purposes:

1. To demonstrate that all contractual requirements are covered by formal security policies and procedures;

2. To assess the impacts on the SSP of a new contract or a contract modification that changes the security requirements; and,

3. To support the formal CM change control process.

Now, even though our SSP baseline is monolithic, there are multiple contracts and therefore multiple contract baselines. Therefore, to achieve this link while minimizing redundancy, another abstraction is required. We shall designate this as the Protection Metadata (PM) as shown in Figure 1 below.

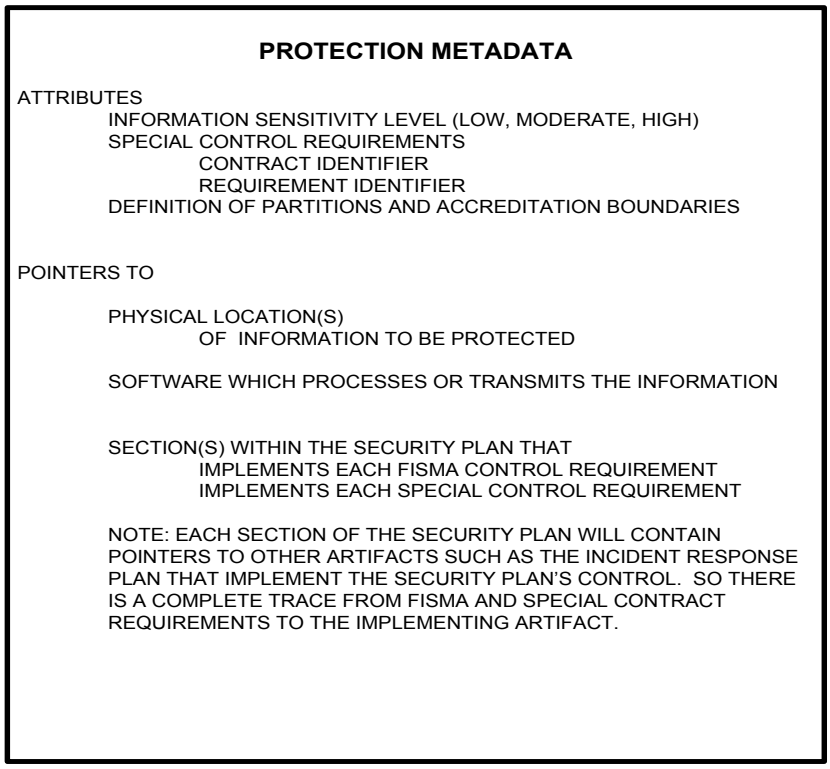

Figure 1 – Protection Metadata

There should be at least one PM for each sensitivity level handled by the organization. For example, if the organization has both low and moderate impact levels, then there should be separate PMs for each. Beyond that, additional PMs can be established for contracts that have unique security requirements

that require special security processes or resources. However, creating additional PMs should be applied judiciously.

PMs can also be used to manage accreditation boundaries. For example, if two or more contracts require the same sensitive information and, if permitted by the contracts, the organization can store single instances of this information on a common device, thus saving resources and eliminating redundancy. In this case, a single AB can be established and the same certification and accreditation package can be used for all such contracts. However, if there is a contractual or other reason for separating a subset of the data, this can be accomplished by establishing an accreditation "island" for that subset. This situation is documented in the PM including the physical and logical security information required to manage the archipelago. Also, the PM would point to the SSP Annex that defines the policies and procedures required to meet the contract's special security requirements.

PM entries should also be identified by a unique taxonomy to allow tracing as shown in Figure 2 below. Each PM should also be baselined and CM controlled.

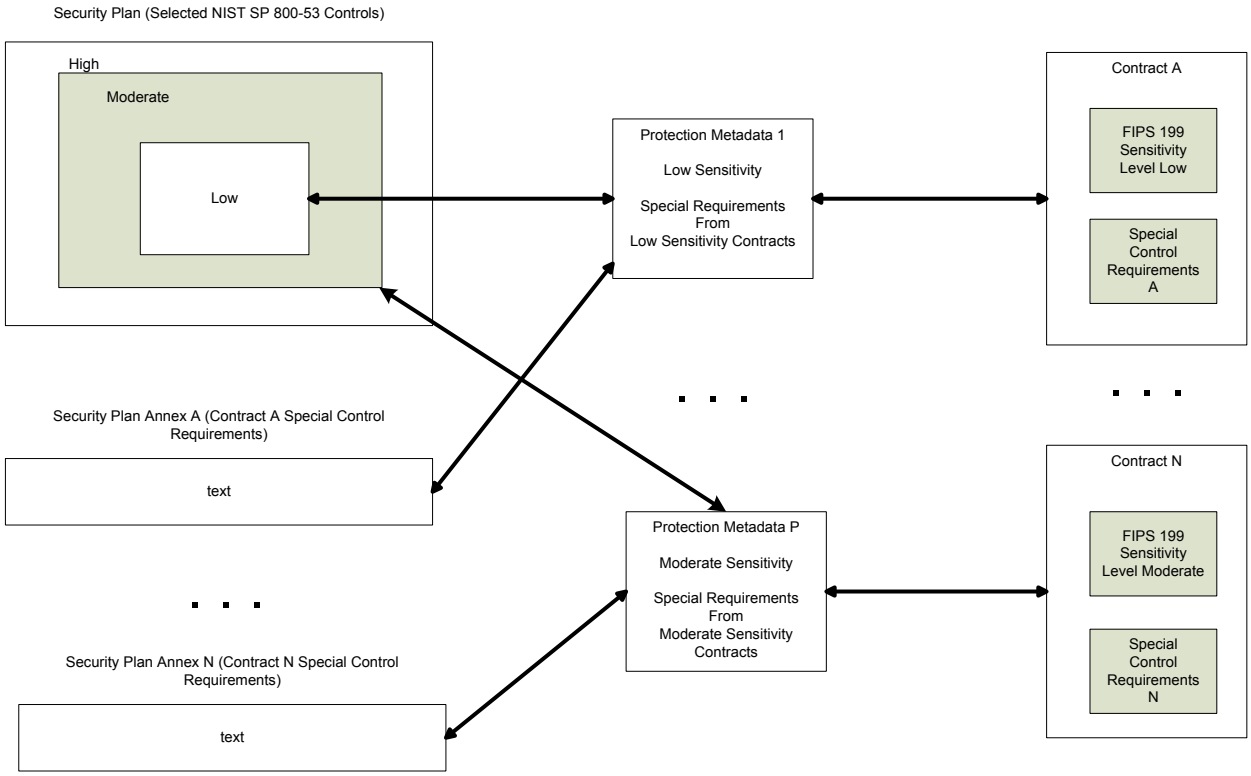

Figure 2 – Example Mapping of Contract Requirements to the SSP via the PMs

The PM should be viewed as a malleable device which should be adapted to each organization's situation. The discussion above is just one example of the concept.

Special controls that are documented in an SPP Annex should be pre-pended with an alphanumeric that identifies the corresponding contract. Then, these new links should be added to the appropriate PM or

a new PM established if this is more efficient in establishing the trace. Naturally, all changes must follow the CM process.

When a new contract/subcontract is received, the organization should immediately establish the data sensitivity using FIPS 199 [3] and analyze and tag any special control requirements that are not covered by NIST SP 800-53. Then, as necessary, the SSP and PMs should be revised as discussed above.

AUTOMATION

The proposed approach enables the application of an automated tool to manage the multiple contract security environment. For example, the tool can:

1. Trace the security requirements from each contract to the corresponding sections of the SSP as well as the cascaded subordinate artifacts;

2. Assist in identifying any gaps;

3. Assist in determining which PM is applicable to new requirements or if a new PM is needed; and,

4. Assist in the CM process.

Such a tool can range from a complex spreadsheet to a more advanced enterprise application. It is recommended that the organization start with a quickly developed and low-cost prototype. Once the process is better understood and refined, a more sophisticated tool might be appropriate.

SUMMARY

The approach presented above is one of several possible alternatives for solving the challenge of managing the security of multiple contracts requiring FISMA and special protection requirements.

The approach has the following advantages:

1. It provides rigorous, defensible proof that all required security controls have been addressed by the organization's Security Program;

2. It reduces costs by managing security resources across contracts that share common protection requirements;

3. It provides configuration management so that all security resources are well defined, the impacts of proposed changes can be evaluated, and approved changes are formally adopted; and,

4. It enables the application of automated tools to significantly reduce the burden of multiple contract security management.

The approach has the disadvantage of requiring the application of identifiers to the controls within security artifacts as well as the security requirements of each contract.

REFERENCES

[1] Federal Information Security Management Act of 2002, Title III of the E-Government Act (PL 107-347)

[2] NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

[3] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

[4] NIST SP 800-128, Guide for Security Focused Configuration Management

[5] NIST SP 800-18, Guide for Developing System Security Plans

ACRONYMS

AB	Accreditation Boundary
CM	Configuration Management
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
PM	Protection Metadata
SC	Special Controls
SSP	System Security Plan
SSPCN	SSP Control Number
SP	Special Publication